Journal Of the Iraqia University (74-8) December(2025)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

الاجراءات التنظيمية للحد من استمرار جرائم الارهاب الالكترونية

رفل صباح نوري الخيقاني
المشرف الأستاذ الدكتور أ.د محمد فرحات

Regulatory Measures to Limit the Continuation of Cyberterrorism Crimes

RAFAL SABAH NOORI
Supervisor: Professor. Mohamed Farhat
mohammad.farhat@iul.edu.lb
rafel.s.nouri@aliraqia.edu.iq

المستخلص:

تُعنى هذه الدراسة بالبحث في الإجراءات التنظيمية الشاملة للحد من استمرار جرائم الإرهاب الإلكتروني، من خلال تحليل التشريعات والأطر المؤسسية الحالية وتقييم مدى فعاليتها. ويهدف البحث إلى كشف الثغرات في الأنظمة الوقائية، والتحديات الناتجة عن الطبيعة العابرة للحدود لهذه الجرائم. وبناءً على ذلك، يقدم البحث مجموعة من التوصيات المتكاملة، تشمل تطوير الأطر القانونية المتخصصة، وتعزيز البنى التقنية للكشف المبكر، وترسيخ التعاون الدولي بين الجهات المعنية. ويخلص إلى أن مواجهة هذا التهديد تتطلب استراتيجية ديناميكية تجمع بين التقنية والتشريع والتعاون، لضمان أمن الفضاء الإلكتروني دون المساس بالحريات الأساسية.الكلمات المفتاحية: الإجراءات التنظيمية، الجرائم، الإرهاب، الالكتروني.

Abstract:

This study investigates comprehensive regulatory measures to mitigate the persistence of cyberterrorism crimes. It does so by analyzing current legislation and institutional frameworks and evaluating their effectiveness. The research aims to uncover gaps in preventive systems and the challenges arising from the cross-border nature of these crimes. Consequently, it presents a set of integrated recommendations, including developing specialized legal frameworks, enhancing technical infrastructures for early detection, and solidifying international cooperation among relevant authorities. It concludes that confronting this threat requires a dynamic strategy that combines technology, legislation, and cooperation to ensure the security of cyberspace without infringing upon fundamental freedoms.Keywords: Regulatory measures, Crimes, Terrorism, Cyber.

المقدمة

يشهد العالم المعاصر طفرة رقمية غير مسبوقة، تداخلت فيها التكنولوجيا مع مختلف مجالات الحياة السياسية والاقتصادية والاجتماعية، الأمر الذي أدى إلى انفتاح الفضاء الرقمي على احتمالات واسعة من الاستخدامات المشروعة وغير المشروعة. وفي ظل هذا التوسع التقني المتسارع، برزت جرائم الإرهاب الإلكتروني بوصفها أحد أخطر التحديات التي تهدد الأمن الوطني والدولي، لما تمتاز به من قدرة على التخفي، وسرعة الانتشار، وضعف الحدود الجغرافية التي يمكن أن تعيق تنفيذها. إن هذا الواقع المستجد فرض على الدول جملة من المتطلبات التشريعية والتنظيمية لضبط هذا النوع من الجرائم، وحماية المجتمعات من آثارها المدمرة.

أولاً: أهمية البحث:

تنبع أهمية دراسة الإجراءات التنظيمية للحد من استمرار جرائم الإرهاب الإلكتروني من كونها تمثل خط الدفاع الأول لحماية الأمن السيبراني للدولة، وترسيخ الاستقرار الاجتماعي، وضمان سلامة البنى التحتية المعلوماتية الحساسة، كالمصارف والمؤسسات الحكومية وشبكات الطاقة والاتصالات. كما أن هذه الدراسة تكتسب أهميتها من الازدياد المطرد في معدل ارتكاب هذه الجرائم، واتساع نطاق الجهات التي تستخدم الفضاء

الأزرق منصة لتنفيذ أعمال إرهابية، سواء كانت جماعات منظمة أو أفراداً يمتلكون مهارات تقنية عالية. ومن هنا تتأكد الحاجة إلى منظومة تشريعية وتنظيمية فعّالة، قادرة على التنبؤ بالتهديدات والتصدي لها.

ثانياً: إشكالية البحث:

على الرغم من تبني العديد من الدول سياسات وقوانين لمواجهة الإرهاب الإلكتروني، إلا أن التطور المتسارع في وسائل التقنية، وتعقيد وسائل الاتصال الرقمي، جعلا الجهود التنظيمية القائمة غير كافية في كثير من الأحيان لملاحقة هذا النوع من الجرائم أو الحد من استمرارها. كما أن الطبيعة العابرة للحدود لهذه الجرائم تُضعف من قدرة التشريعات الوطنية وحدها على مواجهتها، ما يفرض الحاجة إلى إطار تنظيمي أكثر تماسكاً وتكاملاً. ومن هنا يظهر التساؤل الرئيسي الاتي: **إلى أي مدى أسهمت الإجراءات التنظيمية، سواء الوطنية أو الدولية، في الحد من استمرار جرائم الإرهاب الإلكتروني، وما مدى كفاءتها في مواكبة التطورات التقنية المتسارعة؟**

ثالثاً: منهجية البحث

لاستجلاء أبعاد هذا الموضوع، يعتمد البحث على المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية والتنظيمية الوطنية والدولية ذات الصلة، واستعراض التجارب المقارنة في مواجهة الإرهاب الإلكتروني. كما يُستخدم المنهج الاستقرائي في تتبع مظاهر انتشار هذه الجرائم وأسباب استمراريتها، بالإضافة إلى المنهج النقدي لتقييم فعالية الإجراءات التنظيمية الحالية، واقتراح رؤى تطويرية تسهم في رفع كفاءة منظومة المواجهة والحد من تكرار الجرائم الإلكترونية ذات الطابع الإرهابي.

رابعاً: هيكلية البحث:

سوف نقوم بالاعتماد على التقسيم الثنائي من خلال الاتي: **المطلب الأول: تعريف الارهاب الالكتروني وأركانه** الفرع الأول: تعريف الإرهاب الالكتروني الفرع الثاني: أركان جريمة الإرهاب الالكتروني **المطلب الثاني: الوسائل الحديثة في مكافحة الارهاب الالكتروني** الفرع الأول: التنصت والمراقبة الالكترونية الفرع الثاني: أنظمة الحماية الفنية

المطلب الأول تعريف الارهاب الالكتروني وأركانه

يُعد الإرهاب الإلكتروني أحد أبرز التهديدات الأمنية المعاصرة التي فرضتها ثورة التقنية والاتصالات، حيث تجاوز المفهوم التقليدي للإرهاب ليشمل الفضاء الرقمي كبيئة جديدة للتنفيذ والتأثير. ويتحدد تعريفه كنشاط إجرامي منظم يستهدف استخدام الأنظمة والحواسيب والشبكات الرقمية لإلحاق الضرر بالدول أو المجتمعات، أو نشر الذعر، أو تحقيق أهداف أيديولوجية وسياسية. ولا يقوم هذا النوع من الجرائم إلا بتوافر أركانه الأساسية التي تشمل الركن المادي المتمثل في الفعل الإلكتروني الضار (كالاختراق أو تعطيل الخدمات)، والركن المعنوي الذي يقصد به نية الترويع أو الإضرار بالصالح العام، بالإضافة إلى الركن الدولي أو العابر للحدود الذي يعكس طبيعة الفضاء الإلكتروني غير المحدود جغرافياً. ويظهر فهم هذه الأركان ضرورياً لوضع التشريعات والاستراتيجيات الفعالة لمواجهة هذه الظاهرة الخطيرة.ومن أجل بيان أوضح لمصطلح الإرهاب الالكتروني وتعريفه سنقوم بتقسيم هذا المطلب الى فرعين في الأول سنبين تعريف الإرهاب الالكتروني وفي الفرع الثاني سندرس أركان الإرهاب الإلكتروني.**الفرع الأول تعريف الإرهاب الالكتروني** تُعرّف ظاهرة الإرهاب الإلكتروني على أنها الشكل المعاصر للإرهاب الذي يستثمر منصات وتقنيات العصر الرقمي في تحقيق أهدافه. وتتميز هذه الظاهرة بقدرتها على استغلال الفضاء الإلكتروني لبث الرعب وتقويض الأمن الوطني وزعزعة استقرار المجتمعات. وتُعد هذه الجرائم من أبرز التحديات الأمنية الحديثة التي فرضها التطور التكنولوجي المتسارع، مما يستدعي تحليلها من خلال استعراض أبرز التعريفات الأكاديمية والمهنية التي وضعت لإطارتها وتحديد سماتها الأساسية[١]يعرف الارهاب الالكتروني بأنه «اجتماع عدة أشخاص واستعمالهم لكل وسائل العصر الرقمي الحديث والمتمثل بتقنيات المعلومات والاتصالات لتحقيق أغراض محدودة [٢]، كما يعرف بأنه: «ذلك النوع من الإرهاب الحديث الذي يعتمد بصورة كلية على استعمال كل الوسائل والإمكانيات العلمية والتقنية لشبكات الإنترنت وشبكات الاتصالات المعلوماتية» [٣] في سبيل إدخال الخوف والرعب وإلحاق الضرر بالأفراد أو الجماعات المدنية أو المؤسسات الحكومية [٤].يُوضح الجدول الزمني للاستجابة الدولية للإرهاب أن المجتمع الدولي قد بدأ، منذ عام ١٩٦٣، في صياغة أطر قانونية جماعية لمواجهة هذه الظاهرة، حيث تم إقرار تسعة عشر صكاً قانونياً دولياً تحت مظلة الأمم المتحدة والوكالة الدولية للطاقة الذرية، وهي صكوك مفتوحة لانضمام جميع الدول. وفي سياق التطور الدائم لهذه الأطر، قدمت الأمم المتحدة في أكتوبر ٢٠١٢ تعريفاً مركزاً للإرهاب الرقمي باعتباره "استخدام الإنترنت في نشر الأعمال الإرهابية".ولم يكن هذا التعريف الإطاري الوحيد، فقد تقدمت جهات أخرى بتعريفات أكثر تفصيلاً وتقنية. على سبيل المثال، قدمت اللجنة الدولية للصليب الأحمر تعريفاً يركز على الآلية الفنية، حيث عرفت الإرهاب الرقمي بأنه العمليات التي تُنفذ ضد أو عبر أنظمة الحاسوب باستخدام

تيارات البيانات، بهدف اختراق الأنظمة المعلوماتية، أو جمع البيانات ونقلها وتشفيرها أو التلاعب بها، لاستخدامها النهائي في تعطيل أو تدمير أهداف مادية ملموسة مثل المنشآت الصناعية والبنى التحتية الحيوية [٥]في المقابل، توجد رؤية تحليلية أوسع تضع الإرهاب الرقمي في إطار استراتيجي، فتعرفه على أنه نشاط هجومي مقصود بدوافع سياسية، يستهدف التأثير على الرأي العام أو القرارات الحكومية. ويعتمد في ذلك على الفضاء الإلكتروني كوسيط لتنفيذ عمليات عسكرية أو إرهابية، سواء من خلال الهجمات المباشرة على البنية التحتية المعلوماتية، أو عبر الحرب النفسية والمعنوية ونشر خطاب الكراهية، أو باستخدام أسلحة إلكترونية متطورة قد يقتصر تأثيرها على العالم الرقمي أو يمتد ليشمل إلحاق أضرار مادية بالبنى التحتية الحساسة[٦].فضلاً عن ذلك، فقد اطلقت على الإرهاب الإلكتروني مسميات عديدة منها (الإرهاب التقني) الذي يعرف بأنه: «العدوان أو التخويف أو التهديد المادي أو المعنوي باستخدام الوسائل الإلكترونية والصادر من دول أو جماعات أو أفراد على الإنسان، كما سمى (الإرهاب المعلوماتي) والمستخدم في وسائل الاتصالات الحديثة والإنترنت لنشر المعلومات والأفكار التي تتنافى مع القيم والمبادئ التي يرتكز عليها المجتمع الدولي» [٧].ويُعرَّف بأنه إرهاب ناتج عن التطور التكنولوجي وثورة المعلومات من خلال استغلال الإنترنت للهدم والتخريب، وكذلك العدوان أو الترهيب أو التهديد، المادي أو المعنوي، من خلال استخدام الوسائل الإلكترونية الموجهة ضد الدول أو الجماعات أو الأفراد وبشكل عام موجه ضد شخص في دينه أو نفسه أو عرضه أو ماله مع أنواع مختلفة من صور الضرر والفساد على الأرض.وكذلك على أنه استعمال الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية لتخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم.لذلك يعد تبادل المعلومات ونشرها من خلال شبكة الإنترنت من أبرز أشكال الإرهاب الإلكتروني. وخاصة الأشكال الأخرى كانتشار المواقع الإرهابية وتدمير المواقع والنظم المعلوماتية والتجسس الإلكتروني [٨]وقد تعددت جرائم الإرهاب الإلكتروني وذلك بفضل شبكة الإنترنت في تشكيلها ونقل أفكارها وخبراتها بين المنظمات الإرهابية والجماعات والأفراد الذين يشكلونها كما تنوعت بزيادة دور الحركات الإرهابية وجعل اعتمادها الأساس على شبكة المعلومات (الإنترنت) بوصفها وسيلة رئيسية لنشر دعايتها وأفكارها ومبادئها لذلك يعد الإرهاب الإلكتروني من أهم وأحدث أشكال الإرهاب الذي يتمثل باستخدام الموارد المعلوماتية المتمثلة في شبكات المعلومات وأجهزة الكومبيوتر وشبكة الإنترنت، كما يعد من أهم ما يميزه حدوثه عبر شبكة الإنترنت وارتباطه بالمستوى المتقدم الذي تؤديه تكنولوجيا المعلومات في جميع نواحي الحياة في العالم. وهذا ما يشكل محور التمييز بين الإرهاب التقليدي والإرهاب الإلكتروني، إذ إن الأفعال واحدة إلا أن الوسيلة مختلفة.

الفرع الثاني أركان جريمة الإرهاب الالكتروني تتخذ جريمة الإرهاب الإلكتروني من الفضاء الافتراضي مسرحاً لها، مما يجعلها تتميز بسمات تنفرد بها، فضلاً عن أن ذلك لا يعني عدم وجود تشابه لها مع الجرائم التقليدية أو المادية، فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل، ومن خلال هذا التشابه سوف يتمّ التطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة.

١-**الركن القانوني:**إن الركن القانوني للجريمة هو وجود نص يصور الفعل وينص على عقوبته وقت ارتكاب هذا الفعل [٩]، فمبدأ الشرعية الجنائية يمنع المسئولية الجنائية ما لم يتوفر النص القانوني فلا جريمة ولا عقوبة إلا لنص واحد، وعندما يكون النص الخاص بتجريم مثل هذه الأفعال لا تغطي النصوص الموجودة النصوص الموجودة، تم الامتناع عن المسؤولية وتحقق أوجه قصور في مكافحة مثل هذه الجرائم[١٠]، غير أن السؤال المطروح هو مدى تطبيق مبدأ الشرعية على الجرائم التي ترتكب عبر الإنترنت؟

١ – **مدى انطباق النصوص القائمة على الجرائم الإلكترونية**.إن تعقيد المشكلات الناجمة عن استخدام أجهزة الكمبيوتر وشبكاتها جعل من الصعب القضاء عليها بسبب عدم وجود نصوص قادرة على معالجة هذه المشكلات، بما في ذلك الاستخدام غير القانوني للإنترنت. [١١].لا يتطور القانون الجنائي دائمًا بنفس السرعة التي تتطور بها التكنولوجيا، ولا بنفس المهارة التي يضعها العقل البشري في الاستفادة من هذه الابتكارات لسوء الاستخدام، لذلك، وكاستنتاج أولي ومنطقي، يُعتقد بأن القانون الجزائي لا يكفي من ناحية المبدأ في مواجهة هذا النمط من الإجرام خصوصاً أن النصوص قد وضعت للتطبيق وفق معايير معينة كانت سائدة أيام وضعها.

٢ – **الحاجة إلى تدخل المشرّع لمواجهة الجرائم الإلكترونية**.تُعد الجريمة الإلكترونية، ومن ضمنها الإرهاب الرقمي، نتاجاً حتمياً للتطور التكنولوجي المتسارع، مما شكل تحدياً كبيراً للنصوص الجنائية التقليدية التي لم تُصمم أساساً لمجاراة هذا النوع من الابتكار الإجرامي. وأدركت غالبية دول العالم، ولا سيما تلك المتقدمة في مجال البناء التشريعي، هذه الفجوة القانونية، فسارعت إلى وضع تشريعات متخصصة لمواجهة هذه الجرائم المستحدثة[١٢].وتعد الولايات المتحدة الأمريكية من الدول الرائدة في هذا المضمار، حيث أصدرت قانوناً خاصاً بحماية الحاسوب والشبكات المحوسبة في عام ١٩٧٦. وتبع ذلك تحديد معهد العدالة القومي الأمريكي في عام ١٩٨٥ لأبرز خمسة أنماط لهذه الجرائم، وهي: الجرائم الداخلية للحاسوب، والاستخدام غير المشروع لشبكات المعلومات عن بُعد، والتلاعب غير المصرح به في الشبكات المحوسبة، ودعم الأنشطة الإجرامية

عبر هذه النظم، إضافة إلى سرقة المكونات البرمجية والمادية. وفي عام ١٩٨٦، صدر قانون أكثر تطوراً لتعريف المصطلحات وتحديد إطار قانوني شامل لجريمة نظم المعلومات، مما عزز الدور المحلي للولايات المتحدة في مكافحة هذه الظاهرة من خلال تشريعات وطنية متناسقة مع الأطر الاتحادية[١٣].على الصعيد الدولي، يبرز تفاوت صارخ في القدرات والتشريعات بين الدول، مما يُعرف بالفجوة الرقمية. ففي حين تقدمت دول في سن قوانين متخصصة، لا تزال دول أخرى، خاصة تلك التي تعاني من تأخر تقني ومعلوماتي، تعتمد على تطبيق نصوص قانون العقوبات التقليدي على الجرائم الإلكترونية. وقد أثبتت هذه النصوص قصوراً واضحاً في التطبيق الفعال، مما يدفع نحو ضرورة إما تبني تشريعات جديدة أو اللجوء إلى التفسير الموسع للنصوص القائمة لمحاولة سد هذا الفراغ التشريعي الخطير.

ثانياً: الركن المادي.إن تحديد الركن المادي للجرائم المرتكبة عبر الإنترنت يطرح سلسلة من الصعوبات التي تفرضها طبيعة الوسيلة التي ارتكبت فيها الجريمة، وهي الجانب التقني، وهذا ما يميز ركنها المادي، الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للإنترنت، ومن هنا تبدأ التساؤلات التي تتعلق ببداية النشاط التقني أو الشروع فيه، مكان بداية العنصر المادي ونهايته، وأجزاء السلوك الإجرامي المرتكب في العالم المادي أو في العالم الافتراضي، وغيرها من الأسئلة المتعلقة بطبيعة الجريمة[١٤].يتطلب النشاط أو السلوك المادي في الجريمة الإلكترونية وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضًا معرفة ببدء هذا النشاط والشروع فيه ونتيجته؛ على سبيل المثال، يقوم مرتكب الجريمة بتجهيز الكمبيوتر للتحقيق في وقوع الجريمة، فيقوم بتنزيل برامج القرصنة، أو يعد هذه البرامج بنفسه، كما قد يحتاج إلى إنشاء صفحات تحتوي على أشياء أو صور مخلة بالآداب العامة وتحميلها على الجهاز المضيف، ويمكن أيضا مع جريمة إعداد برامج الفيروسات[١٥] تمهيداً لبثها.

المطلب الثاني الوسائل الحديثة في مكافحة الارهاب الالكتروني

تتميز الجرائم المعلوماتية بطابعها العالمي العابر للحدود، مما يجعلها ظاهرة لا تعترف بالحدود الجغرافية أو الإطارات القانونية المحلية الضيقة. وقد فرضت هذه الطبيعة نفسها على المجتمع الدولي، حيث أصبح التعاون والتنسيق المشترك بين الدول ضرورة ملحة لمواجهة هذا التحدي المتشعب.ولقد تعقدت هذه المواجهة بشكل كبير مع تطور بنية هذه الجرائم، حيث انتقلت من أعمال فردية أو مجموعات غير منظمة إلى عمليات منفذة من قبل كيانات إجرامية منظمة عابرة للقوميات. وغالباً ما تتشكل هذه الشبكات الإجرامية ليس على أساس روابط تقليدية كالعرق أو الدين أو الجغرافيا، بل تتحد حول هدف مشترك، سواء كان تحقيق مكاسب مادية ضخمة أو إلحاق ضرر استراتيجي.لذلك، فإن المواجهة الفعالة تتطلب تبني استراتيجيات متكاملة تعتمد على وسائل متطورة تتناسب مع الطبيعة الفريدة والمتطورة لهذه الجرائم. يجب أن تركز هذه الاستراتيجيات على تدابير وقائية واستباقية تهدف إلى منع وقوع الجرائم من الأساس، مع ضمان أن تكون هذه الآليات مرنة وقادرة على التكيف مع الأشكال المستجدة للتهديدات السيبرانية[١٦].**في ضوء ذلك سنقوم بتقسيم هذا المطلب الى فرعين رئيسيين، نتناول في الفرع الأول التنصت والمراقبة الإلكترونية، فيما نستعرض في الفرع الثاني أنظمة الحماية الفنية.الفرع الأول التنصت والمراقبة الالكترونية** تُمثل المراقبة في العمل الشرطي نشاطاً منظماً يعتمد على الرصد المتعمد والمستمر لتحركات فرد معين، أو ما يجري في موقع محدد، أو متابعة اتصال هاتفي. وتهدف إلى وضع الشخص محل الاهتمام تحت الملاحظة المباشرة لأفراد الشرطة لتسجيل أي أفعال غير قانونية قد تصدر عنه، أو تتعلق بممتلكات أو مواقع معينة، والتي من شأنها الإضرار بالأمن العام أو النظام الاجتماعي، أو تحويل تهديد محتمل إلى ضرر فعلي بطريقة خفية وسرية، دون إثارة شكوك المراقَب. ويشترط في القائمين على هذه المهمة الحيادية وعدم التسرع في الأحكام، والتحلي بالصبر والدقة في التوثيق، بهدف تجميع المعلومات أو التحقق من البيانات الاستخباراتية الموجودة[١٧]أما المراقبة الإلكترونية عبر الإنترنت، فهي عملية تقنية يقوم بها مختص باستخدام أدوات تكنولوجيا المعلومات للتحري وجمع البيانات عن مشتبه به (سواء كان شخصاً أو مكاناً أو شيئاً مرتبطاً بزمن معين) لتحقيق غاية أمنية أو غيرها. وفي هذا الإطار، تُعد المراقبة الإلكترونية أداة لجمع الاستخبارات ينفذها ضباط مختصون في مكافحة الجريمة الإلكترونية، مستخدمين تقنيات متقدمة مثل برنامج كارنيفور، الذي لعب دوراً حاسماً – خاصة بعد أحداث ١١ سبتمبر – في تعقب المجرمين والتحقيق في قضايا تهدد الأمن القومي. ويستخدم مكتب التحقيقات الفيدرالي وهذا البرنامج لفحص وتتبع رسائل البريد الإلكتروني المشبوهة في قضايا الجرائم الإلكترونية[١٨].غير أن تطبيق المراقبة الإلكترونية يثير تساؤلاً جوهرياً حول الحدود الفاصلة والمشتركة بين مراقبة شبكات الحاسوب (مثل تصفح الإنترنت والمراسلات) ومراقبة المحادثات الهاتفية وتسجيلها. فكلتاهما تتضمنان التطفل على اتصالات خاصة، مما يفتح نقاشاً مستمراً حول التوازن بين متطلبات الأمن الوطني وضرورة حماية الخصوصية الفردية وحرمة الحياة الخاصة، وهي معادلة قانونية وأخلاقية معقدة في العصر الرقمي[١٩].يوضح الإطار القانوني الحالي أن سلطة القاضي الجزائي فيما يتعلق بمراقبة المكالمات الهاتفية تنحصر في صلاحية منح الإذن أو رفضه، دون أن يمتد اختصاصه إلى تنفيذ الإجراء بنفسه أو إدارة عملية المراقبة مباشرة. إذ أن تنفيذ المراقبة يقع ضمن صلاحية النيابة العامة التي يمكنها إجراؤها بنفسها أو بتكليف أحد

معاونيها، ولا يحق للقاضي تعيين منفذ محدد. أما إذا كان قاضي التحقيق هو المختص بالدعوى، فإنه يتمتع بسلطة الأمر بالمراقبة الهاتفية مباشرة.وفي كل الأحوال، يشترط على كل من قاضي التحقيق والنيابة العامة ألا يلجأوا إلى هذا الإجراء إلا إذا كان ضرورياً لكشف الحقيقة في جناية أو جنحة يعاقب عليها بالحبس مدة تزيد على ثلاثة أشهر. ويجب أن يصدر الأمر مسبباً، وأن لا تتجاوز مدته الأولية ثلاثين يوماً، قابلة للتجديد لمدد مماثلة، مع اختصاص القاضي الجزائي بتجديد الأمر إذا كانت المراقبة قد بدأت بناءً على طلب النيابة العامة[٢٠]من الناحية التقنية، تجدر الإشارة إلى أن اتصالات شبكات الحاسوب غالباً ما تستخدم خطوط الهاتفنفسها، وذلك عبر جهاز المودم الذي يحول الإشارات الرقمية من الحاسوب إلى موجات تناظرية قابلة للنقل عبر الخطوط الهاتفية المصممة أصلاً للأصوات. ويتطلب هذا عملية تعديل في محطة الإرسال (لتحويل الرقمي إلى تناظري) وتعديل عكسي في محطة الاستقبال (لتحويل التناظري مرة أخرى إلى إشارات رقمية يفهمها الحاسوب). [٢١]وبناءً على هذا التحليل، يتضح وجود أرضية تقنية وقانونية مشتركة بين مراقبة المكالمات الهاتفية التقليدية والمراقبة الإلكترونية لاتصالات الحاسوب. لذلك، ومن وجهة نظرنا، يمكن التعامل قانوناً مع المراقبة الإلكترونية بالاستناد إلى الأحكام والقواعد المنظمة للمراقبة الهاتفية الواردة في قانون العقوبات والإجراءات الجنائية. ومع ذلك، يجب التأكيد على أن النصوص الإجرائية الحالية الخاصة بمراقبة وتسجيل المحادثات الهاتفية لا تكفي وحدها لمواكبة التعقيد المستجد في مراقبة شبكات الحاسوب، مما يستلزم إدخال تعديلات وتحديثات محددة عليها لضمان فعاليتها وشرعيتها في مواجهة هذا النوع من الجرائم.[٢٢].وينبغي ألا يفوتنا أن نوضح سماح الكثير من الدول بهذا الإجراء المراقبة الإليكترونية ولكن في ظروف معينة، ففي فرنسا يجيز قانون ١٠ تموز ١٩٩١، اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات، وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتصنت على شبكات اتصالات الحاسب، إن كانت هناك جرائم خطيرة ارتكبها.شهدت الولايات المتحدة وغيرها من الدول الغربية اهتماماً متزايداً بتنظيم التعامل مع الجرائم المعلوماتية، حيث برز ذلك في عدد من الأحكام القضائية التي شددت على ضرورة احترام الخصوصية الرقمية. فقد اعتبرت المحاكم الأميركية أن التقنيات المستخدمة من بعض الأجهزة الأمنية – ومنها ما يتعلق بالتنصت على البريد الإلكتروني – تُعد تدخلاً في الحياة الخاصة للأفراد، مما يوجب إخضاعها لرقابة قضائية صارمة ومنع استخدامها بلا ضوابط.ولم تقتصر النقاشات المتعلقة بالمراقبة الإلكترونية على الغرب، إذ أثارت عدة أحداث في دول أخرى جدلاً واسعاً حول حدود الرقابة الحكومية. فقد شهدت الصين موجة انتقادات عندما طالبت الشركات المصنعة للحواسيب بإدراج برامج إلزامية لحجب المحتوى غير المرغوب، الأمر الذي عُدّ نوعاً من التقييد الإجباري لحرية الاستخدام. كما لفتت التجربة الإيرانية خلال الانتخابات الرئاسية الأنظار، بعدما اعتمد المستخدمون على الإنترنت لنقل الأخبار التي حاولت السلطات الحد من تداولها، يقابله تشديد حكومي على مراقبة المنصات الرقمية، مما أثار مخاوف من توسع الرقابة غير القضائية على الفضاء الإلكتروني وتداعياتها على خصوصية الأفراد[٢٣].وفي السياق ذاته، أصبحت أنظمة المراقبة البصرية جزءاً أساسياً من البنية الأمنية في المؤسسات المالية والمصرفية. فالكاميرات توزّع في محيط المصرف وفي أروقته الداخلية وعلى أجهزة الصراف الآلي بهدف توفير تغطية شاملة. وتعمل بعض الدول المتقدمة على ربط هذه الأنظمة مباشرة بمراكز الشرطة لتمكينها من متابعة أي طارئ في الوقت الحقيقي، بما يسهّل التعامل السريع مع الجرائم المحتملة ويوفر معلومات دقيقة حول أدوات المجرمين وأساليبهم، الأمر الذي يعزز من قدرة الأجهزة الأمنية على الاستجابة الفعالة.وتطور الأمر ليشمل اعتماد برامج تقنية متقدمة تساعد على توقع شكل الأشخاص عبر تحليل صور قديمة لهم، حيث تستطيع تلك البرامج توليد صورة تقريبية لمشتبه به وفقاً للعمر المفترض أو التغييرات المتوقعة في ملامحه. وتستفيد جهات التحقيق من هذه الأدوات في إعداد صور أولية يمكن تعميمها للمساعدة في عمليات البحث والتعقب[٢٤]

الفرع الثاني أنظمة الحماية الفنية في ظل التنامي المستمر للجرائم الحديثة وتطور أساليب الجناة، أصبح من الضروري أن تعمل أجهزة الشرطة والأمن بوتيرة أعلى من الجهوزية والتأهب، وأن تبقى منتشرة في مختلف المناطق لمواجهة أي نشاط إجرامي محتمل. فالتعقيد الذي بات يميز أنماط الجرائم، لاسيما المرتبطة بالتقنيات الرقمية، يفرض على فرق التحقيق امتلاك الوسائل الفنية اللازمة التي تساعدهم في كشف الجرائم وتتبع مرتكبيها والحد من قدرتهم على الإفلات.وبين يدي أجهزة الأمن مجموعة من الأدوات التقنية المتقدمة التي جرى تطويرها لمواجهة التحديات الناجمة عن الإرهاب المعلوماتي والجريمة الإلكترونية. ومن أبرزها ما يأتي[٢٥]:

أولاً: تقنيات تشفير البيانات يقوم مبدأ التشفير على تحويل النصوص أو البيانات إلى رموز معقدة لا يمكن قراءتها إلا بواسطة حامل مفتاح التشفير. وتستخدم شركات تقنية عالمية – ومنها شركات كندية متخصصة – بطاقات إلكترونية تحوي المعلومات السرية والتواقيع الرقمية داخلها بدلاً من الاحتفاظ بها في ذاكرة الجهاز، بهدف تقليل فرص الاختراق. ومع ذلك، يبقى نجاح التشفير مرهوناً بمدى حماية مفاتيح الشفرة، إذ إن ضياعها أو كشفها يعطل الفائدة المرجوة منه على المدى البعيد.

ثانياً: كلمات المرور وحماية الدخول تعد كلمة المرور إحدى أكثر وسائل الحماية شيوعاً، وهي عبارة عن مجموعة من الأرقام أو الرموز التي تتيح الولوج إلى النظام. ويرى خبراء الأمن السيبراني أن فعاليتها تعتمد على شروط عدة، أهمها تغييرها بشكل دوري، وتجنب استخدام كلمات يسهل تخمينها مثل تاريخ الميلاد أو أرقام السيارات، بالإضافة إلى عدم إعادة استعمال كلمات السر الملغاة.ورغم ذلك، فإن هذه الوسيلة ليست حصينة بالكامل؛ فبرامج الاختراق قادرة على تجربة آلاف الاحتمالات خلال ثوانٍ عبر ما يعرف بهجمات "القوة الغاشمة"، كما يمكن للمهاجم مراقبة المستخدم أثناء إدخال كلمة المرور أو تصوير لوحة المفاتيح خلسة، فضلاً عن أن كثيراً من المستخدمين يفضلون كلمات سهلة التذكر مما يسهل على المخترقين الوصول إليها.

ثالثاً: الأنظمة الحيوية (البيومترية) تعتمد هذه التقنيات على الخصائص الجسدية الفريدة لكل شخص، مثل بصمة الأصابع، أو بصمة العين، أو نبرات الصوت، أو شكل الأذن، أو طريقة التوقيع. وتستخدم هذه الخصائص للسماح بالدخول إلى الأجهزة أو الأنظمة الحساسة بحيث يصبح من المستحيل تقريباً لشخص آخر أن ينتحل هوية المستخدم.غير أن الأنظمة الحيوية ليست مثالية؛ فالتغيّر الطبيعي في الأعضاء بسبب المرض أو الإصابة قد يؤدي إلى فشل التعرف على المستخدم الحقيقي، كما أن الأجهزة البيومترية مرتفعة التكلفة نسبياً، وتحتاج إلى صيانة دورية، وقد تسجل أخطاء تقنية تمنع صاحب البيانات نفسه من الدخول إلى نظامه.

رابعاً: تقنيات التشويش والحجب تستخدم بعض المؤسسات وسائل إلكترونية متخصصة لإرباك محاولات التجسس، عبر تحويل البيانات المتداولة إلى إشارات غير مفهومة لا يمكن إعادة قراءتها إلا عبر شفرة معينة. ورغم فعالية هذه الوسيلة من حيث الحد من اعتراض المعلومات، فإن تقنيات فك التشويش تطورت هي الأخرى، وظهرت برامج قادرة على تجاوز كثير من أنظمة الحجب التقليدية، مما يجعل هذه الوسائل بحاجة دائمة للتحديث والتطوير المستمر[٢٦].بالإضافة إلى حماية النظام المتكامل للمعلومات، حيث أن هذه الحماية تقتضي مراعاة اعتبارات معينة لوضع خطة تأمين النظام المتكامل للمعلومات، ولتحقيق هذا التأمين يتطلب ما يلي:

أ_ تأمين الجهاز الإلكتروني: وذلك عن طريق وضع كلمات المرور للوصول إلى البيانات المخزنة على وسائل التخزين الموجودة في الجهاز والمتصلة به، واستخدام الأساليب العلمية في وضعها مثل استخدام أساليب بحوث العمليات وسلاسل ماركوف، كما يتعين تغييرها كل فترة زمنية ان يحصر وضعها في شخص او عدد من الاشخاص بعينهم، وفي حالة وجود شبكة للاتصال بين الحاسبات يجب أن يكون لكل نهاية طرفية متصلة بالجهاز مستخدم خاص بها مختلف عن النهاية الطرفية الأخرى لكي يحدد من خلاله البيانات المسموح وصولها إلى النهاية الطرفية واسترجاعها[٢٧].

ب_ تأمين التشغيل: ويتطلب ذلك تأمين الوثائق الخاصة بالنظام وتدريب الكوادر على التشغيل السليم للنظام وعدم ترك آية مخلفات أو وثائق تدل على كيفية التشغيل أو الوصول الى البيانات أو التخلص من المخلفات أولاً بأول، واعداد بطاقات شخصية للعاملين بنظام المعلومات تختلف عن بطاقات بقية العاملين بالجهة.

ج_ تأمين الموقع: وفيه يتم وضع خطة تأمين للمبنى بالكامل والخاص بأجهزة الجهاز الالكتروني ونظم الاتصالات، وأن يكون العاملين في مجال الجهاز الالكتروني بمعزل عن آية عاملين آخرين، وأن يكون لهم مناطق محددة لاستقبال الزائرين وان يعطى لكل عامل منهم كروت ممغنطة ببصمة اليد أو الصوت يستطيع من خلالها الدخول إلى اماكن تخزين البيانات والمعلومات أي اماكن وجود الأجهزة الإلكترونية.

نضف إلى ذلك حماية المعلومات الحساسة التي يعتقد أن المجرمين يسعون الحصول عليها، أو الدخول غير الشرعي لقواعد المعلومات ضمن الموقع، ويتم ذلك بتغيير كلمة المرور بشكل متكرر، أو مراقبة الدخول الى الموقع وتسجيل وقت الدخول والجهة الداخلية وعنوانها، أو تعقيد الدخول باستخدام التوقيع الالكتروني، أو بصمة الابهام أو البصمة الصوتية أو بصمة العين[٢٨].

د_ تأمين نظم المعلومات: هذا يتطلب تأمين المعدات الخاصة بالاتصالات وخصوصاً خطوط الاتصال لمنع الدخول عليها وسرقة البيانات والمعلومات أثناء نقلها للأجهزة الأخرى.

إلى جانب حماية الشبكات التقنية ودرء مخاطر البرمجيات الخبيثة، فإن التعامل مع الجريمة الإلكترونية يقتضي اعتماد منظومة متكاملة من التدابير التنظيمية والأمنية والقانونية والتعاون الدولي، بما يعزز القدرة على الحد من تنامي هذا النوع من الجرائم داخلياً وخارجياً. ويمكن إبراز أهم الإجراءات وفقاً لما يأتي[٢٩]:

أولاً: الإجراءات الإدارية والأمنية

١-نشر الوعي المجتمعي

يُعد التعليم والتثقيف الدعامة الأولى لأي سياسة فعّالة في مواجهة الجرائم الإلكترونية. فتنظيم حملات إعلامية وتوعوية عبر وسائل الإعلام المختلفة يتيح للمواطن إدراك خطورة إساءة استخدام الوسائل الرقمية، ويعرّفه بالأساليب الوقائية التي تمنع وقوعه ضحية للجرائم الإلكترونية، كما يشجع على التعاون مع الجهات المختصة عند الاشتباه بأي نشاط غير قانوني(٣٠).

ثانياً: دعم الدراسات والبحوث المتخصصة إن تشجيع البحوث العلمية التي تدرس طبيعة الجريمة الإلكترونية وآلياتها وأساليب ارتكابها يُعد خطوة أساسية لتطوير سياسات وقائية فعّالة. فالدراسات المتعلقة بجرائم مثل غسل الأموال الإلكتروني، أو تحليل أنماط الهجمات، تتيح بناء قاعدة معرفية حقيقية يمكن من خلالها صياغة برامج وقائية دقيقة تستجيب للمتغيرات التقنية المتسارعة.

ثالثاً: تطوير وسائل الحد من آثار الجريمة يتطلب التصدي للمخاطر الرقمية البحث الدائم عن أدوات يمكنها إحباط الجرائم أو إرباك مرتكبيها وتقليل آثارها لأدنى مستوى ممكن. ويتحقق ذلك من خلال تعزيز أنظمة الرقابة الداخلية، وتحسين الإجراءات الإدارية، ووضع خطط دقيقة للمراقبة تشمل الموظفين وأنظمة المعلومات، إلى جانب تطوير مهارات الكوادر عبر برامج تدريب حديثة في مجالات الأمن السيبراني والتحقيق الرقمي.

رابعاً: مكافحة الفساد المرتبط بالفضاء الإلكتروني تتطلب خطورة الجرائم التي يمكن أن تُرتكب من داخل المؤسسات نفسها — كتسريب المعلومات الحساسة أو العبث بالنظم المالية أو الإلكترونية — تعزيز منظومات مكافحة الفساد. فملاحقة الموظفين الذين يستغلون مناصبهم لتسهيل الجرائم الإلكترونية أمر ضروري، خاصةً في الحالات التي تتعلق بالأسرار التجارية والصناعية والعسكرية أو بنقل الأموال إلكترونياً بطرق غير قانونية.

خامساً: تعزيز قدرات أجهزة الشرطة والعدالة الجنائيةيتطلب التصدي للجرائم الإلكترونية امتلاك مؤسسات إنفاذ القانون منظومات متخصصة قادرة على فهم طبيعة هذه الجرائم وتعقب مرتكبيها. ومن ثمّ، فإن تطوير وحدات الشرطة والنيابات والأجهزة القضائية المختصة، وتوفير الوسائل التقنية الحديثة لها، يُعد خطوة أساسية لتحقيق فاعلية أكبر في التحقيق وضبط الجناة. كما أن التنسيق بين مختلف مؤسسات العدالة – سواء كانت شرطية أو قضائية أو تقنية – يساعد على تجنب العمل المتشتت ويضمن تكاملاً مؤسسياً يسهم في تقليص فرص انتشار هذا النوع من الجرائم.

سادساً: الارتقاء بالتدريب وتطوير الكفاءاتيُعد بناء القدرات البشرية أحد أهم مرتكزات مواجهة الجريمة الإلكترونية. ويتحقق ذلك من خلال تحديث البرامج التدريبية ورفع المستوى المهني للعاملين في أجهزة إنفاذ القانون، بهدف تمكينهم من التعامل مع الأدوات الرقمية الحديثة وامتلاك مهارات التحقيق الإلكتروني. كما يستحسن اعتماد برامج تدريب مشتركة على المستويين الإقليمي والدولي لضمان تبادل الخبرات، ومتابعة أحدث التطورات التقنية وأساليب العمل الناجحة في الدول الأخرى، وبذلك تصبح أنظمة العدالة الجنائية أكثر قدرة على مواجهة التحديات المتغيرة وتتسم بمرونة وعدالة أوسع(٣١).

سابعاً: مكافحة مصادر التمويل غير المشروع ومواءمة التشريعات عد الاتجار بالمخدرات أحد أخطر مصادر الدخل غير المشروع، إذ تولّد هذه التجارة أموالاً طائلة تُستغل لاحقاً في تنفيذ أنشطة إجرامية تعتمد على الوسائل الإلكترونية، سواء عبر إخفاء العائدات أو غسلها أو تحويلها خارج نطاق الرقابة باستخدام الأنظمة الرقمية والمصرفية. ومن هنا تأتي ضرورة دعم الجهود الرامية إلى تقويض شبكات إنتاج المخدرات وتوزيعها، لما يشكله ذلك من خطوة أساسية في الحد من قدرة الجريمة المنظمة على استخدام التكنولوجيا لتوسيع نشاطها.وفي السياق نفسه، تصبح الحاجة ملحة لتشجيع المشرعين العرب على التعامل مع الجرائم المستحدثة المرتبطة بالفضاء الإلكتروني، كتجريم فتح الحسابات الوهمية، وأساليب غسل الأموال الرقمية، والمعاملات المالية التي تُجرى تحت أسماء مزيفة. كما يقتضي الأمر تعديل التشريعات المدنية والمالية والتنظيمية لتستجيب لطبيعة المخاطر الجديدة، إلى جانب تعزيز تبادل المعلومات التشريعية بين الدول العربية عبر الأمانة العامة لمجلس وزراء الداخلية العرب، بما يساهم في بناء قاعدة تشريعية مشتركة تواجه الجرائم الإلكترونية وما يرتبط بها من جرائم اقتصادية ومنظمة. وتعد إجراءات مصادرة عائدات الجريمة أحد أبرز التطورات الحديثة في هذا المجال.ومن التدابير التي يمكن أن تعتمدها الدول كذلك: تجميد أو مصادرة الأصول التي استُخدمت في ارتكاب الجرائم الإلكترونية أو التي نشأت عنها، أو فرض جزاءات مالية تتناسب مع الأرباح المحققة من النشاط الإجرامي. كما قد تتطلب بعض الحالات تنسيقاً ثنائياً يتعلق بكيفية التصرف في الأموال المصادرة بناءً على طلب متبادل بين الدول(٣٢).

الخاتمة

بعد استعراض وتحليل الإجراءات التنظيمية الوطنية والدولية المتعلقة بالحد من استمرار جرائم الإرهاب الإلكتروني، يتبين أن هذا النوع من الجرائم يشكل تحدياً حقيقياً للمنظومات القانونية والأمنية على مستوى العالم، نظراً لسرعة تطور أدواته، وطبيعته المعقدة، واتصاله الوثيق بالفضاء السيبراني المفتوح الذي لا يعترف بالحدود الجغرافية. وقد حاولت الدول سنّ تشريعات وإقامة هياكل مؤسسية للتصدي لهذه الظاهرة، إلا أن الفجوة بين التطور التقني وبين الإجراءات التنظيمية ما تزال قائمة بمستويات متفاوتة، وهو ما يجعل تقويم التجارب التنظيمية ضرورة علمية وعملية.

وفي نهاية هذا البحث فقد قمنا بالتوصل الى مجموعة من النتائج والمقترحات والتي سوف نستعرضها على الشكل الاتي:

أولاً: النتائج:

١-إن الإجراءات التنظيمية الحالية، على الرغم من أهميتها، ما تزال غير *كافية* لمواكبة التطور المتسارع في وسائل ارتكاب جرائم الإرهاب الإلكتروني، الأمر الذي يؤدي إلى بقاء هذه الجرائم في حالة تطور مستمر يفوق قدرة التشريعات التقليدية على الاحتواء والمكافحة.

٢-إن نجاح مواجهة الإرهاب الإلكتروني لا يتحقق فقط من خلال التشريعات، بل يتطلب **تكاملاً** بين الجهود القانونية والتقنية والأمنية والإعلامية، إضافة إلى التعاون الدولي، إذ لا يمكن لأي دولة منفردة وضع حد لجرائم عابرة للحدود بطبيعتها.

ثانياً: المقترحات:

١-ضرورة تحديث التشريعات الوطنية بشكل دوري، من خلال إدراج نصوص قانونية مرنة تستجيب للتطورات التقنية الجديدة، وإنشاء وحدات متخصصة داخل المؤسسات الأمنية والقضائية للتعامل مع هذا النوع من الجرائم، مع تعزيز القدرات الفنية للعاملين فيها.

٢-تعزيز التعاون الدولي عبر تبادل المعلومات والخبرات، وإبرام اتفاقيات ثنائية ومتعددة الأطراف لملاحقة مرتكبي جرائم الإرهاب الإلكتروني، وتطوير منصات مشتركة لرصد التهديدات السيبرانية بشكل استباقي، بما يحدّ من فرص استمرار الجرائم قبل وقوعها.

قائمة المصادر والمراجع

First: Books

1.Ahmed Saad Mohamed Al-Husseini, Procedural Aspects of Crimes Arising from the Use of Electronic Networks, New University House, Alexandria, 2019.

2.Ayman Abdel Hafez, Technical and Security Trends in Confronting Cybercrimes, No publisher, No place of publication, 2005.

3.Jameel Abdul-Baqi Al-Saghir, The Internet and Criminal Law, Al-Nahda Al-Arabiya Publishing House, Cairo, 2012.

4.Khaled Aboul Fotouh, Computer Virus, the Malady of Modern Technology, 1st ed., Al-Kotob Al-Ilmiyah for Publishing and Distribution, Cairo, 1990.

5.Saeed Abdul Latif Hassan, Proving Computer Crimes and Crimes Committed via the Internet, Al-Nahda Al-Arabiya Publishing House, Cairo, 2004.

6.Adel Abdel Sadeq, Cyberterrorism, Power in International Relations: A New Pattern and Different Challenges, Al-Ahram Center for Political and Strategic Studies, Cairo, 2009.

7.Mohamed El-Nobi Mohamed Ali, Internet Addiction in the Age of Globalization, Safaa Publishing House, Amman, 2009.

8.Mohamed Obeid Al-Kaabi, Crimes Arising from the Unlawful Use of the Internet Network, Al-Nahda Al-Arabiya Publishing House, Cairo, No publication year.

9.Mohamed Mamdouh Badir, Combating Cybercrime through Internet Networks and Digital Forensics as a Means of Proving Crimes Committed via the Internet, A Comparative Study, 1st ed., Center for Arab Studies Publishing and Distribution, Cairo, 2019.

10.Mostafa Mohamed Moussa, Cyberterrorism, 1st ed., Egyptian National Library and Archives, Cairo, 2009.

11.Mostafa Mohamed Moussa, Electronic Surveillance via the Internet Network - A Comparative Study between Traditional and Electronic Security Surveillance, Book Five - First Edition, Egyptian National Library and Archives, Cairo, 2003.

12.Mounir Al-Genbehi and Mamdouh Al-Genbehi, Electronic Information Security, University Thought Publishing House, Alexandria, 2006.

13.Nasr Shouman, Modern Criminal Technology and its Importance in Criminal Evidence, First Edition, The Modern Book Institution, Beirut, 2011.

14.Hoda Hamed Kashkosh, Electronic Computer Crimes in Comparative Legislation, Al-Nahda Al-Arabiya Publishing House, Cairo, 2003.

15.Hesham Mohamed Farid Rostom, Procedural Aspects of Cybercrimes, 1st ed., Al-Nahda Al-Arabiya Publishing House, Cairo, 2007.

16.Hilali Abdullah Ahmed, Searching Computer Systems and the Guarantees of the Cyber Defendant, Al-Nasr Al-Thahabi Printing Press, Cairo, 1997.

17.Younis Arab, "A Reading of the Legislative Trends for Cybercrimes with a Statement of the Position of Arab Countries and the Experience of the Sultanate of Oman", Workshop on Developing Legislation in the Field of Combating Cybercrimes held in Muscat, Sultanate of Oman, 2-4 April, 2006.

Second: Journal Articles and Papers

1.Terrorism and Cybercrimes", Research published in Informatics Journal, Issue 80, issued by the Arab Center for Information, Beirut, 2010.

2.Jameel Abdul-Baqi Al-Saghir, "The Internet and Terrorism", Research published in the Special Issue of Journal of Legal and Political Sciences, University of Diyala, Baghdad, 2012.

3.Adel Abdel Sadeq, "Does Terrorism Represent a New Form of International Conflict?", Article published in Al-Ahram Newspaper, Issue 156, issued by Al-Ahram Center for Political and Strategic Studies, Cairo, 2007.

4.Abdul-Jabbar Al-Huneis, "The Unlawful Use of Computer Systems from the Perspective of Criminal Law – A Comparative Study", Damascus University Journal for Economic and Legal Sciences, Volume 27, Issue 1, Damascus, 2011.

5.Abdul-Mohsen Badawi Mohamed Ahmed, "Strategies and Theories for Addressing Crime and Deviance Issues in Mass Media", Scientific Symposium on Media and Security, Center for Studies and Research, Department of Seminars and Scientific Meetings, Naif Arab University for Security Sciences, Khartoum, 11-13, 2005.

6.Ammar Abbas Al-Husseini, Procedural Problems in the Field of Cybercrime, Paper presented to the Conference on Information Security and Cryptography, University of Al-Najaf Al-Ashraf, Baghdad, 2008.

Third: Theses and Dissertations

1.Ahmed bin Mohammed Al-Yamani, Criminal Protection of Email: A Comparative Foundational Study, Thesis submitted in partial fulfillment of the requirements for the degree of Master in the Department of Criminal Justice, specialization in Criminal Policy, Naif Arab University for Security Sciences, College of Graduate Studies, Department of Criminal Justice, Riyadh, 2010.

2.Mansour bin Saleh Al-Sulami, Civil Liability for Violation of Privacy in the Saudi Anti-Cybercrime Law, Thesis submitted in partial fulfillment of the requirements for the degree of Master in Criminal Justice, Naif Arab University for Security Sciences, College of Graduate Studies, Department of Criminal Justice, Riyadh, 2010.

هوامش البحث

(١) هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ٢٠٠٣، ص٢٣.

(٢) محمد النوبي محمد علي، ادمان الإنترنت في عصر العولمة، دار صفاء للنشر، عمان، ٢٠٠٩، ص١١٢.

(٣) مصطفى محمد موسى، الارهاب الالكتروني، ط١، دار الكتب والوثائق المصرية، القاهرة، ٢٠٠٩، ص١٧٣.

(٤) جميل عبد الباقي الصغير، «الإنترنت والإرهاب»، بحث منشور في مجلة العلوم القانونية والسياسية عدد خاص، جامعة ديالي، بغداد، ٢٠١٢، ص٥.

(٥) الإرهاب والجرائم المعلوماتية»، بحث منشور في مجلة المعلوماتية، العدد ٨٠، التي تصدر عن المركز العربي للمعلومات، بيروت، ٢٠١٠، ص١٠٠.

(٦) عادل عبد الصادق، «هل يمثل الإرهاب شكل جديداً من أشكال الصراع الدولي»، مقال منشور في جريدة الاهرام، العدد ١٥٦، مركز تصدر عن الاهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٧، ص١٨.

(٧) عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الاهرام للدراسات السياسة والاستراتيجية، القاهرة، ٢٠٠٩، ص٧٨.

(٨) منير الجنبيهي وممدوح الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠٠٦، ص١٠١.

(٩) عبد المحسن بدوي محمد أحمد، "استراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيري"، الندوة العلمية حول الإعلام والأمن، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، جامعة نايف للعلوم الأمنية، الخرطوم ١١-١٣ سنة ٢٠٠٥، ص٥.

(١٠) يونس عرب، "قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان"، مشغل عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية المنعقدة بمسقط، سلطنة عمان، ٢-٤ نيسان، ٢٠٠٦، ص٤٣.

(١١) عبد الجبار الحنيص، " الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي –دراسة مقارنة–، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٧، العدد الأول، دمشق، ٢٠١١، ص١٩٥.

(١٢) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، دون سنة نشر، ص٥٨

(١٣) أحمد بن محمد اليماني، الحماية الجزائية للبريد الإلكتروني دراسة تأصيلية مقارنة، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في قسم العدالة الجزائية، تخصص السياسة الجزائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات، قسم العدالة الجزائية، الرياض، ٢٠١٠، ص٩٩.

(١٤) منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجزائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجزائية، الرياض، ٢٠١٠، ص٧٦.

(١٥) أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار نشر، دون بلد نشر، ٢٠٠٥، ص٥٨.

(١٦) نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، بيروت، ٢٠١١، ص١٤٠.

(١٧) احمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩، ص٧٢.

(١٨) مصطفى محمد موسى، المراقبة الإليكترونية عبر شبكة الإنترنت–دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس– الطبعة الأولى، دار الكتب والوثائق القومية المصرية، القاهرة، ٢٠٠٣، ص١٩٢.

(١٩) هلالي عبد الله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مطبعة النسر الذهبي للطباعة، القاهرة، ١٩٩٧، ص٢١٧.

(٢٠) احمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، مرجع سابق، ص٧٦.

(٢١) احمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، مرجع سابق، ص٧٥.

(٢٢) هلالي عبد الله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص٢٢٠.

(٢٣) احمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، مرجع سابق، ص٨٠.

(٢٤) نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، مرجع سابق، ص١٤٣.

(٢٥) عمار عباس الحسيني، المشكلات الإجرائية في مجال الإجرام المعلوماتي، بحث مقدم إلى مؤتمر الأمن والتشفير المعلوماتي، جامعة النجف الاشرف، بغداد، ٢٠٠٨، ص٤٥.

(٢٦) عمار عباس الحسيني، المشكلات الإجرائية في مجال الإجرام المعلوماتي، مرجع سابق، ص٣٢٦.

(٢٧) سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤، ص١٠.

(٢٨) محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الانترنت، دراسة مقارنة، ط١، مركز الدراسات العربية للنشر والتوزيع، القاهرة، ٢٠١٩، ص١٢٢.

(٢٩) خالد أبو الفتوح، فيروس الكمبيوتر، مرض التكنولوجيا الحديثة، ط١، دار الكتب العلمية للنشر والتوزيع، القاهرة، ١٩٩٠، ص١٦٧.

(٣٠) عمار عباس الحسيني، المشكلات الإجرائية في مجال الإجرام المعلوماتي، مرجع سابق، ص ٣٢٩.

(٣١) هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٧، ص٧٧.

(٣٢) نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، مرجع سابق، ص١٤٤.