المواجهة القانونية والأمنية لجرائم الإرهاب الإلكتروني

م.د هادي طلال هادي

The Legal and security confrontation of cybercrime

Preparation

Hadi talal hadi

الخلاصة

تُعد جرائم الإرهاب الإلكتروني ظاهرة اجتماعية وجدت مع تطور المجتمعات البشرية لتأخذ أشكالاً وصورًا متعددة, فلا يخلو مجتمع من تلك الظاهرة على الرغم مما يشهده العالم من تقدم كبير في العلم والتكنولوجيا والمعلومات في سبيل وضع حد لهذه الظاهرة الخطيرة التي تمس أمن وسيادة الدول.لذلك سارعت الدول إلى دعم أجهزة الشرطة وإيجاد قوانين خاصة لمكافحة هذا النوع من الجرائم كما عقدت بعض الاتفاقيات الدولية في الإطار الدولي والإقليمي, الا أنها كانت وما تزال دون المستوى المطلوب, سيما وأن جرائم الإرهاب الإلكتروني من الجرائم التي تحتاج إلى تظافر الجهود من أجل مكافحتها وضبط تمددها, حيث تمتاز هذه الجرائم بأنها جرائم عابرة للحدود يفترض ان تتمثل مواجهتها بصورة حاسمة وقوية دون المساس بالحقوق العامة والحريات الأساسية, ويحتاج ذلك إلى رقابة حقيقية بين سلطات الدولة التشريعية والتنفيذية والقضائية لضمان مواجهتها من دون انتهاك لحقوق الأفراد التي يحميها الدستور, كما تتطلب مواجهة الإرهاب الإلكتروني البحث في أسباب الجريمة والتصدي لها فكريًا بصورة موازية لا تقل أهمية عن المواجهة القانونية والأمنية لها سواء على الصعيد الداخلي والدولي.

Abstract

Cybercrime is asocial phenomenon found with the development of societies to take multiple forms and images, there is no society without this phenomenon in spite of the great progress made by the world in science, technology and information in order to put an end to this dangerous phenomenon affecting the security and sovereignty of states. Therefore, States have been quick to support the police and to find special laws to combat type of crime, some international conventions were held in the international and regional framework, but they were still below the required level, especially as the crimes that need to be concerted efforts to combat and control the expansion. These crimes are characterized as cross- border crimes which are supposed to be decisive and strong without compromising public rights and fundamental freedoms This requires real control between the legislative, executive and judicial branches of state to ensure that they are addressed without violating the rights of individuals protected by the constitution. It also requires confronting electronic terrorism to research the causes of crime and address them intellectually in parallel, no less important than the legal and security confrontation both domestically and internationally.

الكلمات المفتاحية

١- مكتب التحقيقات الفيدرالي -Federal Bureau of Investigation

٢- المنظمة الدولية للشرطة الجنائية - International Criminal Police Organizati

٣- المكتب الأوروبي للشرطة "اليوروبول" -EUROPOL

مقدمة

أولاً- موضوع البحث:

نظرًا لتزايد الاعتماد في الآونة الأخيرة على تطبيقات الإنترنت بشكل واسع على الصعيدين الداخلي والدولي في كثير من الاعمال والمصالح, حتى أصبح من الصعب انجاز الأعمال بدونها في كثير من مجالات الحياة التي تدار من خلالها. ونتيجة لهذه المكانة المتميزة والفوائد الكثيرة التي لا تحصى مما حققته شبكة الإنترنت, إلا انه في الوقت ذاته استغل الإرهاب هذه الوسائل والإمكانيات الحديثة في الاتصال والتواصل وتطوير آلياته الإرهابية واتباع اساليب تسيء استخدام الشبكة, كاستخدامها لارتكاب جرائم تكون عرضة للهجوم والأخطار فعلي سبيل المثال تنظيم "داعش" الإرهابي وغيره من التنظيمات الإرهابية, يمتلك مئات المواقع الإلكترونية بالإضافة إلى القنوات الفضائية التي يستطيع من خلالها تحقيق اهدافه الغير مشروعة كاستخدام المقاتلين وبث الرعب والزعر بين الناس الآمنين, وهذا ما أدى إلى بروز مصطلح جديد من الجرائم يطلق عليه تسمية "جرائم الإرهاب الإلكتروني" الذي يُعرف بأنه: "الهجمات غير المشروعة أو التهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزونة الكترونيًا التي توجه من أجل الانتقام أو التأثير على الحكومات والشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية". كما يسمى هذا النوع من الإرهاب بالإرهاب الجديد لما تمثله هذه الهجمات من نقلة نوعية في تطوير ظاهرة الإرهاب في العصر الحديث التي تتسم بخصائص متميزة ومختلفة عن إرهاب العقود السابقة من حيث التنظيم والتسليح والأهداف التي أخذت تتفاعل وتتصاعد إلى مديات أبعد وأخطر مع زيادة التقدم الذي احرزته البشرية في تكنولوجيا وسائل الاتصال

المتعددة, وبذلك عد الإرهاب الإلكتروني أحد أخطر الجرائم التي ترتكب من خلال شبكة الإنترنت خاصةً بعد اختراق الإنترنت لجميع الحدود الدولية وهو ما يهدد الأمن القومي لجميع دول العالم. وهنا تعد المواجهة الأمنية والقوانين الداخلية والاتفاقيات الدولية هي أساس مواجهة مثل هذه الجرائم الإرهابية ورصد عناصرها, فقد اتجهت بعض الدول إلى تشريع قوانين خاصة لمواجهة جرائم الإرهاب الإلكتروني, واكتفت دول أخرى بالنص على هذه الجرائم في قوانينها العادية أو قوانين العقوبات الخاصة.فضلاً عن ذلك ان جرائم الإرهاب الإلكتروني تتطلب تعاون دولي حقيقي وفعال من أجل ابراز نتائج إيجابية أفضل في هذا المجال خاصةً ان التطور التكنولوجي وسيطرة شبكة المعلومات الدولية (الإنترنت) لها دور كبير في التأثير على مجريات الكثير من الأمور, وهنا كان لجهود المنظمة الدولية للشرطة الجنائية (الإنتربول), والمساعي الدولية القضائية دور بارز في هذا المجال.

ثانيًا- اهمية البحث: ان اهمية موضوع البحث تكمن من خلال التطرق إلى تحديات ومعوقات مواجهة جرائم الإرهاب الإلكتروني ودور أجهزة الشرطة والقوانين الداخلية ومدى إمكانية التعاون الأمني الدولي التي تعد المرتكزات الأساسية في الحد من جرائم الإرهاب الإلكتروني.

ثالثًا- إشكالية البحث: ان مشكلة البحث تتركز في عدة تساؤلات يمكن اثارتها أو عرضها على النحو الآتي:

- ما هي أهم التحديات التي واجهتها أجهزة الشرطة في مكافحة جرائم الإرهاب الإلكتروني.
- هل ساهمت القوانين الداخلية والاتفاقيات الدولية بوضعها الحالي في الحد من جرائم الإرهاب الإلكتروني.
- هل كان للمنظمة الدولية للشرطة الجنائية (الإنتربول) والمساعي القضائية الدولية دور أساسي في مواجهة جرائم الإرهاب الإلكتروني.

رابعًا- منهجية البحث: المنهج المتبع في هذا البحث هو منهج الدراسة القانونية مع اجراء دراسة تحليلية تأصيلية لكل جزئية من الجزئيات المتعلقة بموضوع البحث الموسوم بـ "المواجهة القانونية والأمنية لجرائم الإرهاب الإلكتروني".

خامسًا- خطة البحث: يقسم موضوع البحث إلى مبحثين يتناول المبحث الأول موقف أجهزة الشرطة من جرائم الإرهاب الإلكتروني في إطار التشريعات الوطنية, أما المبحث الثاني فيتناول موقف التعاون الأمني الدولي في مواجهة جرائم الإرهاب الإلكتروني, بالإضافة إلى خاتمة نستعرض فيها اهم النتائج والتوصيات التي تم التوصل اليها.

المبحث الأول موقف أجهزة الشرطة من جرائم الإرهاب الإلكتروني

في إطار التشريعات الوطنية

ان تطور وسائل الاتصال وانتشارها بشكل واسع على المستوى الاقليمي والدولي ادى إلى تحول العالم إلى قرية صغيرة من حيث سهولة تبادل المعلومات وتقديم الخدمات بشكل سريع سواء للمؤسسات أو للأفراد, وفي مؤازاة ذلك ترتب على هذه الثورة الكبيرة التي حققتها حضارة تقنيات وعصر المعلومات إلى ظهور الإرهاب الإلكتروني الذي يعد اليوم من أخطر الجرائم التي ترتكب عبر شبكة الإنترنت وهو بذلك يمثل تهديدًا وخطرًا مباشرًا للأمن الداخلي والدولي. لذا قامت العديد من الدول بتدعيم أجهزة الشرطة لمواجهة جرائم الإرهاب الإلكتروني خاصةً بعد تعرضها لهجمات إرهابية عاتية, ألزمتها بفرض قوانين صارمة لمواجهة هذا النوع من الجرائم, وهناك دول لا تزال تواجه بعض التحديات والاشكالات القانونية والسياسية والاقتصادية والتعليمية, مما جعل دورها ضعيف في مواجهة هذا النوع من الجرائم الخطرة, عليه تم تقسيم هذا المبحث إلى مطلبين نتناول في المطلب الأول التحديات التي تواجه جهاز الشرطة في مكافحة جرائم الإرهاب الإلكتروني, أما المطلب الثاني نتناول فيه السلطات القانونية لجهاز الشرطة في مواجهة جرائم الإرهاب الإلكتروني.

المطلب الأول: التحديات التي تواجه جهاز الشرطة في مكافحة جرائم

الإرهاب الإلكتروني: ان استخدام شبكات الإنترنت اصبح ذات اهمية اساسية لا يمكن الاستغناء عنها في الحياة البشرية, الا أنها في الوقت ذاته تعتبر خدمة غير مقصودة للتنظيمات الإرهابية التي قامت باستغلالها في إتمام عملياتها ضد أمن الشعوب والمجتمعات من حيث نقل الأفكار والبيانات والمعلومات إلى عناصر الجماعات الإرهابية في غفلة من الأجهزة الأمنية في بداية الأمور, مما أدى إلى انتشار التنظيمات الإرهابية بشكل واسع من خلال البيانات والمعلومات التي يتم إرسالها عبر شبكات الإنترنت. وان مخاطر هذا النوع من الإرهاب يزداد كلما زاد التطور في وسائل الاتصالات وثورة المعلومات "الإنترنت", التي بات الجميع يستخدمها سواء في اتصالاتهم أو تنفيذ وظائفهم أو القيا بأنشطة إرهابية, كالتجسس أو تدمير الفعاليات الإلكترونية للدول والمؤسسات التابعة لها, من خلال الولوج إلى المعلومات الحكومية المخزونة الكترونيًا واستخدامها كوسيلة لابتزاز الحكومات والتأثير عليها لتحقيق أهدافها وايديولوجيتها العدائية, الأمر الذي أدى إلى زيادة عدد

الأصوات المطالبة بمكافحة الجرائم الإلكترونية[١], وهو ما تحقق في عام ٢٠٠١ عندما أبرمت اتفاقية بودابست الأولى لمكافحة الجرائم الإلكترونية[٢].**هنا يثار التساؤل:** ما هي الآليات التي تستخدمها الجماعات الإرهابية لتحقيق جرائم الإرهاب الإلكتروني؟ للإجابة على هذا التساؤل يمكن القول ان الآليات التي تستخدمها الجماعات الإرهابية تتحدد من خلال:

أولاً- استخدام شبكات الإنترنت لتحقيق الهجمات الإرهابية: وذلك من خلال اللجوء إلى الأعمال التخريبية التي تستهدف شبكات الحاسوب والإنترنت سواء كانت عسكرية أو اقتصادية أو أمنية أو غيرها, وهي أشبه ما يكون بعملية الاختطاف الإلكتروني والتي من شأنها تهدد الأمن القومي أو العسكري أو الاقتصادي لدولة ما أو لعدة دول, حيث من الممكن تهديد الاقتصاد الدولي من خلال اقتحام مواقع البورصة العالمية أو اختراق برامج الاتصالات في مطار دولة ما, أو القيام بتعطيل رحلاته والأخطر من هذا كله التسلل إلى الأنظمة الأمنية والتجسس عليها لصالح جماعات إرهابية[٣], ومن أبرز الأمثلة الواقعية على ذلك عندما تمكن أحد القراصنة من السيطرة على نظام الكومبيوتر في مطار أمريكي وإطفاء مصابيح إضاءة ممرات الهبوط مما هدد بحصول كارثة, وكذلك ما حدث في ايطاليا حيث تعرضت عدة وزارات وجهات حكومية ومؤسسات مالية لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها, وما حدث في عام ٢٠٠١ عندما اخترق متسللون حاسبات شبكة كهرباء كاليفورنيا[١]

ثانيًا- استخدام الدعاية كوسيلة لتحقيق الهجمات الإرهابية: وذلك من خلال قيام الجماعات الإرهابية ببث دعايتهم عن طريق الإنترنت, وعادةً ما تتخذ الدعاية شكل اتصالات عبر وسائط متعددة تحمل تعاليم إيديولوجية أو إرشادات عملية أو تقديم شروحًا للأنشطة الإرهابية أو التشجيع على القيام بها, وعلاوة على ذلك فإن بث الدعاية ليس نشاطًا محظورًا في حد ذاته فأحد المبادئ الأساسية للقانون الدولي هو حماية حقوق الإنسان الأساسية التي تشمل الحق في حرية التعبير في حالات مشروعة لا تسبب ضررًا بالأمن القومي للدولة, أما اذا كان الغرض من الدعاية هو الإضرار بالمصلحة العامة للدولة, فان ذلك يعتبر عملاً إرهابيًا مخالفًا للقانون كالتشجيع على العنف أمرًا شائعًا في الدعاية الإرهابية, وكذلك الترويج للخطاب المتطرف الذي يشجع على أعمال العنف[٢]. فضلاً عن ذلك ان الدوافع الأساسية للإرهاب الإلكتروني ترجع إلى أسباب سياسية واقتصادية واجتماعية وفكرية ونفسية, ويمكن أن ترجع إلى أسباب عامة من الصعب معرفتها, ولكن هناك أسباب خاصة أو تحديات تواجه جهاز الشرطة في الحد من الجرائم الإرهاب الإلكتروني, التي يمكن إجمالها على النحو الآتي:

أولاً- التحديات الأمنية: تتمثل في نقص الخبرات الفنية في مجالات تحديد أركان الجريمة الإلكترونية وتقديمها كقضية مكتملة أمام القضاء, بالإضافة إلى صعوبة الرصد والتحقيق ورفع الأدلة الرقمية في كل زمان ومكان, هذه كلها تشكل عوامل تحد من فاعلية المواجهة, فضلاً عن الحدود الفنية والعلاقات بين أطراف أي قضية عبر الإنترنت والتي تتجاوز حدود الدولة الوطنية, وكذلك العدد الهائل من المخالفات والمخالفين على مدار الساعة وهو ما يجعل الضبط والملاحقة من الأمور الصعبة[٣].

ثانيًا- التحديات القانونية وغياب جهة السيطرة والرقابة على شبكات الإنترنت: ان التحديات القانونية تتمثل في عدم استيعابها لجرائم الإرهاب الإلكتروني, فالمجرم يستطيع الانطلاق من دولة لا توجد فيها قوانين صارمة, وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق في هذه الجرائم, وكذلك صعوبة وضع معايير واضحة لتحديد الموقع المتطرف والمحرض على العنف والتباس الكثير من المفاهيم وعدم القدرة على تحديد المسؤول المباشر على المحتوى التحريضي أمام القضاء[١]. كما ان انعدام وجود جهة مركزية موحدة تتحكم فيما يعرض على شبكة الإنترنت وتسيطر على مدخلاتها ومخرجاتها يعد سببًا رئيسيًا في مواجهة ظاهرة الإرهاب الإلكتروني, حيث يمكن لأي شخص الدخول ووضع ما يريد على شبكة الإنترنت وان كل ما تملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول إلى بعض المواقع المحجوبة أو إغلاقها وتدميرها بعد قيام المجرم بنشر ما يريده وهذا من شأنه يعيق النظر في بعض القضايا.

ثالثًا- قلة الوعي الأمني: ان معظم مستخدمين شبكة الإنترنت لا يعود بأهمية الإجراءات التي يجب اتخاذها في تأمين معلوماتهم وأجهزتهم أثناء الاتصال بالشبكة حيث يتعامل معظم مستخدمي شبكة الإنترنت باستخفاف ظاهر مع ما يسمعون به يوميًا من اختراقات, وقد أظهرت استطلاعات الرأي ان ثلثي مستخدمي الوصلات عالية السرعة لا يستخدمون جدرانًا نارية[*] أو يستخدمونها ولكن بشكل خاطئ وهذا ما يساعد العابثين والمجرمين على تحقيق أهدافهم[٢].

رابعًا- صعوبة اكتشاف وإثبات الجريمة الإرهابية: في كثير من جرائم الإرهاب الإلكتروني لم يتم العلم بوقوع الجريمة أصلاً, وخاصةً في مجال جرائم الاختراق إذ تتعرض الأجهزة يوميًا لمحاولات اختراق دون أن يشعر مستخدموها, حيث يكتفي بتشغيل برنامج حماية يكشف عن هذه المحاولات مثل "Internet Zone" للتحقيق من تفشي هذه الهجمات الإرهابية, وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع

التي يستهدفها قبل ان ينفذ جريمته, بالإضافة إلى ذلك ان صعوبة الإثبات تعد من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني لأنها تعطي المجرم أملاً في الإفلات من العقوبة[١].

خامساً- سهولة الاستخدام وقلة التكلفة: ان شبكات الاتصال (الإنترنت) أصبحت زهيدة التكلفة ومتوفرة في جميع دول العالم بخلاف عقد الثمانينات من القرن الماضي, ونظرًا لسهولتها وقلة تكلفتها مما جعلها فرصة مهيئة للإرهابيين في الوصول إلى أهدافهم غير المشروعة والقيام بجرائم الإرهاب الإلكتروني[٢]. اعتمادًا على ما تقدم يمكن القول ان خطورة جرائم الإرهاب الإلكتروني تتعاظم, وتزداد التحديات لدى جهاز الشرطة في مكافحتها بحالتين الأولى: عند اتساع اعتماد المجتمعات على تقنية أنظمة المعلومات سواء في نطاق الدولة الواحدة أو في النطاق الاقليمي أو الدولي, أما الحالة الثانية فتكون عند ضآلة أو انعدام البيئة التشريعية اللازمة لمكافحة الجرائم المستحدثة والتي منها جريمة الإرهاب الإلكتروني.فضلاً عن ذلك يلاحظ منذُ سنوات عديدة إعداد الكثير من الأبحاث والدراسات الأمنية في مواجهة الظواهر الإجرامية, إلا أن الواقع يؤكد أن تلك الأبحاث والدراسات تظل حبيسة المكتبات, ولا يخرج منها إلى أرض الواقع الا القليل, مما يجعل جهاز الشرطة يستمر في اعتماده على الوسائل البدائية لمواجهة الجريمة التي تتطور بشكل سريع يومًا بعد يوم, ويرجع ذلك إلى عدة أسباب يمكن إيجازها على النحو الآتي:

١- عدم قناعة العديد من قيادات أجهزة الشرطة بالوسائل العلمية من الناحية التطبيقية, والتي قد تتأخر نتائجها قليلاً إلا أنها تقوم بتصحيح النظام الإداري وتقويته بما يسمح بمواجهة جميع الجرائم بصفة عامة, وجريمة الإرهاب الإلكتروني بصفة خاصة.

٢- افتقار جهاز الشرطة إلى نظام إداري يربط بين الأبحاث والدراسات الخاصة بتطوير المهام الشرطوية من جهة, وبين تطبيق ذلك من الناحية العملية من جهة أخرى.

٣- عدم وجود قانون أو نظام إداري قوي بالدولة ينظم عملية التنسيق بين أجهزة الدولة المعنية بمواجهة جرائم الإرهاب الإلكتروني, وبين الوزارات والمؤسسات التعليمية.

المطلب الثاني السلطات القانونية لجهاز الشرطة في مواجهة جرائم

الإرهاب الإلكتروني: يعد الإرهاب الإلكتروني جريمة جنائية لاحتوائها على أبعاد مختلفة من الجرائم كالقتل واستخدام المفرقعات والسطو والسرقة والإتلاف, لذلك قامت العديد من الدول بتدعيم جهاز الشرطة في مواجهة جرائم الإرهاب الإلكتروني, خاصةً تلك الدول التي تعرضت لهجمات إرهابية عاتية الأمر الذي جعلها أمام قوانين صارمة لا تتناسب مع الحقوق والحريات التي كانت تنادي بها, بل تتصارع معها أحيانًا, وقد يحسم هذا الصراع من خلال مدى سيطرة الأجهزة الأمنية على فرض الأمن فكلما إستتب الأمن كان للحقوق والحريات المكانة الأسمى في المجتمع, ومتى انتشرت الجريمة كان للقوانين التي تسلب الحريات مكانها واحترامها حتى يتم تحقيق الأمن بشكل كامل. فاذا كان مفهوم الإرهاب بصورة عامة أصبح مصطلح تقليدي واضح المعالم فإن الإرهاب الإلكتروني لا يزال جريمة مستحدثة يكتنفها بعض الغموض لأنها جريمة تعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابها, ومن حيث دور الفاعل وطبيعة سلوكه, وما يقوم بتسببه بأضرار واسعة الانتشار وعظيمة الأثر على المجتمع والأفراد, ومن أجل الوقوف على المرتكزات القانونية لجريمة الإرهاب الإلكتروني يتطلب أولاً معرفة أركان جريمة الإرهاب الإلكتروني بوصفها فعل إجرامي لا بد ان تتوافر فيها بعض الشروط اللازمة لقيامها وهذه الأركان تكون على نوعين هما:

أولاً- الركن المادي لجريمة الإرهاب الإلكتروني: تتوافر صور وأشكال الركن المادي لجريمة الإرهاب الإلكتروني من خلال إمكانية وقوع الفعل باستخدام تقنية أنظمة المعلومات, وذلك من خلال:

(أ) استخدام قدر كاف من العنف التهديدي وان استخدام العنف كمفهوم تقليدي في ظل سلوك إلكتروني معنوي يأتيه الفاعل يبقى خارج نطاق البحث, وان أمكن تصور مفهوم مستحدث للعنف المقصود بالنص ذو بعد معنوي بمعنى أن ينظر إلى العنف كنتيجة لسلوك معنوي إلكتروني, ووفقًا لذلك يمكن تصور عنف معنوي ظاهر في مدى قدرة الفاعل على استخدام تقنية أنظمة المعلومات بقدر كافٍ لإيقاع الضرر المقصود, أما التهديد بالعنف فالأمر ممكن في ظل بيئة إلكترونية[١], وهنا يكون تحقيق السلوك الإجرامي مؤكدًا في جريمة الإرهاب الإلكتروني.

(ب) ان يؤدي استخدام العنف أو التهديد به إلى إيقاع الرعب بين الناس أو تعرض حياتهم للخطر, وهنا تتحقق النتيجة الضارة بمجرد حدوث تغيير في النطاق المادي أو المعنوي الذي طاله الفعل أي حدوث تغيير في السلوك الإجرامي للفعل. فالنتيجة الضارة لجريمة الإرهاب

الإلكتروني تزداد خطورتها كلما اتسع استخدام الحواسيب الآلية والشبكات المعلوماتية, مما يجعلها هدفًا سهل المنال فبدلاً من استخدام المتفجرات تستطيع الجماعات الإرهابية الضغط على لوحة المفاتيح بغية تحقيق آثار تدميرية تفوق مثيلتها التي يستخدم فيها المتفجرات, حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية أو تعطيل أنظمة الدفاع الجوي أو التحكيم في خطوط الملاحة الجوية والبرية والبحرية أو شل محطات إمداد الطاقة والماء أو اختراق الأنظمة المصرفية وإلحاق الضرر بأعمال البنوك وغير ذلك من الأعمال الإرهابية المشابهة[٢].

(ج) تعتبر العلاقة السببية هي الصلة التي تربط ما بين السلوك الإجرامي والنتيجة الضارة, وتثبت ان ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة الضارة, وعلى مستوى جرائم الإرهاب الإلكتروني تكون العلاقة السببية من خلال ارتباط السلوك الإجرامي المتمثل باستخدام الإنترنت بصورة مخالفة للقانون بالنتيجة الضارة المترتبة على الفعل المخالف للقانون[٣]. ومما تجدر الاشارة اليه ان الجاني في بعض الاحيان قد يقوم بتحقيق النتيجة من خلال السلوك الإجرامي, كاستخدام الإنترنت مثلاً لتجنيد المقاتلين للقيام بتنظيم مسلح ضد طائفة معينة واستطاع من وراء هذا الفعل أو السلوك تحقيق الهدف المرجو من سلوكه, فهنا تكون الجريمة تامة وحتى وان لم يترتب على فعله أي نتيجة, ففي كل الأحوال يكون هنا الجاني معرضًا للمسائلة الجنائية في كلا الحالتين عن الجريمة التامة وعن الشروع في الجريمة. وفي إطار هذه المحددات يمكن تصور أشكال السلوك المعنوي القادر على اظهار الإرهاب الإلكتروني إلى حيز الوجود كجرائم مستوجبة العقاب وذلك من خلال[١]:

١- استخدام العنف أو التهديد باستخدامه بهدف تعرض أمن وسلامة المجتمع للخطر أو الاخلال بالنظام العام, وهنا لا يشترط تحقيق الضرر أو الإخلال بل يكتفي بمجرد احتمال وقوعه, كتلاعب الفاعل بأنظمة إدارة وتشغيل الإشارة الضوئية أو اختراق الفاعل لأنظمة ضخ الغاز عبر منشآت الدولة الحيوية.

٢- استخدام العنف أو التهديد باستخدامه بهدف إلحاق الضرر بالبيئة أو المرافق العامة, مثال ذلك التلاعب بأنظمة ضخ المياه والكهرباء باستخدام تقنية أنظمة المعلومات.

٣- استخدام العنف أو التهديد باستخدامه بهدف تعطيل أحكام الدستور والقوانين.

٤- استخدام العنف أو التهديد باستخدامه بهدف الإضرار بالموارد الوطنية وتعرضها للخطر .

٥- استخدام العنف أو التهديد باستخدامه بهدف اختراق شبكات تقنية أنظمة المعلومات أو التشويش عليها.

أي بمعنى ان أي عمل إلكتروني أو التهديد باستخدامه يؤدي إلى تعرض أمن وسلامة المجتمع للخطر أو أدى إلى الاخلال بالنظام العام يمكن ان يعتبر ضمن نطاق جرائم الإرهاب الإلكتروني.

ثانيًا- الركن المعنوي لجريمة الإرهاب الإلكتروني: اذا كانت الجريمة بشكل عام تقوم على الركن المعنوي القائم على عنصري العلم والإرادة فإن الإرهاب الإلكتروني لا يكتفي فيه القصد العام, بل لا بد ان يعلم الفاعل بالسلوك الإجرامي الذي يرتكبه وإرادة ارتكاب هذا السلوك لقيام الجريمة, أي ان يتوفر ثبوت القصد الخاص بالإضافة إلى القصد العام في نية الفاعل وهو يقوم باستخدام تقنية نظم المعلومات, وان يهدد بإيقاع أحد الأغراض المعلنة في الجريمة[٢]. فضلاً عن ذلك ان التكييف القانوني لجريمة الإرهاب الإلكتروني يتطلب ان يكون قائمًا على مبدأ شرعية الجرائم والعقوبات مع الالتزام بمبادئ الضرورة والتناسب عند التجريم والعقاب, وهذا ما فعله المشرع العراقي في قانون مكافحة الإرهاب رقم (١٣) لسنة ٢٠٠٥ الذي بين بأنه "كل فعل إجرامي يقوم به فرد أو جماعة منظمة استهدف فردًا أو مجموعة أفراد أو جماعات أو مؤسسات رسمية أو غير رسمية أوقع الأضرار بالممتلكات العامة أو الخاصة بغية الإخلال بالوضع الأمني أو الاستقرار والوحدة الوطنية أو إدخال الرعب والخوف والفزع بين الناس أو اثارة الفوضى تحقيقًا لغايات إرهابية"[١], ويتضح من ذلك ان المشرع العراقي حدد الأفعال التي تعد اعمالاً إرهابية فضلاً عن تحديد العقاب المقرر لكل عمل من هذه الاعمال الإرهابية[٢]. ونظرًا لكون جمهورية العراق من أكثر الدول التي عانت من ويلات الإرهاب وما خلفه من عنف وترويع بين أوساط المواطنين الأبرياء, مما دفع المشرع العراقي إلى وضع نظام إجرائي خاص للتعامل مع الجرائم الإرهابية والتصدي لها ومواجهتها من خلال وضع قواعد تشريعية تسمح بالتعامل مع الطبيعة الخاصة للجرائم الإرهابية والتوسع في منح جهات إنفاذ القانون وتكليف جهاز الشرطة سلطات أوسع لمواجهة الجرائم الإرهابية والسيطرة عليها.وبذلك نصت المادة (١/٣) من قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥, على اعتبار كل فعل ذو دوافع إرهابية من شأنه تهديد الوحدة الوطنية وسلامة المجتمع ويمس أمن الدولة واستقرارها أو يضعف من قدرة الأجهزة الأمنية في الدفاع والحفاظ على أمن المواطنين

وممتلكاتهم وحدود الدولة ومؤسساتها سواء بالاصطدام المسلح مع قوات الدولة أو أي شكل من الاشكال التي تخرج عن حرية التعبير التي يكفلها القانون. كما اشارت المادة (٢/٣) من قانون جهاز مكافحة الإرهاب العراقي رقم (٣١) لسنة ٢٠١٦, ان تنفيذ العمليات الأمنية والخطط الاستراتيجية لمكافحة جرائم الإرهاب تتم من خلال:

١- تنفيذ عمليات المراقبة والتحري بناءً على الأوامر القضائية.

٢- مراقبة الاتصالات ومواقع التواصل الاجتماعي والمواقع الإلكترونية بناءً على أوامر قضائية.

٣- تنفيذ أوامر القبض الصادرة من قبل القاضي المختص وفقًا لقانون مكافحة الإرهاب.

٤- التنسيق والتعاون وتبادل المعلومات مع الأجهزة الأمنية والأجهزة ذات العلاقة.

٥- التنسيق والتعاون وتبادل المعلومات ذات العلاقة بمكافحة الإرهاب مع الأجهزة النظرية للدول العربية والأجنبية.

٦- تعقب مصادر تمويل الإرهاب بهدف تجفيفها بالتعاون والتنسيق مع مكتب مكافحة غسيل الأموال والبنك المركزي العراقي والجهات الأخرى ذات العلاقة. ويتضح من ذلك ان المشرع العراقي قد منح الأجهزة الأمنية سلطات واسعة تساعدهم في مواجهة جرائم الإرهاب بصورة عامة, وجرائم الإرهاب الإلكتروني بصورة خاصة, واشتراط صدور إذن بإجراء عمليات مراقبة الاتصالات وشبكات الإنترنت من السلطة القضائية مع توافر التدابير الإجرائية المصرح بها كضمانات إجرائية مناسبة في تلك العمليات.**وهنا يثار التساؤل** عن كيفية مواجهة البرامج الإلكترونية التي تقوم بهجمات إرهابية وهي غالبًا لا تدار في داخل العراق, وانما تدار من دول أخرى خصوصًا وان قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥, وقانون جهاز مكافحة الإرهاب العراقي رقم (٣١) لسنة ٢٠١٦, لم ينص أو يتطرق إلى معالجة مثل هذه الحالات وهذا ما يدلل على وجود قصور في القانون ينبغي مراجعته. كذلك في حال إلقاء القبض على شخص يدير صفحة تابعة لجماعات إرهابية كيف يمكن أثبات آثار الجريمة وحتى لو تم أثبات آثار الجريمة فإن قانون أصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١, سيقف عائقًا أمام أثبات الجريمة الإلكترونية, لأن القضاء العراقي لا يأخذ بالأدلة الإلكترونية إلا في حدود ضيقة جدًا وهذا ما أكدت عليه المادة (٢١٣) من قانون أصول المحاكمات الجزائية العراقي, وهذا أيضًا يدل على وجود قصور في القانون ينبغي مراجعته.ففي الولايات المتحدة الأمريكية منح التشريع الوطني سلطات واسعة لأجهزة الشرطة في مكافحة جرائم الإرهاب الإلكتروني وذلك بموجب قانون "باتريوت عام ٢٠٠١" لمكافحة الإرهاب, الذي تضمن في القسم الثاني من الباب الأول منه توسيع نطاق أوامر التصنت والمراقبة لتشمل التصنت على المكالمات الهاتفية ومعالجة المعلومات والسماح بمراقبة الشبكات الإلكترونية, والسماح لمكتب التحقيقات الفيدرالي بالوصول إلى معلومات البريد الصوتي المخزونة من خلال مذكرة تفتيش وليس من خلال قوانين التصنت الأكثر صرامة[١]. وأشار الجزء (٢١٦) من القانون ذاته السماح لأجهزة الشرطة ان تحصل على كل عناوين البريد الإلكتروني التي تتواصل مع الشخص المشتبه فيه, مع فرض القانون على القضاة ان يمنحوا عناصر "FBI"[*] تصريحًا بالحصول على هذه العناوين بمجرد ادعائهم ان تلك المعلومات تتعلق بتحقيق جنائي, وبموجب هذا القانون لا يحق لـ "FBI" ان يطلع على مضمون الرسالة بل يطلع على العنوان فقط, كما أعطى القانون لأجهزة الشرطة الحق في معرفة كل المواقع الإلكترونية للأشخاص الذين يتراسلون معه والاطلاع عليها دون الحصول على تصريح جديد, وسمح هذا القانون لأي قاضي في محكمة المقاطعة في الولايات المتحدة الأمريكية بإصدار أوامر تسمح بهذه المراقبة وإصدار مذكرات تفتيش وتحريات عن المتهمين أو المشتبه في تورطهم في أنشطة إرهابية[٢].أما المشرع المصري منح بموجب قانون مكافحة الإرهاب المصري لسنة ٢٠١٥, أجهزة الشرطة سلطات واسعة في اتخاذ التدابير اللازمة للقبض على الاشخاص الذين يمثلون خطرًا على الأمن العام للدولة واحتجازهم وتفتيش مساكنهم دون التقيد بقانون الإجراءات الجنائية, كما خول القانون ذاته جهاز الشرطة بتسجيل المحادثات والرسائل في المواقع الإلكترونية لمنع الجرائم الإرهابية وضبط مرتكبيها, بالإضافة إلى ذلك جرمت المادة (٢٩) من القانون استخدام المواقع الإلكترونية في ترويج الأفكار والمعتقدات التي تدعو لارتكاب جرائم إرهابية[٣]. يتضح من ذلك ان جهود الدول في مكافحة جرائم الإرهاب الإلكتروني على المستوى الداخلي ما تزال دون المستوى المطلوب, سواء فيما يتعلق بإيجاد محاكم متخصصة أو دوائر تحقيق متخصصة للنظر في مثل هذا النوع من الجرائم خصوصًا ان جريمة الإرهاب الإلكتروني تتميز بذاتية خاصة من الناحية القانونية نظرًا لجسامتها وهو ما ينعكس بوجه خاص في تجريم أي عمل يساعد على وقوع الإرهاب والذي تقوم به الجماعات الإجرامية كتمويل الاعمال الإرهابية على سبيل المثال, ورغم الخطورة الحقيقية للجريمة الإرهابية إلا أن جهاز الشرطة يبقى الصمام الأمان للحد من هذه الجريمة الخطيرة ونظرًا لتطور جريمة الإرهاب الإلكتروني وعناصرها, أصبح من الضروري تطوير آليات العمل بجهاز الشرطة لكي يكون مواكبًا مع التطور الرهيب في عالم الجريمة, وان آليات التطور لا تقف

على تحديث الآلات والمعدات والاسلحة, وانما تمتد إلى تطوير رجال الشرطة انفسهم من حيث اعدادهم وتأهيلهم بما يتواكب مع تطور الجريمة الإرهابية وخطورتها.

المبحث الثاني موقف التعاون الأمني الدولي في مواجهة جرائم

الإرهاب الإلكتروني: لا شك ان جريمة الإرهاب الإلكتروني بالإضافة إلى كونها من الجرائم التي تمس الكيان الداخلي للدولة أي كونها من الجرائم الداخلية فأنها تمتد أيضًا إلى الصعيد الدولي. كانت صور التعاون الأمني الدولي من أهم الصور في مجال مكافحة جرائم الإنترنت وتعقب مجرمي المعلوماتية وشبكة الإنترنت وتعقب الأدلة الرقمية وضبطها, والقيام بعمليات التفتيش العابر للحدود لمكونات الحاسب الالي المنطقية والأنظمة المعلوماتية وشبكات الاتصال, وهذه كلها أمور تستدعي القيام ببعض العمليات الشرطوية والأمنية المشتركة لمكافحة هذا النوع من الجرائم الخطرة ووضع حد لها. بذلك حققت المواجهة الأمنية الدولية نجاحًا ملموسًا في مكافحة جرائم الإرهاب الإلكتروني الا ان التعاون الدولي في هذا المجال يقف عند حد معين وتبقى أسباب انتشار ظاهرة الإرهاب الإلكتروني تساعد في نمو أجيال أخرى من الإرهابيين, ولمعرفة صور التعاون الأمني الدولي في هذا المجال تقسم الدراسة في هذا المبحث إلى مطلبين يتناول المطلب الأول جهود منظمة الإنتربول في مواجهة جرائم الإرهاب الإلكتروني, ويتناول المطب الثاني المساعي القضائية الدولية لمواجهة جرائم الإرهاب الإلكتروني.

المطلب الأول: جهود منظمة الإنتربول (Interpol)(١) في مواجهة جرائم

الإرهاب الإلكتروني: تعتبر جرائم الإرهاب الإلكتروني من الجرائم الدولية إذا كانت مخالفة للقواعد الدولية التي تترتب عليها المسؤولية الجنائية, سواء تلك التي نصت عليها الاتفاقيات الدولية أو تضمنتها القواعد الدولية العرفية, أو من خلال توافر العناصر الآتية[١]:

١- ان لا يقتصر الإرهاب الإلكتروني على دولة بعينها, وإنما يتجاوز الحدود الوطنية للدولة سواء فيما يتعلق بالمتهمين أو بالوسائل المستخدمة.

٢- ان تتم الأعمال الإرهابية بدعم الدولة أو تشجيعها أو موافقتها التي يوجد فيها مرتكبو هذه الأعمال أو بدعم دولة أجنبية, وهذا ما جاء في المادة الثانية من اتفاقية المعاقبة على تمويل الإرهاب في عام ١٩٩٦, مثال ذلك استخدام بعض وسائل الإعلام لخدمة أهداف معينة.

٣- تعلق الإرهاب الإلكتروني بالمجتمع الدولي على اعتباره يمثل تهديدًا لأمن هذا المجتمع, كما أنه لا يقبل أي حل تفاوضي ولا يبغي سوى النصر مهما كان الثمن غاليًا في فقد الأرواح والدمار الذي يحققه.

٤- اذا بلغت الاعمال الإرهابية المتمثلة باستخدام التكنولوجيا الحديثة حدًا كبيرًا من الجسامة, ففي هذه الحالة لا ينظر إلى المجني عليهم أفرادًا بل ينظر إلى الإنسانية كلها محلاً لهذا الاعتداء, وهذا بلا شك يعد جريمة دولية بوصفها ماسة بالقيم التي يؤمن بها المجتمع الدولي.

كما أضاف بعض الفقه[٢], صفة الدولية على جرائم الإرهاب الإلكتروني على اعتبار أن هذه الجريمة مرتبطة بالشبكة الدولية الإنترنت, كما لو قام الجاني الذي يحمل جنسية دولة معينة باستخدام شبكة الإنترنت في اقليم دولة أخرى لتحريض الأفراد في مجتمع معين ودفعهم للالتحاق بتنظيم مسلح للقيام بأعمال مسلحة ضد دولة معينة معادية لنظامه السياسي بدافع نصرة دين معين أو طائفة أو مجتمع معين وهذا يعني ان جريمة الإرهاب الإلكتروني لا تعد جريمة دولية إلا اذا توافر الركن الدولي فيها أي وقوع الجريمة من دولة ضد دولة أخرى بقصد المساس بحسن سلامتها وأمنها الداخلي والخارجي, وهذا الركن يلزم توافره لخضوع الفعل لأحكام القانون الدولي حتى وان لم تنص عنه الاتفاقيات المتعلقة بهذا الخصوص. هنا كان للمنظمة الدولية للشرطة الجنائية (الإنتربول) دورًا في مكافحة جرائم الإرهاب الإلكتروني من خلال تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة, وجمع البيانات والمعلومات المتعلقة بالمجرم والجريمة عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في اقاليم الدول المنضمة إليها وتتبادلها فيما بينها, فضلاً عن التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها, لا سيما الجرائم المتشعبة في عدة دول كجرائم الإنترنت. مرت جهود المنظمة في هذا المجال بمراحل متعددة نظرًا لتنوع أنظمة الدول المختلفة, فكان هناك خياران لأنظمة الاتصال داخل هذه الشبكة أولهما هو أنموذج يخصص للدول المركزية وتجري الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بوساطة السكرتارية العامة, والثاني للدول اللامركزية, وتجري الاتصالات فيه مباشرةً بين أجهزة الشرطة في الدول المختلفة[١].ففي سبتمبر عام ٢٠١٧ افتتحت المنظمة الدولية للشرطة الجنائية (الإنتربول), أعمال جمعيتها لمناقشة مشكلات جرائم الإرهاب الإلكتروني, وكانت أهم المحاور التي تمت مناقشتها هي تبادل المعلومات بين أجهزة الشرطة واعتماد الإنتربول على مستخدمي الشبكة

العنكبوتية للحصول على معلومات تخص المتهمين[٢].مما لا شك فيه ان أهم وسائل التحري عن اتجاهات الجريمة في الخارج لمنع وصولها إلى دولة ما, والتي تتبعها المنظمة الدولية للشرطة الجنائية (الإنتربول) هي الحصول على المعلومات التي يوفرها الإنتربول من خلال استخباراتها الجنائية وشبكة معلوماتها الحاسوبية التي تضم الكثير من المعلومات المتجددة في هذا المجال, من خلال تحقق المنظمة الدولية للشرطة الجنائية (الإنتربول) عدة مهام مفيدة في مجال تبادل المعلومات والتعاون الدولي ضد الجريمة المرتكبة عبر الدول بالإضافة إلى ان هذه المنظمة ركزت أنشطتها على الجرائم الإلكترونية كجريمة غسيل الأموال وغيرها من الجرائم[٣]. وفي ذات السياق ان المنظمة الدولية للشرطة الجنائية (الإنتربول) تشغل حاليًا شبكة اتصالات لاسلكية مؤمنة تغطي كافة أنحاء العالم من خلال ربط المكاتب الوطنية للدول الأعضاء مع بعضها البعض, وقد تسهل هذه الشبكة النقل السريع للرسائل الإلكترونية والتي تشمل الرسائل المكتوبة والصور الفوتوغرافية والبصمات, كما طورت هذه المنظمة منظومة الاتصالات الشرطوية العالمية "i-7/24" لوصول أجهزة إنفاذ القانون في الدول الأعضاء, الأمر الذي يتيح للمستخدمين المرخص لهم تبادل البيانات الشرطوية الهامة فيما بينهم والوصول إلى قواعد بيانات المنظمة, وذلك كله من أجل تسهيل عمل المنظمة بشكل فعال وكفوء[١]. يمكن القول دور المنظمة الدولية للشرطة الجنائية (الإنتربول) في التعاون الدولي يقتصر على الجوانب الآتية:

١- التعاون الدولي في إعطاء المعلومات حول مجرم موقوف أو هارب والتزويد ببصمات أصابعه والآثار الأخرى التي يرتكبها في محل الحادث.

٢- التعاون على تحذير الدول من وقوع جرائم جديدة قد يقوم بها مجرم مطلق السراح, وذلك من أجل حماية الأمن الدولي.

٣- التعاون الدولي على مكافحة الجرائم الخطيرة التي ظهرت حديثًا في المجتمع الدولي كجريمة الإرهاب الإلكتروني وغيرها من الجرائم.

اعتمادًا على ما تقدم على الرغم من الجهود التي بذلتها المنظمة الدولية للشرطة الجنائية (الإنتربول) في سعيها لمكافحة الجريمة بصورة عامة وجرائم الإرهاب الإلكتروني بصورة خاصة, إلا ان الملاحظ ان ازدياد ظاهرة الإجرام الإلكتروني بات يشكل تهديدًا خطيرًا على المجتمع الدولي, حيث ان محترفي الجرائم أصبحوا يستفادون من التطور التكنولوجي لتنفيذ عملياتهم الإجرامية, فإذا ما اكتفت المنظمة الدولية للشرطة الجنائية (الإنتربول) بما لديها من وسائل وأساليب لمكافحة الجريمة فأنها تكون خلال فترة وجيزة بعيدة كل البعد عن اداء دورها في مكافحة الجريمة. ومن الجدير بالذكر فقد تم أنشاء وكالات إقليمية لمكافحة الجرائم على غرار منظمة الإنتربول, منها وكالة تطبيق القانون الأوروبية "يوروبول"[١], وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في مجالات مكافحة الجرائم الدولية الكبيرة العابرة للحدود كجرائم الإرهاب الإلكتروني وغيرها من الجرائم, وفي الإطار العربي صدر عن جامعة الدول العربية اتفاقية حديثة تعنى بمكافحة جرائم الإنترنت, سميت "الاتفاقية العربية لمكافحة جرائم المعلومات" التي دخلت حيز التنفيذ عام ٢٠١٠, وتعد هذه الاتفاقية نقطة تحول في التعاون العربي لمكافحة هذه الجرائم الخطرة. رغم ذلك فان الجهد الدولي يبقى ناقصًا لعدم وجود اتفاقية دولية أو إقليمية متخصصة بجرائم الإرهاب الإلكتروني تناقش آلية مكافحة هذه الجرائم الخطرة, وملاحقة المجرمين والقبض عليهم وتبادل المعلومات بين الدول والاختصاص القضائي كون هذه الجرائم عابرة للحدود يسهل ارتكابها ويصعب إثباتها.

المطلب الثاني :المساعي القضائية الدولية لمواجهة جرائم

الإرهاب الإلكتروني: نظرًا لكون جرائم الإنترنت ذات طابع دولي فإن آثارها تمتد لعدة دول وملاحقة مرتكبيها وتقديمهم للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال إجرائية خارج حدود الدولة, لذلك تشير معظم الاتفاقيات الدولية الخاصة بالجرائم ومكافحتها إلى المساعدة القضائية المتبادلة[١], والتي تتخذ في المجال الجنائي صورًا متعددة منها:

أولاً- تبادل المعلومات: يتضمن تبادل المعلومات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أو أمنية أجنبية بصدد جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والاجراءات التي اتخذت ضدهم, كما يشمل تبادل المعلومات تبادل السوابق القضائية للجناة[٢], وهذا ما نصت عليه المادة (٧/د) من اتفاقية المنظمة الدولية العربية للدفاع الاجتماعي ضد الجريمة عام ١٩٦٤, على ان "يعمل المجلس لتحقيق أغراض المنظمة فيما يتعلق بتبادل المعلومات والبيانات والاحصائيات والمطبوعات".كذلك ما نصت عليه المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي عام ١٩٨٥, تحت عنوان: "تبادل المعلومات" على ان تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية, كما تتبادل المعلومات المتعلقة بالتنظيم القضائي, وتعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية والتنسيق بين

الأنظمة القضائية لدى الأطراف المتعاقدة حسبما تقتضيه الظروف الخاصة بكل منها. وفي إطار جرائم الإرهاب الإلكتروني نرى ضرورة أبرام اتفاقيات ثنائية أو جماعية للتعاون الدولي بشأن تبادل المعلومات المتعلقة بهذا النوع من الجرائم الخطرة والتغلب على جميع التحديات التي تواجهها, خاصةً وان مؤتمر الأمم المتحدة الثامن لمنع الجريمة الذي عقد في هافانا عام ١٩٩٠, حث الدول الأعضاء للكشف عن جهودها المتعلقة بمكافحة الجرائم المعلوماتية والعمل على مضاعفة أنشطتها على الصعيد الدولي فيما يتعلق بتبادل المعلومات في المسائل المرتبطة بالجرائم الإلكترونية, كما أكد المؤتمر على ضرورة توافق وتطابق قوانين الدول الأعضاء فيما بينها في المسائل الجنائية المتعلقة بهذا النوع من الجرائم[١], ويمكن لهذه المقررات التي جاء بها مؤتمر الأمم المتحدة ان تساعد على فتح آفات جديدة للتعاون الدولي منها[٢]:

١- وضع معايير دولية لأمن المعالجة الآلية للبيانات.

٢- وضع معايير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم الإلكترونية العابرة للحدود.

٣- ابرام اتفاقيات دولية تنطوي على نصوص تنظم اجراءات التفتيش والضبط المباشر الواقع عبر الحدود الدولية على الأنظمة الإلكترونية المتصلة فيما بينها.

ثانيًا- نقل الإجراءات: يراد بنقل الإجراءات قيام دولة ما بمقتضى اتفاقية معينة باتخاذ إجراءات جنائية لجريمة ارتكبت في اقليم دولة أخرى ولمصلحة هذه الدولة وذلك متى ما توافرت شروط معينة من أهمها[٣]:

١- ان يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات.

٢- ان تكون هناك شرعية في الإجراءات التي يتم اتخاذها أي بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن الجريمة نفسها.

٣- ان تكون الإجراءات التي يتم اتخاذها تؤدي دورًا مهمًا في الوصول إلى الحقيقة كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها.

وقد أشارت العديد من الاتفاقيات الاقليمية والدولية إلى نقل الإجراءات كصورة من صور المساعدة القضائية الدولية, منها اتفاقية الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية[١], وكذلك المادة (٢١) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[٢].ومن أبرز الامثلة على ما تقدم في عام ١٩٩٥, قام مجرم من الأرجنتين بالدخول بصورة غير مشروعة إلى شبكة الحاسوب في مركز آمرية الرقابة البحرية للاستطلاع المحيطي في سانيتاغو بكاليفورنيا, حيث قام بتعديل بعض الملفات وإزالة أسماء وكلمات السر الشخصية للمستخدمين وقدرت الخسائر المادية لهذا الفعل في شبكة ناسا (NASA) بأكثر من مائة ألف دولار[٣]. ونتيجة لهذا الفعل الخطير تعاونت عدة جهات لمتابعة المجرم وتم الحصول على أمر قضائي من المحكمة المختصة يسمح بالدخول والتنصت على الاتصالات الإلكترونية التي امكن من خلالها تحديد هوية المجرم بنجاح من بين (١٦٥٠٠) حساب من حسابات المستخدمين وكشفت بعدها التحريات بان المجرم هو شاب من الأرجنتين يبلغ عمره (٢١) عامًا, واستنادًا إلى المعلومات التي قدمت إلى السلطات الأرجنتينية قامت الأخيرة بتنفيذ مذكرة تفتيش وضبط مقر إقامة المتهم وضبطت معدات حاسبه الشخصي بمساعدة المنظمة الدولية للشرطة الجنائية (Interpol) وبموجبها صدرت مذكرة جنائية من الحكومة الأمريكية تتهمه بانتهاك القوانين ذات الصلة بالحاسوب, وقد اعترف المتهم بذلك وحكم عليه بالوضع تحت المراقبة لمدة (٣) سنوات وغرامة مقدارها (٥٠٠) دولار[٤], ويلاحظ من خلال هذه القضية جهود التعاون الدولي في مكافحة جرائم الإرهاب الإلكتروني وتقديم الدعم والاسناد في سبيل الوصول إلى مرتكب الجريمة.

ثالثًا- الإنابة القضائية الدولية: يراد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها[٥]. وبذلك تسهل الإنابة القضائية الدولية الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل اقاليم الدول الأخرى مثال ذلك إجراء التفتيش والضبط والمعاينة. **وهنا يثار التساؤل:** هل تساهم الاتفاقيات الدولية بوضعها الحالي في الحد من جرائم الإرهاب الإلكتروني؟ للإجابة على هذا التساؤل يمكن القول ان مواجهة جرائم الإرهاب الإلكتروني بصورة خاصة يتطلب تعاون دولي حقيقي وفعال من أجل تحقيق نتائج إيجابية أفضل في هذا المجال خاصةً وان شبكة المعلومات الدولية (الإنترنت) ذات تطور تكنولوجي رهيب وانتشارها بشكل واسع على المستوى الدولي, لذا لابد من تعديل الاتفاقيات الدولية المتعلقة بجرائم الإرهاب الإلكتروني كونها انشئت في وقت لا يتناسب مع التطور الكبير في تكنولوجيا المعلومات. كذلك ضرورة تفعيل المرتكزات الأساسية للتعاون الدولي للحد من جرائم الإرهاب الإلكتروني التي تتمثل في الآتي:

١- إعادة تفعيل التعاون الدولي في مجال مكافحة جرائم الإرهاب بصورة عامة وجرائم الإرهاب الإلكتروني بصورة خاصة, من خلال ابرام الاتفاقيات الثنائية أو الجماعية أو إجراء التعديل على الاتفاقيات الحالية بصدد ملائمتها مع التطور التكنولوجي الحديث, وان تسمح بإمكانية تبادل المعلومات بين الدول بصورة سريعة ودقيقة, كذلك لابد من تدعيم فكرة التعاون القانوني والقضائي الدولي وتجاوز فكرة عدم قابلية الحكم الأجنبي للتنفيذ بحجة ان الحكم الجنائي هو مظهر لسيادة الدولة وحقها في توقيع العقاب.

٢- الاتفاق على ذاتية محددة للإرهاب من خلال وضع آلة إعلامية دولية صادقة ومحايدة لمعالجة القضايا الشائكة التي تمثل عقبة رئيسية في التفرقة بين أعمال الإرهاب الإلكتروني, وبين الحفاظ على الحقوق والحريات التي تعتبر من الأعمال المشروعة وصولاً إلى اتفاق قانوني لمواجهة مثل هذه الأشكال.

٣- العمل على تعديل التشريعات الداخلية للدول وجعلها متسقة ومتطابقة مع أحكام الاتفاقيات الدولية خاصةً فيما يتعلق بجرائم الإرهاب الإلكتروني.

الخاتمة

تعد الحماية الدستورية والقانونية والأمنية من أهم الدعائم الأساسية في مواجهة جرائم الإرهاب الإلكتروني, لذا لابد للدول التي تواجه موجات عاتية للإرهاب الإلكتروني ان تسارع في تشريع قوانين متخصصة واتخاذ تدابير استثنائية لمواجهة تلك الظاهرة التي تروع الآمنين وتنشر حالة الرعب والفزع بين الأفراد. فمن خلال سلطات إنفاذ القوانين المتمثلة بأجهزة الشرطة يمكن تقييم مدى ملاءمة القوانين للتوفيق في تحقيق المصلحة العامة لمواجهة جرائم الإرهاب الإلكتروني والحفاظ على أمن وسلامة الأفراد, وهنا فإن جهاز الشرطة يعد الحكم الفصل بين قوة القانون ومدى أثره في مكافحة هذه الجرائم الخطرة, كما فرضت فكرة التعاون الدولي نفسها بين أجهزة الشرطة بسبب تطور وسائل الاتصال التي تمكن المجرمين من الإفلات وارتكاب جرائم عابرة للحدود الدولية, وهنا كانت المنظمة الدولية للشرطة الجنائية (الإنتربول) وثيقة الصلة بين الدول لمكافحة الجرائم, وعقدها العديد من المؤتمرات لمناقشة ظاهرة الإرهاب الإلكتروني.وفي إطار البحث في دراسة المواجهة القانونية والأمنية في جرائم الإرهاب الإلكتروني خلصنا إلى النتائج الآتية:

١- جرائم الإرهاب الإلكتروني تعني الهجمات غير المشروعة أو التهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزونة الكترونيًا التي توجه من أجل الانتقام أو التأثير على الحكومات والشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية.

٢- الآليات التي تستخدمها الجماعات الإرهابية لتحقيق جرائم الإرهاب الإلكتروني تتمثل باستخدام شبكات الإنترنت, وكذلك استخدام الدعاية كوسيلة لتحقيق الهجمات الإرهابية.

٣- اتضح لنا ان التحديات التي تواجهها أجهزة الشرطة في مواجهة جرائم الإرهاب الإلكتروني تزداد وتتعاظم عند اتساع اعتماد المجتمعات على تقنية أنظمة المعلومات سواء في نطاق الدولة الواحدة أو في النطاق الاقليمي والدولي, وكذلك تزداد التحديات عند ضآلة أو انعدام البيئة التشريعية اللازمة لمكافحة جرائم الإرهاب الإلكتروني.

٤- اتضح لنا ان جهاز الشرطة في بعض الاحيان يستمر في اعتماده على الوسائل البدائية لمواجهة الجريمة التي تتطور بشكل سريع يومًا بعد يوم, ويرجع ذلك لعدم قناعة العديد من قيادات أجهزة الشرطة بالوسائل العلمية من الناحية التطبيقية, والتي قد تتأخر نتائجها قليلاً إلا أنها تقوم بتصحيح النظام الإداري وتقويته بما يسمح بمواجهة جميع الجرائم بصفة عامة, وجريمة الإرهاب الإلكتروني بصفة خاصة, أو افتقار جهاز الشرطة إلى نظام إداري يربط بين الأبحاث والدراسات الخاصة بتطوير المهام الشرطوية من جهة, وبين تطبيق ذلك من الناحية العملية من جهة أخرى, أو لعدم وجود قانون أو نظام إداري قوي بالدولة ينظم عملية التنسيق بين أجهزة الدولة المعنية بمواجهة جرائم الإرهاب الإلكتروني, وبين الوزارات والمؤسسات التعليمية.

٥- تتميز جرائم الإرهاب الإلكتروني بذاتية خاصة من الناحية القانونية نظرًا لجسامتها وهذا ما ينعكس بشكل خاص في تجريم أي عمل يساعد على وقوع الإرهاب الذي تقوم به الجماعات الإجرامية كتمويل الاعمال الإرهابية على سبيل المثال ورغم الخطورة الحقيقية لجرائم الإرهاب الإلكتروني إلا ان جهاز الشرطة يبقى الصمام للحد من هذه الجرائم الخطيرة.

٦- اتضح لنا بان هناك بعض الدول مثل الولايات المتحدة الامريكية قامت بتشريع قوانين متخصصة واتخاذ تدابير استثنائية لمواجهة جرائم الإرهاب الإلكتروني, بينما خلت تشريعات دول أخرى مثل العراق ومصر من تشريع وطني يسمح بمواجهة جرائم الإرهاب الإلكتروني, وكذلك

خلت من المساعدات القانونية والقضائية المتبادلة, كما يلاحظ ان التدابير المتخذة من قبل هذه الدول غير ملائمة وغير فعالة لمواجهة مثل هذه الجرائم الخطرة, مما يتيح فرص أفضل للعناصر الإرهابية لتحقيق أهدافهم غير المشروعة.

٧- اتضح لنا ان الجهود التي بذلتها المنظمة الدولية للشرطة الجنائية (الإنتربول) غير مجدية في مكافحة جرائم الإرهاب الإلكتروني خصوصًا ان ازدياد ظاهرة الإجرام الإلكتروني بات يشكل تهديدًا خطيرًا على المجتمع الدولي, وان محترفي الجرائم اصبحوا يستفادون من التطور التكنولوجي لتنفيذ عملياتهم الإجرامية, فاذا ما اكتفت منظمة الإنتربول بما لديها من وسائل وأساليب لمكافحة الجريمة فأنها تكون خلال فترة وجيزة بعيدة كل البعد عن اداء دورها في مواجهة مثل هذه الجرائم الخطرة.

٨- يلاحظ بان هناك تفاوت كبير بين الدول في مواجهة جرائم الإرهاب الإلكتروني فبعض الدول المتقدمة تكنولوجيًا لها صيت كبير في مواجهة جرائم الإرهاب الإلكتروني, والبعض الآخر من الدول تفتقد ذلك ومن هنا لابد من تفعيل التعاون الدولي من خلال ابرام اتفاقيات ثنائية أو جماعية أو اجراء تعديل على الاتفاقيات الحالية ذات الصلة بصدد ملاءمتها مع التطور التكنولوجي الحديث لكي تسمح بإمكانية تبادل المعلومات بين الدول بصورة سريعة ودقيقة, وكذلك لابد من تدعيم فكرة التعاون القانوني والقضائي الدولي في ذلك.

كما خلصنا في ضوء البحث في دراسة "المواجهة القانونية والأمنية لجرائم الإرهاب الإلكتروني" إلى بعض التوصيات المتواضعة لعلها **تكون ذات منفعة وفائدة لمكافحة هذه الظاهرة أو الحد من آثارها وهي:**

١- نقترح اعتماد الأجهزة الأمنية على الوسائل العلمية في أعمال البحث والتحري والاعتماد على الدراسات الميدانية والبحوث المتخصصة في رصد جرائم الإرهاب الإلكتروني, وذلك في سبيل تطوير أساليب عملهم في مواجهة هذه الجرائم الخطرة.

٢- نقترح التنسيق والتكامل بين القوانين الجنائية الوطنية والاتفاقيات الدولية, لأن جرائم الإرهاب الإلكتروني خاصةً تتطلب تطور تشريعي في العديد من القوانين الوطنية لضبط المجرمين والقضاء على تلك الظاهرة أو الحد منها.

٣- تنمية القدرات العقلية والذهنية لرجل الشرطة وذلك من خلال اختيار الاساليب العلمية والتدريبية المناسبة, وكذلك إحاطة رجل الشرطة بالقوانين المعمول بها في مواجهة جرائم الإرهاب الإلكتروني بصفة دورية وما يستجد منها, وذلك له الأثر الأكبر في إحكام الإجراءات القانونية اللازمة وهي الوسيلة التي تؤدي إلى تحديد وقياس فعالية برامج الإعداد المهاري لرجل الشرطة, ومدى قدرتها وملاءمتها الحقيقية لرفع كفاءته في مواجهة جرائم الإرهاب الإلكتروني.

٤- دعم الأجهزة الأمنية المسؤولة عن مكافحة جرائم الإرهاب بصورة عامة, وعن جرائم الإرهاب الإلكتروني بصورة خاصة, وذلك بإنشاء أجهزة مخصصة لمواجهة الجريمة داخل أجهزتها الأمنية سواء كانت تلك الأجهزة مستقلة بذاتها أم كانت تابعة لجهاز الشرطة بصورة عامة.

المصادر

أولاً- القوانين:

١- قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥.

٢- قانون جهاز مكافحة الإرهاب العراقي رقم (٣١) لسنة ٢٠١٦.

٢- قانون مكافحة الإرهاب المصري لسنة ٢٠١٥.

ثانيًا- الكتب:

١- د. أحمد أبو الحسن زرد, قوانين مكافحة الإرهاب- تطبيق لالتزام دولي, القاهرة: الروينو للنشر, بدون ذكر سنة النشر.

٢- د. أحمد فتحي سرور, حكم القانون في مواجهة الإرهاب, بيروت: الدار الجامعية, ٢٠٠٥.

٣- القاضي جلال محمد الزغبي, القاضي أسامة أحمد المناعسة, جرائم تقنية نظم المعلومات الإلكترونية, الطبعة الأولى, عمان: دار الثقافة

٤- أمير فرج يوسف, جريمة مكافحة الإرهاب الإلكتروني, الطبعة الأولى, الإسكندرية: دار الكتب والدراسات العربية, ٢٠١٥.

٥- جميل عبد الباقي الصغير, الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, القاهرة: دار النهضة العربية للنشر,١٩٩٩.

٦- د. حسن طاهر داوود, جرائم نظم المعلومات, الطبعة الأولى, الرياض: مطبعة جامعة نايف العربية للعلوم الأمنية, ٢٠٠٠.

٧- د. عادل مشموسي, مكافحة الإرهاب, الطبعة الأولى, بيروت: منشورات زين الحقوقية, ٢٠١١.

٨- د. علي حسن الشرفي, الارهاب والقرصنة البحرية, الطبعة الأولى, الرياض: جامعة نايف العربية للعلوم الأمنية, ٢٠٠٦.

٩- الإرهاب والقرصنة البحرية, منشورات جامعة نايف العربية للعلوم الأمنية, الطبعة الأولى, ٢٠٠٦.

١٠- د. محمد الفاضل, التعاون الدولي في مكافحة الإجرام, دمشق: منشورات جامعة حلب, ١٩٩٢.

ثالثًا- المقالات والدوريات:

١- حوراء رشيد يوسف, الإرهاب الإلكتروني وطرق مواجهته, مقال منشور في مركز الفرات, ٢٠١٧.

٢- روني حداد, الإرهاب الإلكتروني وتحديات مواجهته, مجلة الأمن السيبراني, العدد ٣٩٤, ٢٠١٨.

٣- استخدام الإنترنت في أغراض إرهابية, منشورات منظمة الأمم المتحدة, ٢٠١٣.

٤- د. هشام محمد فريد رستم, الجرائم المعلوماتية وأصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي, بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت من (١-٣) مايو سنة ٢٠٠٠.

رابعًا- الكتب الانكليزية:

1- Edward C. Liu, Government Collection of Private Information: Background and Issues Related to the USA Patriot Act Reauthorization in Brief, May 19-2015.

2- Malcolm Anderson, Policing the World- Interpol the Politics of International Police Co, Operation- Clarendon Press- Oxford, 1989.

خامسًا- المواقع على الشبكة الدولية (الإنترنت):

١- حازم سعيد, دور الإنتربول في مكافحة الإرهاب اقليميًا ودوليًا, ٢٠١٨, مقال منشور على الشبكة الدولية (الإنترنت) على الرابط التالي: https//www.europarabct.com

٢- رياض هاني بهار, دور الإنتربول بالتصدي للجريمة المنظمة, ٢٠١٢, مقال منشور على الشبكة الدولية (الإنترنت) على الرابط التالي: http://www.m.ahewar.or/

٣- مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين الذي عقد في هافانا سنة ١٩٩٠, ص٣, منشورات الأمم المتحدة على الرابط التالي: www.un.org

الهوامش

(١) في بحث لوزارة الدفاع الأمريكية أمكن تحديد العديد من القطاعات المعتمدة على انظمة تقنيات المعلومات والتي يمكن ان تكون هدفًا للعمليات الإرهابية الإلكترونية منها أنظمة المياه والكهرباء وأنظمة اتصالات الطوارئ باستخدام برامج خاصة قد تتوافر بأيدي الإرهابيين, كما لوحظ ان الاهتمام الأمريكي بظاهرة الإرهاب الإلكتروني بدأ مبكرًا, حيث أسس الرئيس الأمريكي "بيل كلنتون" ابان فترة رئاسته لجنة خاصة للحماية من جرائم الإرهاب الإلكتروني, مهمتها تحديد القطاعات المستهدفة مثل قطاع الماء, والغاز, والكهرباء, وشبكات الحاسوب الآلي, ومن خلال ذلك تم انشاء مراكز في كل ولاية للتعامل الفعال لاحتمالية استهداف هذه المنشآت من أية أفعال إجرامية. راجع في ذلك الموقع الإلكتروني على الشبكة الدولية الإنترنت على الرابط التالي: www.mipc.gov

(٢) تم اعتماد اتفاقية "بودابست" لمكافحة الجريمة الإلكترونية من قبل لجنة وزراء مجلس أوروبا في دورتها المائة وتسعة, حيث فتح التوقيع عليها في ٢٣ تشرين الثاني ٢٠٠١ بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية, وقد تضمنت الاتفاقية أربعة فصول الفصل الأول: استخدام المصطلحات, والفصل الثاني: التدابير الواجب اتخاذها على الصعيد المحلي- القانون الموضوعي والقانون الإجرائي, والفصل الثالث: التعاون الدولي أما الفصل الرابع: تضمن الأحكام الختامية. راجع في ذلك الموقع الإلكتروني على الشبكة الدولية الإنترنت على الرابط التالي: https//ar.wikipedia.org

(٣) أمير فرج يوسف, جريمة مكافحة الإرهاب الإلكتروني, الطبعة الأولى, القاهرة: دار الكتب والدراسات العربية, ٢٠١٥, ص١٢٧.

(١) الإرهاب والقرصنة البحرية, منشورات جامعة نايف العربية للعلوم الأمنية, الطبعة الأولى, ٢٠٠٦, ص٢٣٤

(٢) منشورات منظمة الأمم المتحدة, استخدام الإنترنت في أغراض إرهابية, ٢٠١٣, ص٤.

(٣) روني حداد, الإرهاب الإلكتروني وتحديات مواجهته, مجلة الأمن السيبراني, العدد ٣٩٤, ٢٠١٨, ص٢.

(١) روني حداد, الإرهاب الإلكتروني وتحديات مواجهته, مرجع سابق, ص٣.

(*) يقصد بالجدار الناري: هو نظام يوفر حماية للشبكة عبر ترشيح البيانات المرسلة والمستقبلة عبر الشبكة, بناءً على قواعد يحددها المستخدم, وان الهدف من الجدار الناري هو تقليل أو إزالة وجود الاتصالات الشبكية غير المرغوب فيها والسماح في الوقت نفسه للاتصالات المشروعة ان تنقل بحرية, حيث يوفر الجدار الناري طبقة أساسية من الحماية تمنع المهاجمين من الوصول إلى خوادم الحاسوب بطرق خبيثة. راجع في ذلك الموقع الإلكتروني على الشبكة الدولية الإنترنت على الرابط التالي: www.academy.hsoub.com

(٢) د. علي حسن الشرفي, الارهاب والقرصنة البحرية, الطبعة الأولى, الرياض: جامعة نايف العربية للعلوم الأمنية, ٢٠٠٦, ص ٢٣٨.

(١) أمير فرج يوسف, جريمة مكافحة الإرهاب الإلكتروني, مرجع سابق, ص١٣٦.

(٢) حوراء رشيد يوسف, الإرهاب الإلكتروني وطرق مواجهته, مقال منشور في مركز الفرات, ٢٠١٧, ص٢.

(١) د. عادل مشموسي, مكافحة الإرهاب, الطبعة الأولى, بيروت: منشورات زين الحقوقية, ٢٠١١, ص١٧٢.

(٢) أمير فرج يوسف, جريمة مكافحة الإرهاب الإلكتروني, مرجع سابق, ص١٦٢-١٦٣.

(٣) المرجع السابق, ص١٦٤.

(١) القاضي جلال محمد الزغبي, القاضي أسامة أحمد المناعسة, جرائم تقنية نظم المعلومات الإلكترونية, الطبعة الأولى, عمان: دار الثقافة للنشر, ٢٠١٠, ص١٧٧-٢٧٨.

(٢) د. عادل مشموسي, مكافحة الإرهاب, مرجع سابق, ص١٧١.

(١) راجع: المادة (١) من قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥.

(٢) راجع: المادة (٤) من قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥.

(1) Edward C. Liu, Government Collection of Private Information: Background and Issues Related to the USA Patriot Act Reauthorization in Brief, May 19-2015, P.3.

(*) يقصد بـ "FBI" اختصارًا لـ "Federal Bureau of Investigation" وهي وكالة حكومية تابعة لوزارة العدل الأمريكية وتعمل كوكالة استخبارات داخلية وقوة لتطبيق القانون في الدولة.

(٢) د. أحمد أبو الحسن زرد, قوانين مكافحة الإرهاب- تطبيق لالتزام دولي, القاهرة: الروينو للنشر, بدون ذكر سنة النشر, ص٨١.

(٣) راجع: المادة (٢٩) من قانون مكافحة الإرهاب المصري لسنة ٢٠١٥.

(١) يقصد بالإنتربول هي المنظمة الدولية للشرطة الجنائية "International Criminal Police Organization" التي تعد أكبر منظمة شرطة دولية أنشئت عام ١٩٢٣ وتتكون من قوات الشرطة لـ (٩٠) دولة, مقرها الرئيسي في مدينة ليون بفرنسا, ومن أبرز مهامها وصلاحياتها هي:

- منع الجريمة ومكافحتها من خلال تعزيز التعاون والابتكار في المجالين الشرطي والأمني.
- تبادل المساعدة على أوسع نطاق ممكن بين جميع سلطات إنفاذ القوانين الجنائية.
- ضمان قدرة أجهزة الشرطة على التواصل في ما بينها بشكل مأمون في العالم أجمع.
- إتاحة إمكانية الاطلاع على البيانات والمعلومات الشرطوية من جميع أنحاء العالم.
- تقديم الدعم العملي في مجالات إجرام محددة ذات أولوية.
- تطوير المعارف والمهارات اللازمة لعمل أجهزة الشرطة على الصعيد الدولي بشكل فعال.

(١) د. أحمد فتحي سرور, حكم القانون في مواجهة الإرهاب, بيروت: الدار الجامعية, ٢٠٠٥, ص١١١.

(٢) د. حسن طاهر داوود, جرائم نظم المعلومات, الطبعة الأولى, الرياض: مطبعة جامعة نايف العربية للعلوم الأمنية, ٢٠٠٠, ص١١٠.

(١) أمير فرج يوسف, جريمة مكافحة الإرهاب الإلكتروني, مرجع سابق, ص٢٦٠.

(٢) حازم سعيد, دور الإنتربول في مكافحة الإرهاب اقليميًا ودوليًا, ٢٠١٨, مقال منشور على الشبكة الدولية (الإنترنت) على الرابط التالي: https//www.europarabct.com

(٣) المرجع السابق.

(١) رياض هاني بهار, دور الإنتربول بالتصدي للجريمة المنظمة, ٢٠١٢, مقال منشور على الشبكة الدولية (الإنترنت) على الرابط التالي:

http://www.m.ahewar.org/

(١) يقصد بـ "يوروبول: هي شرطة أوروبية أنشئت لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة إليها.

(١) يقصد "بالمساعدة القضائية المتبادلة": كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم, راجع في ذلك أمير فرج يوسف, جريمة مكافحة الإرهاب الإلكتروني مرجع سابق, ص٢٦١.

(٢) د. محمد الفاضل, التعاون الدولي في مكافحة الإجرام, دمشق: منشورات جامعة حلب, ١٩٩٢, ص٣٥٢.

(١) راجع: مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين الذي عقد في هافانا سنة ١٩٩٠, ص٣, على الرابط التالي:

www.un.org

(٢) د. هشام محمد فريد رستم, الجرائم المعلوماتية وأصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي, بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت من (١-٣) مايو سنة ٢٠٠٠, ص٤٩.

(٣) أمير فرح يوسف, جريمة مكافحة الإرهاب الإلكتروني, مرجع سابق, ص٢٦٢-٢٦٣.

(١) اعتمدت هذه الاتفاقية بموجب قرار الجمعية العامة للأمم المتحدة رقم (٤٥/١١٨) في ١٤ كانون الأول سنة ١٩٩٠.

(٢) اعتمدت هذه الاتفاقية في الدورة الخامسة والعشرون للجمعية العامة للأمم المتحدة في ١٥ تشرين الثاني سنة ٢٠٠٠ وجاء في المادة (٢١) منها على ان "تنظر الدول الأطراف في إمكانية ان تنقل إحداها إلى الأخرى إجراءات الملاحقة المتعلقة بجرم مشمول بهذه الاتفاقية في الحالات التي يعتبر فيها ذلك النقل في صالح سلامة وإقامة العدل وخصوصًا عندما يتعلق الأمر بعدة ولايات قضائية بهدف تركيز الملاحقة".

(3) Malcolm Anderson, Policing the World- Interpol the Politics of International Police Co, Operation- Clarendon Press- Oxford, 1989, P.98.

(4) Ibid, P.99.

(٥) جميل عبد الباقي الصغير, الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, القاهرة: دار النهضة العربية للنشر,١٩٩٩, ص٨٣.