



وزارة التعليم العالي والبحث العلمي
جامعة أكلي محمد أولحاج - البويرة
كلية الحقوق والعلوم السياسية



مكافحة الإرهاب الإلكتروني في ضوء القانون الدولي والتشريع الوطني

مذكرة تخرج لنيل شهادة الماستر في القانون
تخصص: قانون جنائي وعلوم جنائية

تحت إشراف الأستاذ:
د- محمدي محمد لمين

إعداد الطالبتين :
- حدادي خلود
- رمان كنزة

لجنة المناقشة:

الأستاذ:.....أ/ يحيى فاتيح رئيسا
الأستاذ:.....د/ محمدي محمد لمين..... مشرفا ومقررا
الأستاذ:.....أ.د/ زعادي محمد جلول.....ممتحنا

السنة الجامعية: 2026/2025

شكر وعرفان

الحمد لله الذي وفقنا لإتمام هذا العمل، والصلاة والسلام على رسول الله.

نتقدم بخالص الامتنان إلى أستاذنا المشرف الدكتور محمد لمين

محمودي على توجيهاته القيمة ودعمه العلمي المستمر طيلة مسار البحث.

كما نشكر أعضاء لجنة المناقشة على وقتهم الثمين وما سيقدمونه من

إثراء لهذا العمل.

كل الشكر والتقدير لكل من ساندنا، من الأهل والأصدقاء، ولكل من

كان عوناً لنا في إتمام هذه الدراسة.

اهداء

إلى نفسي، التي صبرت واجتهدت حتى بلغت هذا المقام.

إلى روح والدي الغالية حورية "رحمة الله عليها"، التي رحلت عن عالمنا تاركةً في قلبي أثراً لا يمحوه الزمن، رحمها الله وجعل مثواها الجنة.

إلى والدي العزيز جمال، قدوتي ومصدر إلهامي، الذي لم ييخل عليّ يوماً بدعمه وتشجيعه، حفظه الله وأطال في عمره.

إلى سندي وعزوتي، أخواتي إيمان، فريال، وسيليا، كنتم لي دائماً خير عون وسند في مساري الدراسي.

إلى أخي سعيد، رفيق دربي وعضدي في مسيرتي؛ شكراً لكونك السند الذي لا يميل

إلى شريك حياتي ورفيق دربي فؤاد، شكراً لوجودك الداعم، ولصبرك وتشجيعك الذي كان لي حافزاً في كل خطوة،

إلى قرة عيني، ابنة أخي الصغيرة سدره، التي تملأ حياتنا بالبراءة والأمل.

إلى أصدقائي الذين تقاسمت معهم دروب الدراسة، وأوفوا بالعهد والوفاء

إلى كل من كان له بصمة في نجاحي، أهدي ثمرة هذا الجهد.

اهداء

إلى نفسي،

لكل ما بذلته من مثابرة، ولجهودي التي لا تكل، وللقدرة التي استمدتها من أعماق ذاتي لأتجاوز كل تحدٍ واجهته في هذا المسار.

إلى أمي الغالية " حكيمة "

يا نبع الحنان الذي لا ينضب، ويا سر وجودي. كانت دعواتك لي نوراً يضيء دربي، وثقتك بي دافعي الأكبر للنجاح. حفظك الله وأطال في عمرك ومتعك بالصحة والعافية.

إلى أبي العزيز، محمد،

يا سندي وقودتي في الحياة. شكراً لك على كل التضحيات التي قدمتها، وعلى نصائحك السديدة، وشكراً لأنك كنت دائماً أول المؤمنين بقدراتي.

إلى أخوتي، دالية وأنايس،

لوجودكن الثمين، وتشجيعكن المستمر، ولكل لحظات الفرح التي تقاسمناها معاً.

إلى إخوتي، رمضان وأنايس،

على مودتكم الأخوية الصادقة، ودعمكم الذي لا يلين، ولأنكم كنتم خير رفاق لي في هذه المغامرة.

إلى رفيق دربي (A.Y)،

شكراً لأنك النور في لحظات الشك، وأجمل ما في رحلتي. بوجودك بجانبني، تصبح كل الصعاب أهون، وكل نجاح أجمل. شكراً لإيمانك بي ولرعايتك التي تجعل من هذا المسار حكاية مميزة. هذا النجاح هو نجاحك أيضاً.

إلى أصدقائي،

الذين كانوا خير سند، شكراً لوجودكم، وللحظات الجميلة التي جمعتنا، ولكلمات التشجيع التي دفعتني دائماً نحو الأمام.

قائمة المختصرات

ص: صفحة

ص ص : من الصفحة إلى الصفحة

ط: طبعة

د ط: دون ذكر الطبعة

ج ر ج ج : الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية

تح: تحقيق.

مقدمة

يشهد العالم المعاصر منذ أواخر القرن الماضي طفرة تكنولوجية هائلة وثورة معلوماتية غير مسبوقة، فرضت تحولات جذرية في مختلف مناحي الحياة البشرية، وإذا كان هذا الفضاء الرقمي والشبكات المعلوماتية قد ساهما في تقريب المسافات وتسهيل تبادل المعارف وتحقيق رفاهية المجتمعات، إلا أنهما في المقابل أفرزا بيئة رقمية افتراضية استغلتها جماعات الجريمة المنظمة والتنظيمات المتطرفة لإنتاج أنماط إجرامية مستحدثة تتجاوز معها مفاهيم السيادة الوطنية والحدود الجغرافية التقليدية، ويأتي على رأسها "الإرهاب الإلكتروني".

وتعد ظاهرة الإرهاب الإلكتروني نتاجاً حتمياً للتقاطع الخطير بين العقيدة الإرهابية المتطرفة والوسائل التقنية فائقة التطور؛ فلم يعد الفضاء السيبراني مجرد وسيلة للتواصل المتبادل، بل تحول إلى ساحة حرب بديلة ومفتوحة، تلجأ إليها الجماعات التخريبية لتحقيق مآربها مستفيدة من الخصائص البنيوية التي تميز البيئة الرقمية كالفورية، والسرعة، والانتشار الواسع، وصعوبة التتبع الأمني والإثبات الجنائي الرقمي. هذا المصطلح يُمثل الدمج الفعلي بين دلالة "الرعبة" و"الخوف" لغويةً واصطلاحاً، وبين الوسيلة التقنية "الإلكترونية" القائمة على الأنظمة والبرمجيات والمواقع؛ فهو يجسد التطور الأخطر للإرهاب الكلاسيكي بعد أن استُبدلت فيه الأسلحة والمتفجرات التقليدية بالشفيرات والبرامج الخبيثة. وتكمن خطورة هذا السلوك الإجرامي المستحدث في كونه جريمة عابرة للحدود، تنفذ بأساليب تقنية تخلف أضراراً كارثية معنويةً وماديةً دون الحاجة للتواجد الميداني للجناة.

الأمر الذي يفرض على الباحث في العلوم الجنائية ضرورة تمييزه بدقة عن الجرائم المعلوماتية التقليدية كالقرصنة العابرة أو السرقة الرقمية، وذلك بالتركيز على "المعيار الغائي" الذي يحرك الإرهاب الإلكتروني، حيث يتجاوز مجرد تحقيق الربح المادي ليتجه مباشرة نحو بث الرعب الجماعي، وزعزعة الاستقرار والأمن القومي للدول، ومن منظور القانون الجنائي، تبرز الصعوبة التشريعية في تأطير هذه الجريمة ضمن قوالب قانونية موضوعية تضمن الردع

والملاحقة دون الإخلال بالمبادئ الدستورية. وهو ما يستوجب فحص الأركان القانونية المكونة لها؛ بدءاً من الركن الشرعي كضمانة لتجريم السلوك بناءً على النصوص الجزائية الوطنية والاتفاقيات الدولية، مروراً بالركن المادي الذي يمثل النشاط الإجرامي الخارجي المعتمد على الوسيلة الإلكترونية (كالإختراق، القصف الإلكتروني، والتخريب الرقمي للبنى التحتية)، وصولاً إلى الركن المعنوي القائم على القصد الجنائي الخاص الموجه لتدمير الأنظمة أو تهديد سلامة الدول والمجتمعات.

وفي الواقع العملي، تبلورت هذه الظاهرة في صور تطبيقية بالغة الخطورة، تشمل استخدام الفضاء السيبراني في عمليات غسيل الأموال الإلكترونية لتمويل النشاطات الإرهابية، وممارسة التجسس الإلكتروني لسرقة البيانات السيادية، وصولاً إلى شن الهجمات الرقمية لتعطيل المرافق الحيوية.

أسباب الموضوعية لاختيار الموضوع

القصور الإجرائي التقليدي: عجز القواعد القانونية الكلاسيكية (سواء الإجرائية أو الموضوعية) عن استيعاب الأدلة الرقمية، مما يتطلب دراسة كيفية تطويع القانون لمواجهة الجريمة الافتراضية.

الاستغلال التنظيمي للفضاء السيبراني: تحول الإنترنت من مجرد أداة تواصل إلى بيئة متكاملة تستغلها الجماعات الإرهابية في التمويل (كالعملات الرقمية)، التجنيد، وبث الدعاية الهدامة.

تهديد البنى التحتية الحيوية: خروج الإرهاب الإلكتروني من إطار السب والشتم أو الاختراق البسيط، إلى مرحلة شل الأنظمة الحيوية للدول (كشبكات الطاقة، والمطارات، والمؤسسات المالية) مما يعد حرباً حقيقية.

الأسباب الذاتية في اختيار الموضوع: مواكبة السياسة الجنائية المعاصرة: الرغبة في فهم التوجه الحديث للمشرع (خاصة الجزائري) في الموازنة بين حماية الحريات الرقمية للمواطنين وبين فرض الرقابة والأمن السيبراني.

البحث في "فقه القانون المستحدث": شغل الباحث الشخصي بالتعامل مع النصوص القانونية المرنة والمستحدثة، والتي تتطلب تجديداً مستمراً للذهنية القانونية لمواكبة التطور التقني.

أهمية الدراسة:

خطورة السلاح الجديد: تكمن أهمية الموضوع في أن الإرهاب الإلكتروني أصبح أسهل وأخطر من الإرهاب التقليدي، لأنه يدمر منشآت دول كاملة بضغطة زر ومن خلف الشاشات.

تحديث القوانين: تبيان مدى حاجة القوانين الحالية للتطوير والتجديد لكي تتماشى مع الجرائم الذكية والسريعة التي تحدث على الإنترنت.

مساعدة القضاء: تقديم حلول واضحة لرجال الأمن والقضاة تساعدهم على فهم "الدليل الرقمي" وكيفية تتبع المجرمين عبر الحدود.

حماية المجتمع والدولة: حماية الأنظمة الحيوية في الدولة (كالمنظومات البنكية، الاتصالات، والمؤسسات الأمنية) من خطر الاختراق والشلل.

أهداف الدراسة

ضبط المفهوم الدقيق للإرهاب الإلكتروني وتمييزه عن باقي الجرائم المعلوماتية بناءً على "المعيار الغائي" (بث الرعب وزعزعة الأمن).

تحليل الخصائص والأركان: دراسة الطبيعة الخاصة للجريمة (عابرة للحدود، خفية، وصعوبة الإثبات) وتأسيس أركانها القانونية (الشرعي، المادي، والمعنوي).

رصد الصور والآليات: الإحاطة بالأشكال العملية للظاهرة كتمويل الإرهاب عبر غسل الأموال الرقمي، التجسس السيبراني، واختراق المنشآت الحيوية. 4 تقييم المنظومة التشريعية: فحص مدى فاعلية القوانين الوطنية (كالمرسوم التشريعي الجزائري) والاتفاقيات الدولية والإقليمية في مواجهة هذه الجريمة المستحدثة وسد ثغراتها إشكالية الدراسة: تأسيساً على هذا التداخل المنهجي والقانوني.

وفي ظل التطور المتسارع للفضاء الرقمي، تتبلور الإشكالية المحورية لهذه الدراسة حول التساؤل الرئيسي التالي: كيف تتحقق جريمة الارهاب الإلكتروني وماهي الآليات الدولية والوطنية لمواجهتها؟».

للإجابة على الإشكالية اعتمدنا على المنهج الوصفي من خلال تقديم المفاهيم العامة المتعلقة بجوانب الدراسة، بالإضافة إلى المنهج التحليلي من خلال تحليل النصوص القانونية الوطنية والأجنبية، ضف إلى ذلك اتباع المنهج المقارن بما يتضمنه القانون الجزائري وبعض التشريعات الأجنبية الوطنية والدولية.

والإحاطة بجميع جوانب الموضوع، تم تقسيم هذا البحث وفق خطة ثنائية على النحو التالي: الفصل الأول: الإطار المفاهيمي للإرهاب الإلكتروني الفصل الثاني: آليات مكافحة الإرهاب الإلكتروني.

الفصل الأول

الاطار المفاهيمي للإرهاب الالكتروني

الفصل الأول

الاطار المفاهيمي للإرهاب الإلكتروني

تعد ظاهرة الإرهاب الإلكتروني نتاجاً حتمياً للتقاطع بين العقيدة الإرهابية المتطرفة والوسائل التقنية فائقة التطور، حيث لم يعد الفضاء السيبراني مجرد وسيلة تواصل بل أصبح ساحة حرب مفتوحة تتجاوز مفاهيم السيادة التقليدية والحدود الجغرافية. إن استيعاب هذه الظاهرة يفرض أولاً تفكيك بنيتها المفاهيمية، بدءاً من أصولها اللغوية المرتبطة ببث الذعر، وصولاً إلى ماهيتها الاصطلاحية كـ "حرب معلوماتية" تهدف إلى تقويض الأمن القومي للدول عبر استهداف البنى التحتية الحيوية ببرمجيات رقمية بديلة عن الأسلحة التقليدية. وتتجلى خطورة هذا النمط الإجرامي في خصائصه البنيوية الفريدة، فهو جريمة عابرة للقارات تتسم بالسرية وصعوبة الإثبات الرقمي، وتنفذ بأساليب "تظيفة" مادية لكنها كارثية معنوياً وتقنياً، مما يستوجب تمييزه بدقة عن الجرائم المعلوماتية التقليدية والقرصنة العابرة، بالتركيز على "المعيار الغائي" الذي يهدف إلى زعزعة استقرار المجتمع وبث الرعب الجماعي.

وانطلاقاً من هذا التوصيف القائم على اطار والخصائص، يبرز التحدي القانوني في تأطير هذه الجريمة ضمن قوالب تشريعية تضمن الردع والملاحقة، وهو ما يتحقق من خلال فحص الأركان المكونة لها، حيث يشكل الركن الشرعي الضمانة الدستورية للتجريم عبر نصوص قانون العقوبات التي استوعبت الأنماط المستحدثة للإرهاب، بينما يجسد الركن المادي السلوك الإجرامي المتمثل في استغلال البيئة الرقمية (كالاختراق والتهديد البريدي) وما يترتب عليها من نتائج ملموسة في الواقع الافتراضي والمادي.

ولا يكتمل البنيان القانوني للجريمة إلا بالركن المعنوي الذي ينفي وجود الخطأ غير العمدى، ويركز على القصد الجنائي الخاص الذي يحرك إرادة الجاني نحو تحقيق مآرب إيدولوجية أو سياسية، وتتعدد صور هذا الإرهاب في الواقع العملي لتشمل عمليات غسيل الأموال الإلكترونية لتمويل النشاطات التخريبية، والتجسس السيبراني لسرقة الأسرار السيادية،

وصولاً إلى القصف الإلكتروني الذي يستهدف إخراج المؤسسات الحيوية عن الخدمة، مما يجعل من هذه الدراسة وحدة متكاملة تربط بين المفهوم النظري وآليات التنفيذ الواقعي في ظل بيئة تقنية متغيرة باستمرار، وعليه من أجل الإحاطة بمختلف جوانب هذه الظاهرة قسمنا هذا الفصل إلى مبحثين، (المبحث الأول) مفهوم الإرهاب الإلكتروني، و(المبحث الثاني) أركان الإرهاب الإلكتروني وصوره.

المبحث الأول

مفهوم الإرهاب الإلكتروني

يواجه العالم المعاصر تحدياً أمنياً غير مسبوق، فرضته الطفرة النوعية في تكنولوجيا المعلومات والاتصالات، فبقدر ما ساهم الفضاء الرقمي في تقريب المسافات وتحقيق الرفاهية، بقدر ما تحول إلى "بيئة خصبة" لنشوء أنماط إجرامية مستحدثة، يتصدرها الإرهاب الإلكتروني. هذا المصطلح الذي يمزج بين دلالة "الرعبة" اللغوية المتأصلة في الخوف، وبين الوسيلة "الإلكترونية" القائمة على النبضات الرقمية والأنظمة البرمجية، يمثل التطور الأخطر للإرهاب الكلاسيكي، حيث استبدلت فيه المتفجرات بالشفيرات البرمجية، والمواجهة الميدانية بالاختراقات العابرة للحدود.

تتجلى خطورة هذا النوع من الإرهاب في خصائصه البنيوية التي تجعله عصياً على الإثبات والملاحقة؛ فهو جريمة "عابرة للقارات" تتلاشى فيها الحدود الجغرافية، وهي "جريمة نظيفة" من حيث افتقارها للعنف المادي الملموس، لكنها كارثية من حيث الأثر المعنوي والمادي على البنى التحتية للدول، إن صعوبة الإثبات الرقمي وغياب البصمة المادية التقليدية، جعلت من الإرهاب الإلكتروني سلاحاً مفضلاً للجماعات المتطرفة التي تسعى لتحقيق أجندات سياسية أو أيديولوجية تحت غطاء من التخفي التقني.

ومع تداخل المفاهيم في الفضاء السيبراني، يبرز التحدي القانوني في تمييز الإرهاب الإلكتروني عما يشابهه من جرائم؛ فهو يلتقي مع "الجريمة المعلوماتية" في الوسيلة التقنية، لكنه

ينفصل عنها في الغاية التي تتجاوز الربح المادي إلى زعزعة الاستقرار العام. كما أنه يتقاطع مع "القرصنة الإلكترونية" في آليات الاختراق، إلا أنه يتفوق عليها في كونه فعلاً ممنهجاً يهدف لبث الرعب الجماعي وتقويض الأمن القومي، إن هذا الاشتباك المفاهيمي يستوجب وضع إطار قانوني وفقهي دقيق يحدد ذاتية الإرهاب الإلكتروني، بما يضمن تكييفاً قضائياً سليماً يواجه "إرهاباً بلا حدود" يهدد كيان الدولة والمجتمع في العصر الرقمي. ومن خلال هذا المبحث سنقوم بدراسة تعريف الإرهاب الإلكتروني (المطلب الأول) وخصائص الإرهاب الإلكتروني وتمييزه بالجرائم المشابهة (المطلب الثاني).

المطلب الأول

تعريف الإرهاب الإلكتروني

شهد العالم في العقود الأخيرة تطوراً متسارعاً في مجال تكنولوجيا المعلومات والاتصال، الأمر الذي أسهم في إحداث تحولات عميقة في مختلف مجالات الحياة، غير أن هذا التطور لم يقتصر على الجوانب الإيجابية فحسب، بل أفرز أيضاً أنماطاً جديدة من الجرائم التي تستغل الفضاء الرقمي كوسيلة لتنفيذ مخططاتها، وفي مقدمتها ظاهرة الإرهاب الإلكتروني، فقد أصبح الفضاء السيبراني ساحة بديلة للصراع، تلجأ إليها الجماعات المتطرفة لتحقيق أهدافها دون الحاجة إلى المواجهة التقليدية، مستفيدة من السرعة والانتشار الواسع وصعوبة التتبع التي تميز البيئة الرقمية.

وانطلاقاً من خطورة هذه الظاهرة وما تطرحه من تحديات أمنية وقانونية، برزت الحاجة إلى تحديد مفهوم الإرهاب الإلكتروني بشكل دقيق، ويقتضي ذلك الوقوف على أبعاده المختلفة من خلال دراسة تعريفه اللغوي والاصطلاحي، ثم بيان المقصود به في الفقه والقانون، بما يسهم في فهم طبيعته وخصائصه وتمييزه عن غيره من الجرائم المعلوماتية، لذلك يتم التطرق في هذا المبحث إلى التعريف اللغوي والاصطلاحي للإرهاب الإلكتروني (الفرع الأول)، ثم التعريف الفقهي والقانوني له (الفرع الثاني).

الفرع الأول: تعريف اللغوي والاصطلاحي

في ظل التسارع التقني الذي يشهده عصرنا الراهن في تكنولوجيا المعلومات، برزت أنماط إجرامية مستحدثة يتصدرها الإرهاب الإلكتروني، وهو التطور الرقمي للإرهاب الكلاسيكي الذي استبدل الوسائل المادية بالشبكات والأنظمة المعلوماتية، ويتطلب استيعاب هذا المفهوم بعمق تفكيك أبعاده من منظورين (أولاً) لغوي يبحث في الأصول الدلالية للمصطلح، (ثانياً) اصطلاحاً يحدد إطاره العلمي والقانوني، مما يعكس طبيعة التحول في النزاعات المعاصرة داخل الفضاء الرقمي.

أولاً: التعريف اللغوي

لم تكن المعاجم العربية القديمة تعرف "الإرهاب" كمصطلح سياسي أو اجتماعي بمدلوله المعاصر، بل ركزت على الأصل الثلاثي (رَهَبَ)، الذي يدور حول معاني الخوف، الفرع، والاضطراب النفسي¹، فالدلالة اللغوية الأصلية تتمحور حول فعل إثارة الرهبة في النفس².

أما المعاجم العربية الحديثة فقد استعملت مصطلح الإرهاب بشكل صريح، حيث عرّف "المعجم الوجيز" الإرهابيين بأنهم الذين يتخذون العنف وسيلة لبلوغ أهداف سياسية، وهو ما يُظهر البعد السياسي للمفهوم في الاستعمال المعاصر وفي اللغات الأجنبية، يقابل الإرهاب مصطلح (Terror)، وهو يدل على الخوف الشديد أو القلق البالغ أو التهديد غير المألوف³.

أما فيما يخص الشق الثاني من المصطلح، فإن لفظ "إلكتروني" في معاجم اللغة العربية المعاصرة يُنسب إلى "الإلكترون"، ذلك الجسم الدقيق ذو الشحنة السالبة الذي يمثل حجر

¹ أحمد أبي الحسين، بن فارس بن زكريا، معجم مقاييس اللغة، ج 1، تح: عبد السلام محمد هارون، دار الفكر، الأردن، 1979، ص 447.

² سلوى أحمد ميدان، الإرهاب والجهود الدولية لمكافحته، مجلة القانون للعلوم القانونية والسياسية، العراق، جامعة كركوك، العدد الخامس، 2016، ص ص 53-54.

³ ابن منظور، لسان العرب، دار المعارف، القاهرة، 1981، ص 1748.

الزاوية في بناء الذرة، ومن هذا المنطلق العلمي، أصبحت الصفة تُطلق على كل ما يرتكز في تشغيله أو إنتاجه على التقنيات الرقمية والأنظمة الحديثة¹.

ينبثق مصطلح الارهاب الإلكتروني في المصطلح الاجنبي من دمج عبارتي (Cyber) و(Terrorism)، حيث تحيل السابقة (Cyber) إلى كل ما يتصل بالفضاء الرقمي وشبكات المعلومات، بينما تعود كلمة (Terrorism) في جذورها اللاتينية واليونانية القديمة إلى لفظ (Terreur)، الذي كان يُستخدم لوصف الحالة البدنية من الفزع أو "الارتعاش" الناتج عن خوف داهم. ومع تطور الزمن، انتقل هذا المفهوم من توصيف "الرجفة" الجسدية إلى التعبير عن ظاهرة سياسية وإجرامية تهدف إلى زعزعة الاستقرار وبث الرعب، ولكنها في ثوبها "الإلكتروني" باتت تستخدم النبضات الرقمية والبرمجيات كبديل عن الأسلحة التقليدية².

ثانياً - التعريف الاصطلاحي.

تضرب الجذور التاريخية لظاهرة الإرهاب الإلكتروني في أواخر القرن العشرين، حيث تزامنت نشأتها مع بزوغ مفهوم "حرب المعلومات"³.

ومع تسارع انخراط المجتمعات في عصر "المعرفة والاتصال"، بدأت إرهابات هذه الظاهرة تلوح في الأفق، إلا أن معالمها لم تتضح وتتبلور كخطر استراتيجي إلا في أعقاب أحداث 11 سبتمبر، فقد كشفت الدراسات الأمنية والاستراتيجية التي أُجريت في تلك المرحلة عن تحول جذري في تكتيكات الجماعات المتطرفة؛ إذ انتقلت من أنماط الصدام الميداني التقليدي إلى ما يُعرف بـ "حرب الفضاء المعلوماتي"⁴.

¹ أنطوان نعمة وآخرون، معجم المنجد في اللغة المعاصرة، ط2، دار المشرق، بيروت، 2001، ص37.

² محمد عبد المحسن سعدون، مفهوم إرهاب وتجرمه في التشريعات الجنائية الوطنية والدولية، مجلة مركز الدراسات، الكوفة، العراق، جامعة الكوفة، 2008، العدد 07، ص 135. ص ص 13-146.

³ عادل عبد الصادق، استخدام الارهاب الإلكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015، ص104.

⁴ عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استراتيجية الأمن القومي، ورقة مقدمة الى مؤتمر الجرائم المستحدثة وكيفية اثباتها ومواجهتها، المركز القومي للبحوث الاجتماعية والجنائية، مصر، 16/15/ ديسمبر 2010، ص2.

ويعكس هذا التحول النوعي سعياً حثيثاً من قبل التنظيمات المتشددة لاختراق الأنظمة الرقمية الحساسة للدول، رغبةً منها في إيقاع أقصى قدر من الأضرار المادية والمعنوية، مع تحييد عنصر المواجهة المباشرة مع الأجهزة الأمنية والاستخباراتية، وبذلك أصبح الفضاء الرقمي هو الساحة البديلة التي تضمن لهذه الجماعات التأثير الواسع مع الحفاظ على ميزة التخفي والبعد عن رصد القوى التقليدية¹.

يُمثل الإرهاب الإلكتروني تحولاً في أدوات الصراع، حيث تستبدل الدول أو الجماعات أو الأفراد الأسلحة التقليدية بـ الوسائل الرقمية والتقنيات المعلوماتية، والهدف الجوهري هنا هو الاعتداء على الكيانات الطبيعية أو الاعتبارية بدوافع سياسية محضة، سعياً لبث الذعر، أو توجيه الرأي العام، أو ممارسة ضغوط على مراكز اتخاذ القرار الحكومي².

كما يمكن القول إن الإرهاب الإلكتروني يرتبط بتوظيف أدوات التكنولوجيا الحديثة لإحداث حالة من الرعب والاضطراب، استناداً إلى أهداف سياسية، بما يؤدي إلى الإخلال بالنظام العام وزعزعة الأمن والاستقرار، وتعطيل أنظمة الرقابة والسيطرة الإلكترونية، ويترتب على ذلك تعريض أمن المجتمع وسلامته للخطر، فضلاً عن شلّ عمل المرافق العامة والمؤسسات الخاصة، والمساس بالحريات الأساسية وانتهاك كرامة الإنسان³.

إن الإرهاب الإلكتروني هو "إرهاب بلا حدود"، يستخدم الكود البرمجي كسلاح لتدمير الواقع المادي والمعنوي للمجتمعات. (المادة الأولى من الاتفاقية العربية لمكافحة جامعة الدول العربية في رهاب، التي عقدت في إطار 22 نيسان عام 1998).

¹ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، ورقة مقدمة في الدولة التدريبية "مكافحة الجرائم الإرهابية المعلوماتية"، المغرب، 9، 13 أبريل 2006، ص 05.

² اسماعيل عبد الفتاح عبد الكافي، الإرهاب ومحاربه في العالم المعاصر، دار الهيئة العامة لقصور الثقافة للنشر والتوزيع، مصر، 2007، ص ص 13-15.

³ عقلية هادي عيسى، اسراء جود حاتم "الارهاب المعلوماتي (الرقمي) وطرق مكافحته"، المجلة السياسية والدولية، العراق، جامعة المستنصرية، العدد 2010، 16، ص ص 182-183.

الفرع الثاني: التعريف القانوني والفقه

تعددت التعريفات الفقهية والقانونية للإرهاب الإلكتروني نتيجة حداثة هذه الجريمة وتطور الوسائل التقنية المستعملة في ارتكابها، وقد سعى الفقهاء والهيئات الدولية إلى تحديد مفهومها وبيان خصائصها وخطورتها على الأفراد والدول، لذلك يتم التطرق إلى التعريف القانوني(أولاً) ، ثم الفقه للإرهاب الإلكتروني(ثانياً).

أولاً : التعريف القانوني

يتبين بالنسبة لحقوق الإنسان، فإن المشرع الجزائري لم يضع تعريفاً صريحاً ومباشراً لما يُعرف بالإرهاب الإلكتروني، بل تم التطرق إليه بشكل غير مباشر من خلال تجريم بعض الأفعال المرتبطة به. وبصفة عامة، تناول هذا المفهوم ضمن قانون الوقاية من الجرائم المعلوماتية ومكافحتها، خاصة في المادة 87 مكرر من القانون 06-24، حيث نصّ على أنه يُعدّ تخريبياً كل فعل يستهدف أمن الدولة، والوحدة الوطنية، واستقرار المؤسسات وسيورها العادي، أو يهدف إلى نشر الرعب بين السكان، وخلق جو من الخوف وانعدام الأمن، سواء من خلال الاعتداء المعنوي أو الجسدي على الأشخاص، أو تعريض حياتهم أو حريتهم أو ممتلكاتهم للخطر.¹

ثانياً: التعريف الفقه

يرى الدكتور مصطفى محمد موسى أن الإرهاب الإلكتروني هو كل سلوك يتضمن استعمال العنف أو التهديد به بهدف تنفيذ مخطط إرهابي، سواء كان فردياً أو جماعياً، ويكون الغرض منه نشر الخوف والهلع بين الناس أو ترويعهم من خلال إيذائهم أو تعريض حياتهم للخطر، كما قد يستهدف إلحاق أضرار بالبيئة أو بالمرافق والأماكن العامة والخاصة، أو الاستيلاء عليها، أو تهديد الموارد الطبيعية، كذلك قد يهدف إلى تعطيل تطبيق الدستور أو

¹ . أنظر المادة 87 مكرر من الأمر رقم 66- 156 المؤرخ في 08 يوليو 1966 المتضمن قانون العقوبات، ج ر ، عدد 49 مؤرخ في 11 / 06 / 1966، المعدل و المتمم بموجب القانون 06-24 المؤرخ في 28 افريل 2024 ، ج.ر، عدد 30 المؤرخ في 30 افريل 2024 .

القوانين واللوائح المعمول بها، ويتم تنفيذ هذا النشاط غير المشروع باستخدام التقنيات الإلكترونية والرقمية عبر شبكة الإنترنت لتحقيق أهداف إرهابية¹.

يستند الإرهاب الإلكتروني إلى توظيف القدرات العلمية والتكنولوجية، واستعمال وسائل الاتصال الحديثة والشبكات المعلوماتية، بهدف بث الخوف والرعب بين الأفراد والتأثير عليهم، إضافة إلى إلحاق الأذى بهم.

وقد ذهب الفقه الى تعريفه بأنه تجاوز قانوني يرتكبه فرد أو جماعة، غايته احداث خلال جسيم في النظام العام عبر استخدام الشبكة المعلوماتية الدولية².

المطلب الثاني

خصائص الإرهاب الإلكتروني وتمييزه بالجرائم المشابهة

يُمثل الفضاء السيبراني اليوم ساحةً مفتوحة لصراع القوى، حيث لم تعد التهديدات الأمنية محصورة في النطاق المادي الملموس، بل امتدت لتشمل "العنف الرقمي" الذي يتخذ من الأنظمة المعلوماتية وسيلةً ومنطلقاً، ويعد الإرهاب الإلكتروني أحد أخطر إفرازات هذه الطفرة التقنية، مما أوجد تداخلاً مفاهيمياً وقانونياً مع أنماط إجرامية أخرى تشترك معه في البيئة الرقمية وتختلف عنه في الجوهر.

تحديد الذاتية القانونية للإرهاب الإلكتروني يستوجب بالضرورة رسم حدود فاصلة تميزه عن الإرهاب التقليدي الذي يشترك معه في الغاية، وعن الجريمة المعلوماتية التي تتقاطع معه في الوسيلة، وصولاً إلى القرصنة الإلكترونية التي قد تشابهه في آليات الاختراق، وتكمن أهمية هذا التمييز في ضبط التكييف القانوني السليم، وتحديد العقوبات الرادعة التي تتناسب مع

¹ مصطفى محمد موسى، الإرهاب الإلكتروني، دراسة قانونية، أمنية، نفسية، ط1، دار الكتب والوثائق المصرية، القاهرة، ص05.

² اسراء طارق جواد، كاظم الجابري، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، في القانون العام، كلية الحقوق جامعة النهرين، العراق، 2012، ص 23.

خطورة الفعل الإرهابي وما يترتب عليه من زعزعة للأمن القومي وتقويض لاستقرار المجتمعات.

وعليه مما سبق وجب ابراز أهم خصائص الإرهاب الإلكتروني (الفرع الأول) من جهة ومن جهة ثانية المقارنة بين الارهاب الإلكتروني ونظرائه من الجرائم المستحدثة والتقليدية، مع التركيز على المعيار الغائي والوسيلة المتبعة في كل منهما (الفرع الثاني).

الفرع الأول: خصائص الإرهاب الإلكتروني

تتفرد الجرائم المعلوماتية، وفي مقدمتها الإرهاب الإلكتروني، بخصائص تجعلها عضية على المقارنة بالجرائم التقليدية؛ لكونها تنبثق من بيئة رقمية افتراضية تعتمد كلياً على النظم التقنية، مما يمنحها تعقيداً يتجاوز الجرائم المادية، وتخطيها للحدود الجغرافية (أولاً) فضلاً عن تنفيذها دون اللجوء للعنف الملموس (ثانياً)، وتتجلى خصوصيتها في صعوبة رصدها وإثباتها (ثالثاً)، واعتمادها على أساليب تقنية متطورة (رابعاً) وهو ما يضع المنظومات القانونية والعملية أمام تحديات استثنائية تستوجب فهماً عميقاً لطبيعتها غير النمطية.

أولاً: الارهاب الإلكتروني جريمة عابرة للحدود

تتجلى خطورة الجريمة العابرة للقارات في قدرة تكنولوجيا المعلومات الفائقة على تذليل المسافات وتقريب الصلة بين مختلف أرجاء العالم، مما حول مسرح الجريمة إلى نطاق عالمي مفتوح يتجاوز الحدود الجغرافية التقليدية لكونها تُنفذ عبر الفضاء السيبراني، وهو الأمر الذي يفرض تحديات جسيمة على المستويات القانونية والإدارية والتقنية والسياسية، خاصة فيما يتعلق بإجراءات الملاحقة الجنائية الدولية، لا سيما حين يتم إعداد البرمجيات الإجرامية في دولة ما ثم نسخها وتوزيعها لتمتد آثارها العابرة للحدود إلى دول مختلفة حول العالم¹.

¹ أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، مذكرة لنيل درجة ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين 2008، ص 11.

كما ساهم ترابط العالم عبر شبكات الاتصال المعتمدة على الأقمار الصناعية والإنترنت في الانتشار الواسع لجرائم الإرهاب الإلكتروني، حيث تلاشت الحواجز الجغرافية بين الدول نتيجة اندماج العالم في شبكة تقنية موحدة، وانطلاقاً من ذلك، باتت هذه الجرائم تُرتكب في فضاء رقمي لا يعترف بقيود الزمان أو المكان، مما أدى إلى بروز معضلات قانونية وإجرائية معقدة، لا سيما فيما يتعلق بتحديد الدولة التي يتركز فيها الاختصاص القضائي لملاحقة هذه الجرائم، فضلاً عن إشكالية تحديد القانون الواجب التطبيق عليها¹.

ثانياً: جرائم غير العنيفة

لا تقتضي جرائم الإنترنت ممارسة العنف أو بذل مجهود بدني شاق لغرض إتمامها، بل هي تُنفذ بأقل قدر من الجهد المادي مقارنة بالجرائم التقليدية التي تتركز في جوهرها على المجهود العضلي، كما هو الحال في جرائم القتل والاختطاف، أو أفعال الكسر والخلع واصطناع المفاتيح في جرائم السرقة.

وتتميز الجرائم المعلوماتية بكونها جرائم تتسم بالهدوء في طبيعتها، إذ تُرتكب في بيئة رقمية دون ضجيج أو مظاهر عنف مادي، وغالباً ما تتم في سرية تامة بعيداً عن الانتباه المباشر للضحية أو للسلطات²، إذ يتركز تنفيذها على مهارة التعامل مع الحاسب الآلي وتوظيف القدرات التقنية في ممارسات غير مشروعة عبر شبكة المعلومات الدولية (الإنترنت)، حيث يستغل المجرم خبرته في الاختراق أو التجسس أو التغيرير بالقاصرين، ومن هذا المنطلق تُصنف الجرائم المرتكبة عبر الفضاء الرقمي ضمن "الجرائم النظيفة" التي تخلو من إراقة الدماء أو المظاهر العنيفة، فهي لا تعد كونها تلاعباً بأرقام وبيانات يجري تغييرها داخل السجلات

¹ عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص52.

² صالح بن محمد المسند وعبد الرحمن بن راشد المهني، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، العدد29، المجلد 95، أبريل 2000، ص20.

المخزنة في الذاكرة الحاسوبية، مما يجعل أثرها معنوياً وتقنياً لا يترك وراءه أي بصمة مادية في العالم الخارجي¹.

ثالثاً: صعوبة الإثبات

يُعتبر الكشف عن الجريمة الإلكترونية مسألة معقدة، وحتى إذا تم اكتشافها فإن التبليغ عنها وإثباتها يواجهان تحديات كبيرة، ويرجع ذلك إلى أن هذا النوع من الجرائم لا يرتبط بوجود مادي ملموس، بل يحدث داخل بيئة افتراضية، الأمر الذي يزيد من صعوبة التعامل معه من قبل الجهات الأمنية والقضائية².

كما أن أساليب الإثبات التقليدية غالباً لا تكون فعالة في هذا المجال بسبب الطبيعة الخاصة للجريمة الإلكترونية، ويُضاف إلى ذلك نقص الخبرة الفنية والتقنية لدى بعض أفراد الشرطة والهيئات القضائية، مما يشكل عائقاً أمام إثبات هذا النوع من الجرائم، فالتعامل معها يتطلب تكويناً متخصصاً في تقنيات المعلومات وكيفية جمع الأدلة الرقمية وإجراء عمليات التفتيش في بيئة الانترنت³.

ونتيجة لضعف الخبرة أحياناً، قد لا يتم الاهتمام الكافي بالتحري والبحث في هذا النوع من الجرائم، وهو ما يستدعي تعزيزاً لتخصص التقني والأمني والقضائي لمواجهة الجريمة الإلكترونية بفعالية أكبر.

تُعد وسائل المعاينة والإثبات التقليدية في الغالب غير كافية لإثبات الجرائم الإلكترونية، وذلك بسبب طبيعتها الخاصة، إذ يتم ارتكابها عبر شبكة الإنترنت وفي فضاء غير ملموس،

¹ نيا ب موسى البدانية، دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، دورة تدريبية في كلية التدريب، قسم البرامج التدريبية بالقنصرة، المغرب، 2006، ص20.

² محمد عبيد الكعبي والجرائم المنشأة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، ص 32.

³ تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة دكتوراه الفلسفة الأمنية، كلية الدراسة العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص20.

فالنشاط الإجرامي في هذا النوع من الجرائم لا يترك آثاراً مادية واضحة، بل يتمثل في بيانات وإشارات إلكترونية تنتقل عبر الوسائط الرقمية¹.

ويستطيع المجرم الإلكتروني اختراق جهاز الحاسوب الخاص بالضحية، أو التلاعب بالمعطيات المخزنة فيه، أو الاطلاع عليها، أو حتى تدمير النظام بالكامل، دون أن يترك أدلة مادية ظاهرة. ومن جهة أخرى، تطرح مسألة استخراج الدليل الرقمي عدة إشكالات قد تؤثر على قناعة القاضي الجزائي، مما قد يؤدي إلى عدم الأخذ به، وبالتالي إفلات الجاني من العقاب، كما أن التطور التكنولوجي يمنح المجرم الوقت والوسائل الكافية لمحو آثار جريمته أو تغييرها بسرعة كبيرة، وفي ظرف وجيز يكاد لا يُذكر، مما يجعل التعرف عليه أو إثبات تورطه أمراً بالغ الصعوبة.²

رابعاً: أسلوب ارتكاب الجريمة المعلوماتية

تتميّز الجرائم المعلوماتية بخصوصية واضحة من حيث طريقة ارتكابها والأساليب المستعملة فيها. فإذا كانت الجريمة التقليدية غالباً ما تعتمد على القوة المادية أو الجهد العضلي، كما هو الحال في بعض جرائم السرقة التي قد تتطلب الكسر أو الخلع للوصول إلى الشيء محل الجريمة، فإن الجريمة المعلوماتية تعتمد أساساً على الوسائل التقنية والمعرفة المعلوماتية في تنفيذها، وبذلك يتم ارتكاب هذا النوع من الجرائم عبر استغلال الحاسوب أو الشبكات المعلوماتية للوصول إلى المعطيات أو الأنظمة بطريقة غير مشروعة، دون الحاجة إلى استعمال القوة المادية التي تميّز الجرائم التقليدية³.

¹ محمد حماد مرهج الهيتي، الجريمة المعلوماتية دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، مصر، 2014، ص 64.

² موسى مسعود أرحومة، اشكاليات الإجراءات التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية و القانون، أكاديمية دراسات العليا، طرابلس 2009، ص 03 .

³ نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة لنشر والتوزيع، طبعة 02 ، دار وائل لنشر، الجزائر، 2010، ص 57-58.

الفرع الثاني: تمييز الإرهاب الإلكتروني عن الجرائم المشابهة

يعدّ التمييز بين الإرهاب الإلكتروني والجرائم المشابهة معه أمراً ضرورياً لفهم طبيعته القانونية وتحديد حدوده المفاهيمية، خاصة في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصال وما نتج عنه من ظهور أنماط إجرامية حديثة تعتمد على الفضاء الرقمي، ورغم اشتراك الإرهاب الإلكتروني مع كلّ من الإرهاب العادي (أولاً) والجريمة الإلكترونية (ثانياً) والقرصنة المعلوماتية (ثالثاً) في استخدام الوسائل التقنية الحديثة، إلا أنه يتميز عنها من حيث الأهداف والنتائج المترتبة عليه، إذ لا يقتصر على تحقيق منافع مادية أو مجرد اختراق الأنظمة، بل يتجاوز ذلك إلى خدمة غايات سياسية أو أيديولوجية تهدف إلى بث الرعب وتهديد أمن المجتمع واستقراره.

أولاً : الإرهاب العادي

تتمحور العقيدة القانونية في تجريم الإرهاب حول ركيزة ثابتة، وهي توليد حالة من الذعر الناجمة عن استخدام العنف، إذ تظل الغاية الأسمى لكافة أشكال الإرهاب هي بث الرعب وتقويض السكينة العامة في المجتمع.

وعليه، فإن الإرهاب الإلكتروني لا ينفصل في جوهره وغاياته عن الإرهاب التقليدي، إلا أنه يتميز عنه بالاعتماد على "العنف الرقمي" عبر تطبيقات الإنترنت والخدمات المرتبطة بها. فالفرق الجوهرى بينهما لا يكمن في الهدف، بل في الوسيلة العصرية، حيث يتخذ الإرهاب الإلكتروني من أنظمة الحاسب الآلي، والموارد المعلوماتية، والتقنيات المتطورة التي أفرزها عصر المعلومات، أداةً ومنطلقاً لتنفيذ هجماته¹.

¹ نور الله تله، الإرهاب بالوسائل الإلكترونية، مذكرة ماجستير في القانون الجزائي، كلية الحقوق، جامعة دمشق، 2015، 2016، صص 26-27.

ثانياً: الجريمة الإلكترونية

أسهم التقدم السريع في تكنولوجيا الاتصال والاعتماد المتزايد على الأنظمة المعلوماتية في ظهور أشكال جديدة من السلوك الإجرامي عُرِفَتْ بجرائم المعلوماتية أو الجرائم الإلكترونية أو جرائم التقنية الحديثة¹، وقد تنبّه المشرّع الجزائري إلى خطورة هذا النوع من الجرائم، فخصّص له إطاراً قانونياً ضمن القسم السابع من القانون رقم 04-15 المعدّل والمتّم لقانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وذلك في المواد من 394 مكرر إلى 394 مكرر 8²، كما عزّز هذا التنظيم بإصدار القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها³، حيث عرّفت المادة الثانية منه هذه الجرائم بأنها كل اعتداء يقع على أنظمة معالجة المعطيات المحددة في قانون العقوبات، أو أي جريمة أخرى تُرتكب أو يُسهّل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

ومن خلال هذا الإطار يتضح أن الجريمة الإلكترونية والإرهاب الإلكتروني يتقاطعان في عدة سمات مشتركة، من أهمها اعتمادهما على الوسائل التكنولوجية الحديثة، واعتبارهما من الجرائم المستحدثة التي تتجاوز في كثير من الأحيان الحدود الوطنية، إضافة إلى سهولة ارتكابهما وانخفاض تكلفتها المادية مقارنة بالجرائم التقليدية، مع اعتماد مرتكبيهما على قدرات تقنية ومعرفية متقدمة.

ومع ذلك يبقى الاختلاف بينهما قائماً من حيث الغاية، إذ تسعى الجريمة المعلوماتية غالباً إلى تحقيق منافع مالية، بينما يتخذ الإرهاب الإلكتروني بعداً أوسع يرتبط بأهداف سياسية

¹ حسين شفيق، الإعلام الجديد والجرائم الإلكترونية، التسريبات، التجسس الإلكتروني، الإرهاب الإلكتروني، دار الفكر والفن، بدون بلد النشر، 2015، ص 17.

² الأمر رقم 66-156، المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات، المعدّل والمتّم.

³ قانون رقم 04-09 المتعلق بالوقاية بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 الصادر في 5 اوت 2009.

أو أيديولوجية أو دينية، وهو ما يجعله أكثر خطورة لما قد يترتب عنه من تهديد لأمن المجتمع واستقراره.

ثالثاً: القرصنة

تُعرف جريمة القرصنة والاختراق بأنها شكل من أشكال "العصيان المدني الرقمي" الذي يحمل دلالات سياسية تهدف لتعزيز أيديولوجية معينة، وبمفهومها العام، تمثل القدرة على الولوج غير المشروع للهدف عبر استغلال ثغرات أنظمة الحماية¹.

وعادةً ما تنحصر غايات هذه الجرائم في تحقيق مكاسب مادية محدودة، أو مجرد التسلية والإزعاج، حيث يركز هدف القرصان على اختراق الأنظمة والبيانات، وفي المقابل، يتجاوز الإرهاب الإلكتروني ذلك ليكون استغلالاً ممنهجاً للقدرات التقنية والعلمية وشبكات المعلوماتية لتحقيق أجندات أوسع نطاقاً².

¹ عبد الله عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى مؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الانترنت المنعقد من 2 إلى 4 يونيو، القاهرة، مصر، 2008، ص12.

² أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، مطابع جامعة نايف للعلوم الأمنية، الرياض، 2006، ص ص 94-95.

المبحث الثاني

أركان الإرهاب الإلكتروني وصوره

مع التطور السريع لتكنولوجيا المعلومات والاتصال واعتماد المجتمعات المتزايد على الأنظمة الرقمية في حياتها اليومية، ظهرت جرائم جديدة تشكل تهديداً حقيقياً للأمن الوطني والدولي، والأمن الاقتصادي والاجتماعي للمجتمع، وأبرزها الإرهاب الإلكتروني، يشمل هذا النوع من الجرائم أفعالاً متنوعة مثل غسيل الأموال، والتجسس الإلكتروني، والتهديد أو القصف الإلكتروني، التي تستغل الوسائل الرقمية لنشر الرعب وتحقيق أهداف غير مشروعة، ولكي يتم فهم هذه الجرائم قانونياً، يتم الاعتماد على دراسة أركانها الأساسية، وهي الركن الشرعي الذي يضمن وجود نص قانوني يجرم الفعل ويؤطر العقوبة، كما ورد في المواد 87 و394 مكرر من قانون العقوبات الجزائري، ويشمل حماية الأمن الرقمي ومكافحة الاعتداءات الإلكترونية، والركن المادي، المتمثل في الأفعال الظاهرة التي يقوم بها الجاني عبر التكنولوجيا، مثل اختراق الشبكات، إنشاء مواقع إلكترونية، أو إرسال رسائل تهديد، والتي تترتب عليها نتائج ملموسة كالترجيع الجماعي وتعطيل الأنظمة المعلوماتية، وأخيراً الركن المعنوي الذي يركز على إرادة الجاني وقصده الجنائي، سواء العام أو الخاص، الذي يحرك سلوكه ويحدد أهدافه الإجرامية. ويهدف هذا المبحث إلى توضيح هذه الأركان الثلاثة، وتحليل صور الإرهاب الإلكتروني، ويتم تقسيم هذا المبحث إلى أركان الإرهاب الإلكتروني (المطلب الأول) وصور الإرهاب الإلكتروني (المطلب الثاني)

المطلب الأول

أركان الإرهاب الإلكتروني

شهدت المجتمعات الحديثة تحولاً جذرياً نحو الرقمنة والاعتماد المتزايد على أنظمة المعالجة الآلية للمعطيات، مما أفرز تحديات أمنية ومستجدات إجرامية تجاوزت الأنماط

التقليدية إلى فضاء إلكتروني افتراضي. ولضمان حماية الأمن العام والأمن المعلوماتي على حد سواء، وجد المشرع الجنائي نفسه أمام حتمية تكيف الأطر القانونية وتطوير أدوات المساءلة الجزائية لمواجهة ما يُعرف بـ "الإرهاب الإلكتروني" والجرائم المعلوماتية.

ولأجل الإحاطة بأبعاد هذه الظاهرة الإجرامية المستحدثة، وتحديد نطاق المسؤولية الجزائية عنها، تقتضي الدراسة المنهجية تفكيك البنيان القانوني للجريمة والوقوف على أركانها الثلاثة؛ وذلك بالبحث في الركن الشرعي الذي يمثل مظلة المشروعية والغطاء القانوني للتجريم (الفرع الأول)، ثم الغوص في الركن المادي لبيان طبيعة السلوك الرقمي والوسائل المستخدمة في اعتدائه (الفرع الثاني)، والوصول أخيراً إلى تحليل الركن المعنوي للكشف عن الإرادة والنية الإجرامية التي تحرك الجاني في هذا الفضاء الافتراضي (الفرع الثالث).

الفرع الأول: الركن الشرعي

مع تطور المجتمعات واعتمادها المتزايد على الأنظمة الرقمية، برزت الحاجة إلى إطار قانوني متين يضمن حماية الأمن العام والأمن المعلوماتي على حد سواء، ويكمن الركن الشرعي للجرائم في المبدأ الدستوري والقانوني الراسخ الذي ينص على أن «لا جريمة ولا عقوبة ولا تدابير أمن بغير قانون».

في هذا الإطار، (أولاً) تشكل المادة 87 مكرر من قانون العقوبات الجزائي أساس تجريم الإرهاب، حيث تقدم إطاراً شاملاً يغطي جميع أشكال السلوك الإجرامي التقليدية والمستحدثة، بما فيها الإرهاب الإلكتروني، كذلك (ثانياً) نصت المادة 394 مكرر على تجريم الاعتداءات على أنظمة المعالجة الآلية للمعطيات، سواء كانت هدفاً مباشراً أو وسيلة لتنفيذ الجريمة، مما يعكس حرص المشرع على حماية الأمن الرقمي ومكافحة الجرائم الإلكترونية والإرهاب الرقمي.

وبذلك، يمثل الركن الشرعي للجرائم الإرهابية والإلكترونية قاعدة قانونية متكاملة تكفل استجابة فعّالة للتحديات الحديثة، وتضمن حماية المجتمع والدولة على المستويين المادي والرقمي

أولاً : الركن الشرعي الوارد في المادة 87 مكرر

يجد الركن الشرعي لهذه الجريمة مبرره القانوني وأساسه المتين في المبدأ الدستوري والجنائي الراسخ الذي نصت عليه المادة الأولى من قانون العقوبات الجزائري، والمتمثل في قاعدة «لا جريمة ولا عقوبة ولا تدابير أمن بغير قانون»، وهو نص يتميز بالعمومية والشمول، إذ لم يذهب المشرع الجزائري نحو تخصيص هذه الجريمة بنص قانوني ضيق ومنفصل، بل اكتفى بالإحالة إلى الأطر العامة والوصف القانوني للأفعال الإرهابية والتخريبية كما وردت في القسم الرابع، حيث استعرض هناك صور السلوك الإجرامي ومختلف الأفعال المادية المكونة لجريمة الإرهاب، ومن ثم جاءت المادة 87 مكرر لترسم الإطار القانوني الشامل والجامع لمختلف السلوكيات الإجرامية بصفة عامة، وهو ما جعلها تستوعب كافة الأنماط المستحدثة والتقليدية للإرهاب بما فيها "الإرهاب الإلكتروني"، مع الإشارة إلى وجود سند قانوني متم لها في أحكام القسم السابع مكرر¹.

ثانياً: الركن الشرعي الوارد في المادة 394 مكرر

مع التطور التقني المتسارع واعتماد المجتمعات على الأنظمة الرقمية في مختلف المجالات، برزت الحاجة إلى حماية هذه الأنظمة من الاعتداءات الإلكترونية التي تهدد الأمن المعلوماتي، وقد استجاب التشريع الجزائري لهذا التحدي من خلال القانون رقم 04-15 المعدل والمتمم لقانون العقوبات، حيث نصت المادة 394 مكرر على تجريم كل الأفعال التي تمس سلامة أنظمة المعالجة الآلية للمعطيات، سواء كانت هدفاً مباشراً أو وسيلة لتنفيذ الجريمة، ويعكس هذا النص حرص المشرع على صون الأمن الرقمي، فيما تتقاطع التشريعات العربية

¹ المادة 87 مكرر من القانون رقم 24-06 المتضمن قانون العقوبات، سالف الذكر.

الأخرى في تبني سياسات صارمة لمكافحة الجرائم المعلوماتية، بما يشمل حماية الأمن القومي ومكافحة الإرهاب الإلكتروني¹.

تجلت الحماية القانونية ضد الجرائم المعلوماتية في التشريع الجزائري من خلال استصدار القانون رقم 04-15 المعدل والمتمم لقانون العقوبات، والذي استهدف صون أنظمة المعالجة الآلية للمعطيات؛ حيث نصت المادتان 394 مكرر و394 مكرر 7 على تجريم كافة الأفعال التي تمس بسلامة هذه الأنظمة²، سواء اتخذت المعالجة الآلية صفة الوسيلة المساعدة في تنفيذ الجريمة أو كانت هي الغاية والمحل المستهدف بالاعتداء، وفي سياق متصل، تبنت التشريعات العربية نهجاً صارماً في التصدي لهذه الظاهرة، وهو ما يظهر جلياً في النظام السعودي لمكافحة الجرائم المعلوماتية، وتحديداً في مادته السابعة التي أقرت عقوبة السجن لعشر سنوات والغرامة التي تصل لخمسة ملايين ريال لكل من سخر الشبكة المعلوماتية أو أجهزة الحاسب لخدمة المنظمات الإرهابية، سواء بإنشاء مواقع لها، أو تسهيل التواصل مع قياداتها، أو الترويج لأفكارها وتمويلها، وصولاً إلى تجريم نشر طرق تصنيع المتفجرات أو الدخول غير المشروع للأنظمة للحصول على بيانات تمس الأمن القومي والاقتصاد الوطني³.

الفرع الثاني: الركن المادي

الركن المادي للجريمة هو الفعل الخارجي الملموس الذي يمكنك ملاحظته بالحواس، ولا تقوم الجريمة بدونه، لأنه يمثل الاعتداء الذي يمس المجتمع وحقوق الأفراد، كما يساعد وجوده على إثبات الجريمة أمام القضاء.

يقصد بالركن المادي للجريمة النشاط الخارجي الذي يقوم به الجاني من أجل تحقيق النتيجة الإجرامية التي يعاقب عليها القانون، ويكون هذا الفعل موجهاً ضد مصلحة أو حق

¹ المادة 349 مكرر من القانون رقم 24 - 06 سالف الذكر.

² . أنظر المادة 394 مكرر و394 مكرر 7 من قانون العقوبات رقم 04-15 سالف الذكر

³ أنظر المادة 7 من النظام العودي لمكافحة الجرائم المعلوماتية ، الصادر بموجب المرسوم الملكي رقم (م/17) المؤرخ 26 مارس 2007 .

يحميه المشرع، ففي الجرائم التقليدية (أولا) يمكن ملاحظة السلوك الإجرامي بسهولة لأنه يكون فعلاً مادياً واضحاً مثل القتل أو السرقة، (ثانياً) في الجرائم الإلكترونية فتظهر الصعوبة في تحديد هذا السلوك، لأن الجريمة تتم عن طريق معلومات وبيانات تنتقل عبر الحاسوب والشبكات المعلوماتية، وهي أمور غير مادية يصعب الإمساك بها أو ملاحظتها بشكل مباشر.

أولاً: السلوك الإجرامي

يتطلب النشاط الإجرامي في جريمة الإرهاب الإلكتروني وجود بيئة رقمية تعتمد على استعمال الحاسوب والاتصال بشبكة الإنترنت، حيث يقوم الجاني باستغلال هذه الوسائل التكنولوجية لتنفيذ أفعاله غير المشروعة وتحقيق أهدافه الإجرامية، وقد يستخدم المجرم في هذا النوع من الجرائم برامج اختراق أو ينشئ صفحات إلكترونية تحتوي على مواد مخلة بالآداب العامة ويقوم بنشرها عبر الإنترنت، كما قد يقوم بإعداد برامج فيروسات من أجل بثها ونشرها لاحقاً. وفي جرائم الإرهاب الإلكتروني يصعب التمييز بين الأعمال التحضيرية والبدء في تنفيذ الجريمة، لأن مجرد اقتناء برامج الاختراق أو الأدوات التي تساعد على فك الشفرات وكلمات المرور قد يعد جريمة في حد ذاته يعاقب عليها القانون، قد يتخذ الفعل الإجرامي في جرائم الإرهاب الإلكتروني عدة صور وأشكال، من بينها توجيه التهديد عبر المواقع الإلكترونية باستعمال العنف أو نشر الخوف بين أفراد المجتمع وتعريض سلامته للخطر.

كما قد يتم استخدام برامج إلكترونية لتعطيل وسائل الاتصال أو اختراق الشبكات والتشويش عليها، إضافة إلى تعطيل وسائل النقل، وقد يلجأ الجاني أيضاً إلى استعمال برامج خبيثة لاختراق أنظمة الحاسوب وشبكات الاتصال، مما يؤدي إلى تعطيلها أو محو البيانات والبرامج الموجودة فيها أو تدميرها¹.

ومن أهم وسائل الإرهاب الإلكتروني المستخدمة في جريمة الإرهاب الإلكتروني:

¹ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية (مصر)، 2002، ص 114.

1/ البريد الإلكتروني

يُعدّ البريد الإلكتروني من الوسائل المهمة التي قد تُستعمل في مجال الإرهاب الإلكتروني، حيث يستخدمه الإرهابيون للتواصل فيما بينهم وتبادل المعلومات، إضافة إلى نشر أفكارهم والترويج لها من خلال المراسلات الإلكترونية، ويُعرّف البريد الإلكتروني بأنه خدمة تتيح إرسال واستقبال الرسائل والملفات والمعلومات عبر شبكة الإنترنت بسرعة وسهولة، كما يمكن الاطلاع عليها من أي مكان وفي أي وقت، كما قد يلجأ بعض المجرمين إلى اختراق حسابات البريد الإلكتروني الخاصة بالآخرين، من أجل الاطلاع على أسرارهم ومعلوماتهم الشخصية أو التجسس عليها، وذلك بهدف استغلال هذه البيانات في تنفيذ مخططاتهم أو عملياتهم الإجرامية¹.

2/ إنشاء المواقع الإلكترونية

يلجأ بعض الإرهابيين إلى إنشاء وتصميم مواقع إلكترونية على شبكة المعلومات العالمية الإنترنت بهدف نشر أفكارهم والترويج لها، كما تُستعمل هذه المواقع أحياناً لتبادل المعلومات بينهم أو لتقديم إرشادات حول بعض الأنشطة غير القانونية².

ثانياً: النتيجة الإجرامية

وقد تتضمن هذه المواقع محتويات تهدف إلى تعليم طرق اختراق المواقع أو نشر الفيروسات الإلكترونية، إضافة إلى تقديم معلومات تتعلق بوسائل التخريب المعلوماتي، كما قد تُستعمل لنشر طرق تمكّن المستخدمين من الوصول إلى مواقع محجوبة عبر أساليب تقنية مختلفة، مما يجعل هذه المواقع وسيلة خطيرة لنشر مثل هذه الأفكار واستقطاب أشخاص جدد مثل النتيجة الإجرامية الأثر المادي المترتب على السلوك الإجرامي، وهي الركن الثاني من أركان الجريمة المادية، وفي سياق الإرهاب الإلكتروني، لا تقتصر هذه النتيجة على التخريب

¹ عبد الرحمان، مجلة الأمن والحياة ، المجلد 34، العدد5، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2014، ص25.

² محمد عبد الحميد عرفة، علم الإجرام والعقاب، دار المطبوعات الجامعية، الإسكندرية، بدون ذكر سنة النشر، ص 144.

التقني فحسب، بل تمتد لتشمل "عنصر الخطر المعنوي"¹، وتتحقق النتيجة الإجرامية في جريمة الإرهاب الإلكتروني من خلال حالة الخطر التي يسببها الجناة داخل المجتمع. إذ يؤدي هذا النوع من الجرائم إلى تهديد المصالح العامة، كما قد يترتب عنه الإخلال بالأمن والنظام العام، لما يسببه من خوف واضطراب داخل المجتمع.

الفرع الثالث: الركن المعنوي

يُمثل الركن المعنوي الركيزة النفسية للجريمة، حيث يربط بين إرادة الجاني والفعل المجرم بناءً على إدراكه لعدم مشروعيته وآثاره، وتتضاعف أهمية هذا الركن في جرائم الإرهاب الإلكتروني لكونها تقوم على الاستغلال العمدي للتقنية لتحقيق مآرب إرهابية، مما يجعل القصد الجنائي هو المحرك الأساسي لهذا الركن، الأمر الذي يفرض بحث مدى (أولاً) إمكانية قيام هذه الجرائم عبر الخطأ غير العمدي، (ثانياً) تحليل دقيق لعنصري القصد الجنائي العام و (ثالثاً) الخاص اللذين يحددان نية الجاني واتجاه إرادته.

أولاً: انتفاء تصور الخطأ غير العمدي في جريمة الإرهاب الإلكتروني

بالرغم من خلو التشريع الجزائري من تعريف جامع ومانع لماهية "الخطأ غير العمدي"، إلا أن الاجتهاد القضائي تولى هذه المهمة عبر إرساء تعريفات متعددة، خلصت في مجملها إلى أن الخطأ هو كل سلوك إيجابي (فعل) أو سلبي (ترك) إرادي، تترتب عليه نتائج لم يقصدها الفاعل مباشرة أو بصفة غير مباشرة، غير أنه كان بمقدوره تلافيها لو التزم بواجبات الحيطة والحذر الكفيلة بمنع وقوع النتيجة الضارة التي كان من الممكن توقعها وتجنبها².

وبناءً على الاستقراء القانوني لهذا التعريف، يتضح أن جوهر الخطأ يكمن في النتيجة التي تتحقق جراء إهمال الجاني وتقاعسه عن اتخاذ الاحتياطات اللازمة، دون الاعتداد بالفعل

¹ محمد عبد الحميد عرفة، المرجع نفسه، ص144.

² منصور رحمانى، الوجيز في القانون الجنائي العام، د. ط.، دار العلوم للنشر والتوزيع، غنابة 2006، ص125.

المادي المجرد الذي يقتضيه¹، ومن هذا المنطلق، يغدو تصور الخطأ غير العمدي في جريمة الإرهاب الإلكتروني أمراً ممتنعاً، كونها من الجرائم التي لا يتوقف قيامها على تحقق نتيجة مادية محددة، وعليه فإن الركن المعنوي لهذه الجريمة يتمحور حصرياً حول القصد الجنائي باتجاهيه العام والخاص.

ثانياً: القصد الجنائي العام

يُمثل القصد الجنائي الصورة الأشد خطورة ضمن الركن المعنوي، نظراً لتجاوز إرادة الجاني لمجرد ارتكاب الفعل المادي لتشمل الرغبة في تحقيق النتيجة الإجرامية، ورغم أن المشرع الجزائري لم يضع تعريفاً نظرياً للقصد الجنائي، إلا أنه استلزم توافره صراحة في العديد من النصوص لترتيب المسؤولية الجزائية من خلال استخدام مصطلح «عمداً»، وهو ما كرسته المادة 394 مكرر 2 التي نصت على: «كل من يقوم عمداً وعن طريق الغش بما يأتي...»².

وفي هذا الإطار، يُعرف الفقه القصد الجنائي بأنه: «انصراف إرادة الجاني إلى ارتكاب الجريمة مع العلم المسبق بكافة أركانها كما حددها القانون»، ومن هذا التعريف، يتضح أن قيام القصد الجنائي يستوجب بالضرورة اجتماع عنصرين أساسيين هما:

1/ الإرادة

الإرادة هي عبارة عن نشاط نفسي يتجه إلى تحقيق غرض عن طريق وسيلة معينة، فالإرادة ظاهرة نفسية وهي المحرك لأنواع السلوك ذات الطبيعة المادية، تحدث في العالم الخارجي من الآثار ما يشبع به الإنسان حاجاته المتعددة، كما تعرف الإرادة أيضاً على أنها تلك القوة النفسية التي توجه الإنسان إلى تحقيق غاية يتوخاها، ولكي تكون الإرادة معتبرة قانوناً يجب توفر شرطين هما: أن تكون هذه الإرادة مميزة وأن تكون الإرادة حرة الاختيار. ولكي يتوفر القصد الجنائي في جريمة الإرهاب الإلكتروني يجب أن يكون الجاني عالماً بحقيقة

¹ أحسن بوسقيعة، الوجيز في القانون الجنائي العام، ط14، دار هومة، الجزائر، 2014، ص144.

² عمر خوري، شرح قانون العقوبات، قسم العام، محاضرات جامعة الجزائر 1، كلية الحقوق، السنة الجامعية 2010/2011، ص47.

الواقعة الجريمة، سواء كان ذلك من حيث القانون أو الوقائع، ذلك أنه بدون هذا العلم لا يمكن قيام الإرادة، فهي تقوم على أساس العلم بالقانون والواقعة الجرمية¹.

2 / العلم

لا يكتمل البنيان القانوني للقصد الجنائي بمجرد انصراف إرادة الجاني إلى ارتكاب السلوك المادي وتحقيق نتيجته الإجرامية فحسب، بل يستوجب ذلك بالضرورة إحاطة الجاني علماً بكافة العناصر والأركان التي يقوم عليها النموذج القانوني للجريمة، فالعلم يمثل الركيزة التي يدرك من خلالها الفاعل أن سلوكه يشكل اعتداءً غير مشروع على حق أو مصلحة يحميها القانون، فإن المبدأ " لا يعذر أحد بجهله للقانون " يعتبر العلم بالتشريعات مفترض في حق الجميع ، ومن ثم يمتنع على أشخاص الدفع بالجهل كسبب للإعفاء من التبعات القانونية لتصرفاتهم².

ويُعرّف العلم في هذا المقام بأنه تلك الحالة الذهنية ومستوى الإدراك الواعي الذي يسبق مرحلة تنفيذ الإرادة، حيث يعمل على تصور الوقائع وتجسيدها في ذهن الجاني بشكل صحيح ومطابق للواقع، فالعلم هو الذي يرسم للإرادة مسارها ويحدد أطرها وغاياتها نحو تحقيق الواقعة الإجرامية، ومن هذا المنطلق، فإن عنصر العلم في جرائم الإرهاب الإلكتروني يستلزم ازدواجية في الإدراك؛ تشمل العلم بالقاعدة القانونية من جهة، والعلم بالواقعة المادية من جهة أخرى.

وبذلك، يتجسد الركن المعنوي في هذه الجرائم في اتجاه إرادة الفاعل لارتكاب أحد صور الإرهاب الإلكتروني، مع اقتران هذه الإرادة بعلم يقيني بأن المشرع قد أسبغ عليها صفة التجريم والعقاب³.

¹ أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 21، دار بلقيس، الجزائر، 2024، ص 119.

² احسن بوسقيعة، الوجيز في القانون الجزائي العام ، المرجع نفسه ، ص 120.

³ مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الالكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2017، ص55.

ثالثاً: القصد الجنائي الخاص

يتمثل القصد الجنائي الخاص في الغاية المحددة أو المصلحة المرجوة التي تحرك الجاني نحو ارتكاب سلوكه الإجرامي، وهو عنصر يشترطه القانون في جرائم معينة ليكون مكملاً للقصد العام، وفي سياق الإرهاب الإلكتروني، يتجسد هذا القصد من خلال انصراف نية الجاني إلى ممارسة سلوكيات مادية تهدف تحديداً إلى تنفيذ أعمال إرهابية، حيث تتعدد الدوافع التي تقود الشباب للانضمام إلى هذه الجماعات، بدءاً من المحفزات المادية كالبطالة والفقر، أو الدوافع السياسية المرتبطة بغياب العدالة والشعور بالظلم وسلب الحقوق، وصولاً إلى الوازع الديني أو ما يُعرف بالتأثير الوجداني، الذي تستغله المنظمات الإرهابية عبر تحريف تفسير النصوص الشرعية عن مقاصدها الحقيقية¹.

المطلب الثاني

صور الإرهاب الإلكتروني

مع التطور السريع لتكنولوجيا المعلومات والاتصال، ظهرت جرائم حديثة تشكل تهديداً للأمن الاقتصادي والسياسي والاجتماعي للدول، من أبرزها غسيل الأموال، التجسس الإلكتروني، والتهديد أو القصف الإلكتروني. فغسيل الأموال يعد وسيلة رئيسية لتمويل الجرائم المنظمة والإرهاب، بينما يستهدف التجسس الإلكتروني أسرار الدول والمعلومات الحساسة، ويستغل التهديد والقصف الإلكتروني الفضاء الرقمي لبث الرعب وتعطيل الأنظمة والمؤسسات. تهدف هذه الدراسة إلى تحليل هذه الجرائم بدءاً بجريمة غسيل الأموال وعلاقته بالإرهاب الإلكتروني (الفرع الأول)، ثم التجسس الإلكتروني (الفرع الثاني)، وأخيراً حول التهديد والقصف الإلكتروني (الفرع الثالث).

¹ إسراء طارق جواد كاظم الجابري، المرجع السابق، ص72.

الفرع الأول: جريمة غسيل الأموال

تُعد جريمة غسيل الأموال من أخطر الجرائم الاقتصادية الحديثة ذات الأثر السلبي على المجتمعات، حيث يلجأ مرتكبوها إلى أساليب تقنية متطورة وشبكات معقدة لإخفاء المصدر الحقيقي للأموال غير المشروعة وإضفاء طابع قانوني عليها، وتكتسب هذه الجريمة خطورة مضاعفة لارتباطها الوثيق بالجريمة المنظمة، مثل الإتجار بالأسلحة والمخدرات، فضلاً عن دورها المحوري في تمويل التنظيمات الإرهابية، مما جعلها جريمة ذات طابع دولي متزايد يتطلب تضافر الجهود الإقليمية والعالمية لمكافحتها والحد منها، وبناءً على ذلك، فإننا تطرقنا إلى تعريف غسيل الأموال (أولاً)، ثم إلى علاقة الإرهاب الإلكتروني (ثانياً).

أولاً: تعريف جريمة غسيل الأموال

تعددت التعريفات التي تناولت جريمة غسيل الأموال، ويرجع ذلك إلى حداثة هذه الجريمة وسرعة انتشارها في مختلف أنحاء العالم، الأمر الذي جعلها محل اهتمام العديد من المؤتمرات الدولية والتشريعات والفقهاء، الذين سعوا إلى تحديد مفهومها وضبط معالمها، فقد عرّفها بعض الفقه على أنها عملية تحويل أو نقل الأموال المتحصلة من مصادر غير مشروعة أو الناتجة عن التهرب من الالتزامات القانونية إلى صور أخرى من صور الاحتفاظ بالثروة، وذلك بقصد إخفاء مصدرها الحقيقي وإضفاء طابع المشروعية عليها.

كما ذهب اتجاه آخر إلى تعريفها بأنها كل عملية أو إجراء يهدف إلى إخفاء المصدر غير المشروع للأموال التي تم الحصول عليها بطرق غير قانونية.¹

ومن جهة أخرى، فقد تناول المشرع الجزائري جريمة تبييض الأموال ضمن أحكام قانون العقوبات، حيث خصص لها القسم السادس مكرر، واعتبر أن الأفعال المنصوص عليها في المادة 389 مكرر تشكل جريمة تبييض الأموال، ومن بينها:

¹ سيد أحمد عبد الخالق، الآثار الاقتصادية والاجتماعية لغسيل الأموال، د. ط، دار النهضة العربية، القاهرة، 1997، ص 03.

- 1 . تحويل الممتلكات أو نقلها مع العلم بأنها متحصلة من جريمة، بهدف إخفاء أو تمويه مصدرها غير المشروع.
- 2 . إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها.
- 3 . اكتساب الممتلكات أو حيازتها أو استعمالها مع العلم بأنها متحصلة من نشاط إجرامي.
- 4 . المشاركة في ارتكاب هذه الأفعال أو التواطؤ أو المساعدة أو التحريض عليها¹.

ثانياً: علاقة الإرهاب الإلكتروني بجريمة غسيل الأموال

يُعدّ تبييض الأموال إحدى الركائز الأساسية التي تعتمد عليها الجماعات الإرهابية في تمويل أنشطتها وأعمالها الإجرامية، وتوجد علاقة وثيقة بين هذه الجريمة والإرهاب، خاصة في ظل الاستفادة المتزايدة من التقنيات الحديثة ووسائل التكنولوجيا المعاصرة، وتبرز هذه العلاقة بشكل واضح من خلال لجوء الجماعات الإرهابية إلى أساليب الجريمة المنظمة في تنفيذ مخططاتها، إضافة إلى انخراطها في أنشطة غير مشروعة مثل الاتجار بالأسلحة والمخدرات وغيرها من المصادر غير القانونية، وذلك بهدف الحصول على الأموال وتوظيفها في تمويل عملياتها وتحقيق أهدافها الإجرامية².

الفرع الثاني: جريمة التجسس الإلكتروني

يعدّ التجسس الإلكتروني من أخطر الجرائم المعلوماتية التي أفرزها التطور المتسارع في تكنولوجيا المعلومات والاتصال، حيث لم تعد عمليات التجسس تقتصر على الأساليب التقليدية، بل انتقلت إلى الفضاء السيبراني مستهدفة الأنظمة المعلوماتية والبيانات الحساسة، وقد أضحت هذا النوع من الجرائم يشكل تهديداً حقيقياً لأمن الدول واستقرارها، لما ينطوي عليه من إمكانية اختراق الأسرار العسكرية والسياسية والاقتصادية، وتزداد خطورته عندما تتورط فيه جماعات

¹ أنظر المادة 389 مكرر من الأمر رقم 66-156 المتضمن قانون العقوبات، المعدل والمتمم.

² مصطفى طاهر، المواجهة التشريعية لظاهرة غسيل الأموال متحصلة من جرائم المخدرات 02، طبع على نفقة المؤلف، القاهرة، 2004، ص144.

إجرامية أو تنظيمات إرهابية تسعى إلى استغلال الوسائل التقنية الحديثة للإضرار بالمصالح الوطنية وتقويض الأمن العام، الأمر الذي استدعى اهتماماً متزايداً من قبل التشريعات والهيئات الأمنية لمواجهته والحد من آثاره.

يُصنف التجسس كأحد أعرق الأنشطة الاستخباراتية وأشدّها خطورة، حيث لازم الممارسات البشرية تاريخياً عبر مختلف المجالات، لاسيما في النزاعات المسلحة، ومع الطفرة النوعية في تكنولوجيا الإعلام واستخدام الحواسيب والشبكات، تحول التجسس إلى صيغته الرقمية ليشكل الهاجس الأكبر للدول، كونه من أخطر الجرائم التي تستهدف البيانات المخزنة في الأنظمة المعلوماتية، ولا تقتصر خطورة هذا النمط الإجرامي على مجرد استخدام الفضاء السيبراني كأداة، بل تكمن في جوهرها في هشاشة المنظومات الأمنية المخصصة لحماية شبكات المؤسسات والهيئات الحساسة¹،

وفي العصر الراهن، تلاشت الحصانة التقليدية للحدود الجغرافية أمام سطوة أقدار التجسس وتقنيات البث الفضائي، مما وضع سيادة الدول على المحك، لا سيما مع نفاذ الجماعات الإرهابية إلى هذه الوسائل المتطورة².

إن الممكن الحقيقي للخطر في التجسس الإلكتروني لا يتجسد في ممارسات الهواة أو العابثين؛ فهؤلاء غالباً ما تقتصر أضرارهم على إتلاف بيانات يمكن استرجاع نسخها الاحتياطية، بل يبرز التهديد الوجودي حينما تتبنى التنظيمات الإرهابية هذه الجريمة لاستهداف الأشخاص، أو الدول، أو المنظمات الدولية والوطنية على حد سواء.

وترتكز عمليات التجسس الإرهابي على ثلاثة محاور استراتيجية هي: (العسكري، والسياسي، والاقتصادي)، حيث تسعى هذه التنظيمات، بالتنسيق مع أجهزة استخباراتية معادية، إلى اختراق

¹ بن بادة عبد الحليم ، بوحادة محمد سعيد ، جريمة التجسس الإلكتروني نمط جديد من تهديدات السيبرانية الماسة بأمن الدول المنظمة متوفر على الموقع : <http://elmizaine.com> ، تاريخ النشر 03 يوليو 2020 . 2026/05/01 على الساعة

² غادة ناصر، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017، ص30.

أسرار الدولة ومعلوماتها السيادية وتوظيفها في تقويض المصلحة العامة وضرب أركان الوحدة الوطنية¹.

الفرع الثالث: جريمة التهديد والقصف الإلكتروني

مع التطور المتسارع لتكنولوجيا المعلومات والاتصال واتساع نطاق استخدام شبكة الإنترنت، برزت أنماط جديدة من التهديدات التي تستهدف أمن الأفراد والمؤسسات والدول، وقد وجدت الجماعات الإجرامية والإرهابية في الفضاء الرقمي بيئة خصبة لتنفيذ أنشطتها التخريبية بوسائل حديثة تتسم بالسرعة وصعوبة التتبع، الأمر الذي جعل الجرائم الإلكترونية تشكل تحدياً أمنياً وقانونياً معاصراً، وتتنوع هذه الأساليب بين ممارسات تهديد مباشر عبر الشبكة، وهجمات تقنية منظمة تستهدف تعطيل الأنظمة والمواقع الإلكترونية، وهو ما يبرز جلياً من خلال تطرقنا إلى جريمة التهديد الإلكتروني (أولاً)، وإلى القصف الإلكتروني (ثانياً)، باعتبارهما من أبرز صور الاعتداءات التي تستغل الفضاء السيبراني لتحقيق أغراض غير مشروعة.

أولاً: التهديد الإلكتروني

تستغل الجماعات الإرهابية الفضاء الرقمي العالمي كأداة استراتيجية لبث الرعب وزعزعة أمن الأفراد والدول على حد سواء، حيث تتنوع أساليبها في التهديد عبر الإنترنت لتشمل ابتزاز الضحايا بنشر صورهم الخاصة أو مقاطع فيديو وبيانات سرية مقابل مبالغ مالية طائلة، كما يمتد هذا الخطر ليشمل الإفصاح عن الأسرار المهنية للمؤسسات والشركات عبر استدراج الموظفين وسائر فئات المجتمع من خلال البريد الإلكتروني ومنصات التواصل الاجتماعي²، وصولاً إلى توظيف هذه الوسائل في إطلاق تهديدات صريحة باغتيال الشخصيات السياسية أو

¹ الزين بدره هوميل، الإرهاب في القضاء الإلكتروني، رسالة دكتوراه، كلية القانون، جامعة عمان العربية، 2012، ص 177-178.

² سليمان الطعاني الوجيز في التربية الإعلامية، ط1، دار الخليج للنشر والتوزيع، الأردن، عمان، 2020، ص ص 109-108.

تفجير المنشآت الحيوية في الدولة، فضلاً عن شن هجمات تقنية تهدف لتدمير البنية التحتية المعلوماتية ونشر الفيروسات لتخريب الأنظمة الرقمية وإتلافها¹.

ثانياً: القصف الإلكتروني

"يعد القصف الإلكتروني استراتيجية هجومية تعتمد على إغراق المواقع الإلكترونية بمئات الآلاف من الرسائل والبيانات بشكل متزامن، يفوق هذا الضغط الهائل القدرة الاستيعابية للخوادم، مما يتسبب في تعطيل خدمات الشركة ومنع المستخدمين من الوصول إليها، وغالباً ما تستخدم المنظمات التخريبية هذا الأسلوب بهدف تقويض البنية التحتية المعلوماتية وتدمير الأنظمة الرقمية عالمياً"².

¹ إيمان بن سالم، جريمة التجنيد الإلكتروني للإرهاب وفقاً لقانون العقوبات الجزائري، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2018، ص21.

² سليمان الطعاني، المرجع السابق ص109.

خلاصة الفصل

يُمثل الإرهاب الإلكتروني نموذجاً متطوراً للجريمة المنظمة، حيث يتقاطع فيه الفكر المتطرف مع التقنيات الرقمية المتقدمة لتهديد السلم والسيادة الوطنية عبر الفضاء السيبراني. ويتميز هذا السلوك بطابعه العابر للحدود، وسهولة التخفي، وغياب العنف المادي المباشر، مما يتطلب تمييزه بدقة عن الجرائم المعلوماتية التقليدية والقرصنة العادية بالنظر إلى غايته السياسية أو التخريبية. ومن الناحية القانونية، تقوم هذه الجريمة على أركان ثلاثة؛ ركن شرعي يستند لنصوص التجريم، وركن مادي يتجسد في استخدام الحواسيب والشبكات للاعتداء، وركن معنوي يمثل القصد الجنائي الخاص بنشر الرعب. وتتنوع مظاهر هذا الإرهاب في البيئة الرقمية لتشمل عمليات التجسس السيبراني، وغسيل الأموال لدعم التنظيمات، والقصف الإلكتروني لتعطيل البنى التحتية الحيوية.

الفصل الثاني

الجهود الدولية والوطنية لمكافحة الإرهاب
الإلكتروني.

الفصل الثاني

الجهود الدولية والوطنية لمكافحة الإرهاب الإلكتروني.

تُمثل ظاهرة الإرهاب الإلكتروني النتيجة الحتمية لتقاطع الطفرة التكنولوجية المتسارعة مع الأيديولوجيات المتطرفة، حيث تحول الفضاء السيبراني المعاصر من بيئة لتدفق المعارف إلى ساحة حرب افتراضية عابرة للحدود تقتصر إلى الأبعاد الجغرافية التقليدية، وأمام هذا التهديد الوجودي المستحدث، الذي يستهدف البنى التحتية الحيوية والمصالح الاستراتيجية للدول، غداً واضحاً أن المقاربات الأمنية والتشريعية التقليدية المنفردة باتت قاصرة عن محاصرة الجناة أو تتبع أدلتهم الرقمية شديدة التطاير، وانطلاقاً من هذه الحتمية، تداعى المجتمع الدولي لصياغة استراتيجيات قانونية وإجرائية موحدة تهدف إلى ردم الفجوات التشريعية وتقييد الملاذات الآمنة، بيد أن نجاح هذه المنظومة لا يكتمل إلا بمدى استجابة التشريعات الوطنية وقدرتها على المواءمة بين تدابير الردع وصون الحقوق والحريات الأساسية.

وللإحاطة بأبعاد هذه المواجهة وتفكيك آلياتها، ينقسم هذا الفصل إلى مبحثين: ونستعرض فيه الجهود الدولية والإقليمية وآليات التعاون الإجرائي والقضائي والاتفاقيات المشتركة لمكافحة الإرهاب الرقمي وتطويقه (المبحث الأول) ومن جهة نحل فيه الأطر القانونية المقارنة لبعض الدول، مع التركيز على المنظومة التشريعية والإجرائية الجزائية ومقاربتها في حماية الفضاء السيبراني (المبحث الثاني)

المبحث الأول

الجهود الدولية والإقليمية لمكافحة الإرهاب الإلكتروني

لم تعد الظاهرة الإرهابية حبيسة ميادينها التقليدية، بل شهدت تحولاً جذرياً مع الطفرة الرقمية التي ميزت القرن الحادي والعشرين، حيث وجدت الجماعات المتطرفة في الفضاء

السيبراني بيئة خصبة للتخفي والتمويل والتجنيد واستهداف البنى التحتية الحيوية للدول دون التقيد بالحدود الجغرافية

وأمام هذه التهديدات المستحدثة، أدرك المجتمع الدولي عدم كفاية القوانين الوطنية المنفردة لمواجهة جريمة عابرة للحدود، مما فرض ضرورة تعزيز التعاون الدولي والإقليمي ووضع استراتيجيات قانونية مشتركة للتصدي لها، وتقوم هذه المقاربة على مسارين أساسيين: مسار عالمي تقوده الأمم المتحدة والاتفاقيات الدولية المتخصصة، ومسار إقليمي يهدف إلى مواءمة هذه الجهود مع المصالح الأمنية المشتركة للدول.

وبناءً على ذلك، يهدف هذا المبحث إلى دراسة التدابير الدولية المتخذة عالمياً لمكافحة الإرهاب الإلكتروني (المطلب الأول)، وتحليل دور الاتفاقيات والمنظمات الإقليمية في تعزيز الأمن السيبراني وملاحقة مرتكبي هذه الجرائم (المطلب الثاني).

المطلب الأول

الجهود الدولية لمكافحة الإرهاب الإلكتروني

أمام التوسع المتسارع للإرهاب الإلكتروني وما يطرحه من تهديدات عابرة للحدود، برزت الحاجة إلى تكاتف الجهود الدولية من أجل وضع إطار قانوني وتنظيمي يحد من مخاطر الفضاء الرقمي ويضمن أمنه. وقد تجسدت هذه الجهود من خلال إبرام العديد من الاتفاقيات الدولية (الفرع الأول) التي هدفت إلى تجريم الأفعال الإرهابية المعلوماتية وتعزيز التعاون القضائي والأمني بين الدول، إلى جانب الدور الفعّال الذي اضطلعت به المنظمات الدولية (الفرع الثاني)، وعلى رأسها منظمة الأمم المتحدة والمنظمات المتخصصة، في صياغة السياسات والاستراتيجيات الدولية لمكافحة هذا النمط المستحدث من الجرائم.

الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية

أدى تصاعد الإرهاب الإلكتروني إلى تحرك دولي مكثف لصياغة اتفاقيات قانونية تهدف إلى محاصرة التهديدات الرقمية العابرة للحدود وتجريم أشكالها، وتبرز في هذا الإطار

جهود محورية، تبدأ باتفاقية الأمم المتحدة لعام 2000 (أولاً)، التي وضعت أسس التنسيق العالمي لمواجهة إساءة استخدام التكنولوجيا، وصولاً إلى اتفاقية بودابست 2001 (ثانياً)، التي تُعد المرجع التشريعي الأبرز لتوحيد السياسات الجنائية الدولية ضد الجريمة المعلوماتية، تهدف هذه المنظومة القانونية إلى تعزيز التعاون الأمني والقضائي لضمان الملاحقة الفعالة للمجرمين مع مراعاة التوازن بين مكافحة الإرهاب وصون الحريات الفردية.

أولاً: اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55 لسنة 2000

تُعد الاتفاقية العالمية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، الصادرة عن الجمعية العامة للأمم المتحدة بموجب القرار رقم (55/63) في 12 أبريل 2000، وثيقة قانونية محورية جاءت استجابةً للتحديات الأمنية الناجمة عن الطفرة التكنولوجية، حيث شددت على ضرورة التنسيق الدولي لمواجهة الجرائم السيبرانية، مستلهمةً مبادئها من إعلان الألفية الذي دعا إلى تكاتف الجهود ضد الإرهاب والمخدرات والجريمة العابرة للحدود بكافة أبعادها، بما في ذلك الإرهاب الإلكتروني، مع الحرص على إتاحة منافع التكنولوجيا للجميع وفقاً لتوصيات المجلس الاقتصادي والاجتماعي لعام 2000،¹ وتأييداً لمؤتمر الأمم المتحدة الثامن لمنع الجريمة رقم (121/45) المؤرخ 14 ديسمبر 1990 الذي حث على مكافحة إساءة استخدام الحواسيب.²

وقد رسمت المادة 1 من هذه الاتفاقية معالم الاستراتيجية الدولية من خلال حزمة تدابير (أ-ي)، تُلزم الدول بتحديث تشريعاتها لضمان عدم توفير ملاذات آمنة للمجرمين، وتعزيز التعاون في مجالات التحقيق والمقاضاة، وتبادل الخبرات حول المشاكل التقنية والقانونية المستجدة، فضلاً عن تأهيل وتجهيز الكوادر الأمنية، وتفعيل آليات المساعدة المتبادلة لجمع

¹ . علي عدنان الفيل، الاجرام الالكتروني، ط1، مكتبة زين الحقوقية والأدبية، لبنان، 2011، ص 330.

² مؤتمر رقم 121/45 المؤرخ 14 ديسمبر 1990، نقلاً عن: عمر عباس، خضير العبيدي، الارهاب الالكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق جامعة تكريت، العراق، 2019، ص ص 47-48.

الأدلة الرقمية وتبادلها في الوقت المناسب، مع اشتراط إيجاد حلول توازن بين القدرة الحكومية على مكافحة وبين صون الحريات الفردية والخصوصية¹، وفي حين حثت المادة 2 على تبني هذه التدابير في السياسات الوطنية²، أقرت المادة 3 إدراج هذا الملف بصفة دائمة ضمن أجندة منع الجريمة والعدالة الجنائية؛ ورغم خلو نص الاتفاقية من تعريف صريح لمصطلح "الإرهاب الإلكتروني"، إلا أن نطاقها الشامل لمكافحة الجرائم المرتكبة عبر الإنترنت يستوعب بالضرورة الأفعال الإرهابية التي تندرج ضمن هذا الفضاء الرقمي³.

ثانياً: اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001

تمثل اتفاقية بودابست المحطة التشريعية الأولى والأبرز في مضمار مكافحة الجريمة الإلكترونية، فهي ورغم انطلاقها من البيئة الأوروبية، اكتسبت بُعداً دولياً بانضمام قوى عالمية كأمريكا وكندا وجنوب أفريقيا إلى جانب (21) دولة أوروبية، لتجسد بذلك المساعي الحثيثة لمجلس أوروبا والاتحاد الأوروبي في مجابهة الإرهاب الرقمي والجرائم المعلوماتية، وقد توجت هذه المساعي، التي استغرقت أربعة أعوام من التحضير، بتوقيع وزراء خارجية الدول الأعضاء في 5 نوفمبر 2001⁴.

استجابةً للتحديات والمخاوف المتزايدة من إساءة استخدام الفضاء السيبراني، ولضمان حماية فاعلة لسرية البيانات وسلامة الأنظمة الحاسوبية⁵.

وتشتمل الاتفاقية على (48) مادة قانونية تلزم الأطراف الموقعة بتسهيل تسليم المجرمين، وتبادل المساعدات القضائية لجمع الأدلة، واعتماد تشريعات وطنية متوافقة مع

¹ انظر المادة 1 من اتفاقية مكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية رقم 63/55 في 12/04/2000 الصادرة عن منظمة الأمم المتحدة، الجلسة العامة 81، 2000/12/04،

² انظر المادة 2 من اتفاقية مكافحة إساءة استعمال التكنولوجيا لأغراض إرهابية لسنة 2000.

³ انظر المادة 3 من اتفاقية مكافحة إساءة استعمال التكنولوجيا لأغراض إرهابية لسنة 2000.

⁴ اتفاقية بودابست المتعلقة بالجريمة المعلوماتية، المجلس الأوروبي، بودابست، بتاريخ 23 نوفمبر 2001.

⁵ عمر عباس، خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2019، ص 50.

أهدافها الرامية لصياغة سياسة جنائية موحدة تحمي المصالح والممتلكات عبر تعاون دولي وثيق¹، ومن حيث البناء الهيكلي، تتوزع مواد الاتفاقية على مقدمة وأربعة فصول، حيث استعرضت المقدمة المرجعيات الدولية السابقة والجهود الأممية والأوروبية المنجزة، بينما تولى الفصل الأول تحديد المفاهيم الفنية لنظم الحاسوب، وانصرف الفصل الثاني (المواد 2-22) لمعالجة الجوانب الموضوعية والإجرائية للجريمة، في حين خصص الفصل الثالث (المواد 23-35) للتعاون الدولي والاختصاص القضائي في الجرائم العابرة للحدود، وصولاً إلى الفصل الرابع (المواد 36-48) الذي تضمن الأحكام الختامية للاتفاقية.²

تُعد هذه الاتفاقية من المرجعيات القانونية الدولية التي دفعت الدول الأعضاء نحو تجريم طيف واسع من الأنشطة الإرهابية المرتكبة عبر الوسائط الإلكترونية، مُطالبةً إياها بدمج هذه الجرائم التي وصفتها بـ "غير المشروعة" ضمن قوانينها الوطنية، وقد صنفت الاتفاقية الجرائم المعلوماتية³ ضمن أربع مجموعات رئيسية هي:

المجموعة الأولى: الجرائم التي تنتهك أمن وحماية المعلومات الرقمية.

المجموعة الثانية: الجرائم المتصلة والمباشرة بجهاز الحاسوب.

المجموعة الثالثة: الجرائم المرتبطة بمحتوى البيانات والمواد المنشورة.

المجموعة الرابعة: جرائم الإرهاب الإلكتروني بكافة أشكالها.

1/ الأهداف والمواد القانونية لاتفاقية بودابست

وفقاً لما ورد في المذكرة التفسيرية لاتفاقية بودابست (8 فبراير 2001)، فإن الغاية الجوهرية من المواد (2 إلى 13) تكمن في تطوير وتحديث آليات الردع والمكافحة للجريمة

¹ نور الله تله، مرجع سابق، ص 155-156.

² عمر عباس، خضير عبيدي، المرجع نفسه، ص 50-51.

³ خالد حسين أحمد لوطفي، جرائم الأنترنت بين القرصة الإلكترونية والابتزاز الإلكتروني، ط1، دار الفكر الجامعي الإسكندرية، 2018، ص 54.

المعلوماتية. وفيما يخص الجانب المتصل بالإرهاب الإلكتروني، فقد تم تحديد الأفعال الجرمية وفق الآتي:

1. المادة (2): جرمتم الدخول أو الولوج غير المشروع للأنظمة.
2. المادة (3): تناولت جريمة الاعتراض غير القانوني للبيانات.
3. المادة (4) و(5): ركزت على الاعتداء على سلامة البيانات وسلامة الأنظمة المعلوماتية.
4. المادة (6): عالجت إساءة استخدام الأجهزة والتقنيات الحاسوبية.
5. المادة (7) و(8): جرمتا التزوير المعلوماتي والاحتيال المرتبط بالحاسوب.
6. المادة (10): اختصت بالانتهاكات الواقعة على حقوق الملكية الفكرية والحقوق المجاورة.
7. المادة (11) و(12): حددتا الأحكام المتعلقة بالشرع والاشتراك، ومسؤولية الأشخاص المعنوية (الشركات والمؤسسات).
8. المادة (13): أقرت الجزاءات والتدابير العقابية المفروضة على الجرائم المذكورة أعلاه.¹

2. البروتوكول الإضافي (ستراسبورغ 2003)

ارتبطت اتفاقية بودابست ببروتوكول إضافي صدر في 28 يناير 2003 (سلسلة المعاهدات الأوروبية رقم 189)، والذي ركز على تجريم الأفعال ذات الصبغة العنصرية أو المحرصة على كراهية الأجانب عبر الأنظمة الرقمية.

تكتسي المادة (6) من هذا البروتوكول أهمية خاصة، حيث وسعت نطاق التجريم ليشمل الأفعال التي تشكل جرائم دولية (مثل الإبادة الجماعية والجرائم ضد الإنسانية) كما حددها القانون الدولي وقرارات محكمة لندن العسكرية (1945) أو المحاكم الدولية المختصة، وبناءً

¹. عمر عباس، خضير عبيد، المرجع السابق، ص 57، 51.

عليه، فإن أي فعل يُرتكب عبر الوسائل الإلكترونية ويدخل ضمن هذا السياق مثل تجنيد الأطفال يُصنف كجريمة إرهاب إلكتروني تخضع للملاحقة القانونية وفقاً لهذه النصوص.¹

الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الدولية وآليات التعاون الدولي لمكافحتها

تعد ظاهرة الإرهاب الإلكتروني جريمة عابرة للحدود بطبيعتها، مما جعل من الجهود الوطنية المنفردة غير كافية لمحاصرتها، وفرض حتمية اللجوء إلى تعاون دولي مؤسساتي وإجرائي واسع. وانطلاقاً من هذا التحدي، سارعت المنظمات الدولية إلى وضع أطر تشريعية وسياسية تهدف إلى تجفيف منابع الإرهاب الرقمي وتأمين الفضاء السيبراني.

ولا يكتمل هذا الدور التنظيمي إلا بوجود آليات تعاون ميدانية فعالة، تربط بين أجهزة الشرطة والقضاء عالمياً، لضمان ملاحقة الجناة وتوثيق الأدلة الرقمية. وللإحاطة بهذا الموضوع، سنعرض في (أولاً) دور المنظمات الدولية والعالمية المتخصصة في هذا المجال، لننتقل في (ثانياً) إلى آليات التعاون الدولي بجانبها الإجرائي والقضائي.

أولاً: مكافحة الإرهاب الإلكتروني في المنظمات الدولية

تصدى المنظمات الدولية للإرهاب الإلكتروني عبر مسارين؛ مسار تقوده الأمم المتحدة ومجموعة الثماني، ومسار الاقتصادي والدولي تقوده المنظمات المتخصصة، بهدف وضع قواعد دولية موحدة تحكم الفضاء الرقمي وتجرم الاعتداء عليه.

1- منظمة الأمم المتحدة ومجموعة الدول الثمانية.

أ/ منظمة الأمم المتحدة

تبذل منظمة الأمم المتحدة جهوداً فاعلة ومستمرة في مجال مكافحة الإرهاب الإلكتروني، سعياً لمنع أي محاولات اعتداء تستهدف أمن الدول والأفراد عبر الفضاء الرقمي¹، وتتجلى هذه

¹ . ايهاب سمباطي، ترجمة الجديدة والكاملة، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست 2001) البروتوكول الملحق بها، دار النهضة، القاهرة، 2009، ص80.

الجهود من خلال سلسلة من المؤتمرات والقرارات التي وضعت الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة، وقد شكل المؤتمر السابع المنعقد في ميلانو عام 1980 انطلاقة جوهرية في هذا الشأن، حيث أكد على ضرورة الاستفادة من التطورات العلمية والتكنولوجية لمواجهة الجرائم المتعلقة بالحاسوب الآلي²، وتوالت هذه الجهود في المؤتمر التاسع بالقاهرة عام 1995 الذي شدد على وجوب التنسيق الدولي لحماية مخاطر التكنولوجيا، وصولاً إلى المؤتمر العاشر في بودابست الذي اعتبر جرائم الحاسوب نمطاً إجرامياً جديداً يستوجب الحد من أعمال القرصنة.

وفي إطار تعزيز الثقافة الأمنية الرقمية، أصدرت الجمعية العامة للأمم المتحدة القرار رقم (95/45) في 14 ديسمبر 1990 والمتعلق بحماية المعطيات الحساسة ومنع التمييز العنصري³، وتبعه في 12 أبريل 2000 التوقيع على اتفاقية خاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية⁴، كما شهد عام 2002 حراكاً تشريعياً مكثفاً،

حيث تم إقرار الدورة (285/56) في 31 جانفي لدعم استخدام التكنولوجيا من أجل التنمية⁵، تلاه قرار هام في 22 نوفمبر 2002 بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، وقرار آخر في ديسمبر من نفس العام يهدف إلى إرساء "ثقافة عالمية لأمن الفضاء الإلكتروني"، وهو من القرارات المحورية التي استهدفت حماية البنية التحتية الحيوية للمعلومات وحث الدول على تكثيف التعاون لمواجهة الإرهاب الإلكتروني⁶.

¹ . الي يوسف شكري، المنظمات الدولية، ط1، دار الصفاء للنشر والتوزيع، عمان، 2012، ص ص 97-98.

² مريم محمد حسن، تنظيم القانوني لجريمة التجسس المعلومات، رسالة ماجستير، كلية القانون جامعة الكوفة، العراق، 2016، ص162.

³ عمر عباس، خضير العبيدي، مرجع سابق، ص 67.

⁴ محروس نصر غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، العدد 24 الاصدار 9، العراق، 2011، نص 118.

⁵ نجيب بن عمر عوينات، الإرهاب الإلكتروني: مفهوم الجهود الدولية والاقليمية لمكافحةته، مجلة الأستاذ الباحث لدراسات قانونية والسياسية، معهد العالي للإعلامية الكاف جامعة جندوبية، تونس، العدد 6، ص ص 17-18.

⁶ سارة بوحادة، مداخلة حول الأثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية للعلوم السياسية، الجزائر، 2016، ص 13.

ولم تقتصر الجهود على القرارات العامة، بل شملت تقارير استراتيجية للأمانة العامة، ومن أبرزها تقرير عام 2006 المعنون بـ "الاتحاد في مواجهة الإرهاب: توصيات إستراتيجية عالمية لمكافحة الإرهاب"، حيث أفاد الأمين العام صراحة بأن قدرة الإرهابيين على جمع الأموال ونقلها، وحياسة الأسلحة، وتدريب الكوادر عبر الإنترنت، هي عناصر أساسية يجب مواجهتها بعمل دولي منسق يلتزم باحترام حقوق الإنسان والقانون الدولي¹، وفي سياق متصل، نبه مجلس الأمن في القرار رقم (1963) لعام 2010 والقرار رقم (2255) لعام 2015 إلى تزايد لجوء الإرهابيين للإنترنت لأغراض التجنيد، والتحريض، والتمويل، وتسيير الأعمال الإرهابية².

كما جسد مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية (سلفادور - البرازيل 2010)، الذي انعقد تحت عنوان "استراتيجيات شاملة لمواجهة تحديات عالمية"، تطور الرؤية الأممية من خلال وضع جرائم الإنترنت والتعاون الدولي لمكافحتها ضمن بنود جدول أعماله الرئيسية³.

ورغم أن ميثاق الأمم المتحدة لم ينص صراحة على تجريم استخدام المعلومات كأداة إرهابية، إلا أن روح الميثاق ومقاصده تعتبر هذا النوع من الإرهاب انتهاكاً لمبدأ عدم التهديد باستخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي للدول، ويندرج ضمن أعمال العدوان التي تهدد السلم والأمن الدوليين.

يمكن استنتاج أن استراتيجية الأمم المتحدة في مواجهة الإرهاب الإلكتروني قامت على ثلاثة محاور أساسية:

1. التنبيه من مخاطر الأنماط الإجرامية الجديدة وتنمية الوعي الدولي بحجم التهديدات الرقمية.

¹ . مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت لأغراض إرهابية، لتقرير المنشور على الموقع <https://www.unodc.org/>، تاريخ التصفح: 2026/04/12، الساعة 14:40، ص22.

² . نيف أحمد ضاحي شمري، عمر عباس، خضير العبيدي، جرائم الأمن السبراني وآليات مكافحته في إطار القانون الدولي، (1-5-90-9922-978) ISBN 978-9922-90-5-1، International Legal Issues Conferenc-ILIC2020، ص 406.

³ . عمر عباس، خضير العبيدي، مرجع سابق، ص69.

2. الموازنة بين ضمان حرية التعبير والتدفق الحر للمعلومات وبين ضرورة مراقبة الفضاء الرقمي لحفظ الأمن والسلم الدوليين.

3. وضع استراتيجيات علمية وعملية شاملة، وإرساء ثقافة عالمية لأمن الفضاء الإلكتروني، وتطوير أطر التعاون الدولي لمواجهة القرصنة والإرهاب الرقمي.

ب/مجموعة الدول الثمانية

بذلت مجموعة الدول الثماني (G-8) جهوداً حثيثة في مواجهة الإرهاب الإلكتروني عبر توظيف الإعلانات والمؤتمرات الدولية لتعزيز التعاون المشترك، مع التركيز على حماية الحريات والديمقراطية وحقوق الإنسان في الفضاء الرقمي، وفي هذا السياق، شهدت قمة المجموعة المنعقدة في 11 أكتوبر 2004 خطوة إجرائية هامة بإنشاء "الفريق الفرعي للجرائم الإرهابية الإلكترونية التقنية"، حيث اعتمد وزراء العدل والداخلية خلال اجتماعاتهم آلية شاملة للتصدي لجرائم الإنترنت، استندت إلى المبادئ الجوهرية التالية:

- التنسيق الدولي المكثف: التعاون بين كافة الدول لملاحقة مرتكبي الجرائم السيبرانية. ومحاكمتهم بغض النظر عن الموقع الجغرافي الذي وقع فيه الضرر.
- تقويض الملاذات الآمنة: العمل على ضمان عدم وجود بيئات تحمي المعتدين على تكنولوجيا المعلومات، بالتوازي مع تدريب وتأهيل الموظفين المكلفين بإنفاذ القوانين.
- الدعم التقني والمادي: توفير كافة المعدات والأدوات الضرورية لتمكين الجهات المختصة من التعامل بفعالية مع الجرائم ذات الصبغة التقنية العالمية.¹

واستكمالاً لهذا المسار، أصدرت المجموعة في عام 2005 بياناً أكدت فيه على جاهزية وكالات إنفاذ القانون للاستجابة السريعة للتهديدات الإرهابية الإلكترونية والحوادث الأمنية الجسيمة، وفي عام 2006، ناقش اجتماع المجموعة في "موسكو" قضايا الفضاء الإلكتروني (Cyberspace)، وأسفر عن "بيان موسكو" الذي شدد على أهمية التدابير الوقائية الاستباقية.

¹ . خالد حسن، أحمد لطفي، المرجع السابق، ص 159.

كما شهد اجتماع ميونخ في مايو 2007 اتفاقاً بين وزراء العدل والداخلية على تطوير أطر قانونية لتجريم استخدام الإنترنت لأغراض إرهابية. وبحلول عام 2009، التقى الوزراء في روما وأصدروا بياناً قُدم إلى مفوضية الأمم المتحدة لمنع الجريمة، حذروا فيه من أن التطور التقني أفرز مخاطر جديدة مثل إساءة استغلال الشبكات الاجتماعية وخدمات التشفير¹، وأخيراً جاء إعلان فرنسا عام 2011 ليؤكد في بنوده (من 4 إلى 22) على الدور الحيوي للإنترنت في نمو المجتمعات وتعزيز التعليم والحقوق، مع دعوة صريحة لتعزيز التعاون في كافة المحافل الدولية المعنية بحركة الإنترنت².

2/ المنظمات العالمية المتخصصة

أ/ منظمة التعاون الاقتصادي والتنمية

جهود المنظمة الدولية في مكافحة الجرائم المعلوماتية والإرهاب الإلكتروني تتبنى هذه المنظمة استراتيجية دولية رائدة تهدف إلى معالجة التحديات القانونية الناجمة عن استهداف المكونات التقنية، سواء كانت مادية (أجهزة الحاسوب) أو منطقية (البرمجيات والبيانات)، وينبثق هذا التوجه من رؤية المنظمة الرامية إلى دفع عجلة النمو الاقتصادي للدول الأعضاء، وضمان مواءمة الازدهار المادي مع التطور الاجتماعي ومن أبرز المحطات والوثائق الإرشادية حماية الخصوصية: يُعد "دليل حماية الخصوصية وقواعد تدفق البيانات" من أوائل المرجعيات التي أقرها مجلس المنظمة، مع حث الدول الأعضاء على تطبيقه كركيزة أساسية لمجابهة الإرهاب الإلكتروني، سعت المنظمة لضبط المصطلحات من خلال توزيع استبيانات على الأعضاء لتعريف "جرائم الحاسوب" بدقة، وتصنيف الأفعال التي تندرج تحت مظلة الإرهاب الرقمي، بما يضمن تكييف المعاهدات الدولية مع هذه الأنماط المستحدثة، تقرير باريس التاريخي (1983)

¹ مجمع البحوث والدراسات الأكاديمية للسلطات قابوس لعلوم الشرطة، الجريمة الإلكترونية، البحث الحائر على المركز الأول لمسابقة جائزة الأمير نايف عبد العزيز للبحوث الأمنية، عمان، 2016، ص ص 67-69.

² خالد حسن أحمد لطفي، المرجع السابق، ص 160.

عقدت المنظمة اجتماعاً مفصلياً في باريس لبحث مخاطر الإرهاب الإلكتروني¹، تمخض عنه تقرير شهير بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسات الجنائية وتضمن أيضاً قائمة الحد الأدنى وضع قائمة بالانتهاكات المعلوماتية الأساسية التي يتوجب على المجتمع الدولي "تجريمها" وفرض عقوبات رادعة بحق مرتكبيها لضمان الأمن الرقمي العالمي.

ب/ الاتحاد الدولي للاتصالات (ITU).

تأسست هذه المنظمة في أعقاب اتفاقية باريس عام (1865) تحت مسمى "اتحاد التلغراف الدولي"، ثم جرى تعديل تسميتها لتصبح الاتحاد الدولي للاتصالات السلكية واللاسلكية، وقد تعززت مكانتها بانضمامها إلى منظمة الأمم المتحدة كوكالة متخصصة في شؤون الاتصالات، لتتحول إلى المنصة الدولية الأبرز في هذا المجال، وتضم المنظمة في عضويتها (193 دولة) وأكثر من (482) عضواً من الشركات العالمية والقطاعات الصناعية الكبرى في المجالين العام والخاص.²

شهد عام 2005 انعقاد القمة العالمية لمجتمع المعلومات في تونس، والتي ركزت على حتمية التعاون الدولي لمواجهة الجرائم الإرهابية الإلكترونية، وقد أكدت القمة على الدور الجوهري للاتحاد في صياغة آلية متكاملة لتعزيز الثقة والأمن الرقمي، وهو ما تجسد في إطلاق "برنامج الأمن الإلكتروني العالمي"، يهدف هذا البرنامج إلى وضع استراتيجيات فعالة وحلول عملية لترسيخ الأمان في الفضاء المعلوماتي، مؤتمر قطر (2008) من أبرز خطوات الاتحاد تنظيم المؤتمر الدولي حول الأمن الإلكتروني بالتعاون مع مكتبه في دولة قطر، حيث وُجّهت دعوة عالمية لكافة الدول لصياغة وتنفيذ أطر قانونية للأمن السيبراني، حماية البنى التحتية شددت المنظمة على ضرورة تأمين البنية التحتية المعلوماتية الحيوية، باعتبارها الركيزة

¹ يونس عرب، جرائم الكمبيوتر والانترنت، ط1، اتحاد المصارف العربية، بيروت، 2002، ص322.

² . خليل حسين، التنظيم الدولي النظرية العامة والمنظمات العالمية، ط1، دار المنهل اللبناني، بيروت، 2010، ص 454.

الأساسية لمواجهة التحديات والمخاطر الناتجة عن الاندماج في عصر تكنولوجيا المعلومات والاتصالات.¹

ثانياً: آليات التعاون الدولي لمكافحة الإرهاب الإلكتروني

ضمان فعالية المواجهة، استحدث المجتمع الدولي آليات ميدانية تتجاوز الحدود الجغرافية؛ وتتنوع هذه الآليات بين تعاون إجرائي (أولاً) يهدف لجمع الأدلة وتبادل المعلومات، وتعاون قضائي (ثانياً) يركز على ملاحقة الجناة وتسليمهم لضمان عدم إفلاتهم من العقاب.

1/ آليات التعاون الاجرائي لمكافحة الإرهاب الإلكتروني

أ/ المساعدة المتبادلة بين أجهزة الشرطة الجنائية المختصة

يُعد التنسيق الأمني والتبادل المعلوماتي بين الأجهزة الشرطية المتخصصة ركيزة أساسية في إحباط المخططات الإرهابية العابرة للحدود، حيث يتم هذا التعاون عبر قنوات متعددة تشمل المنظمات الدولية، وفي مقدمتها "الإنتربول" الذي يركز جهوده على مكافحة الإرهاب الإلكتروني من خلال تحليل بيانات التواصل الاجتماعي لضبط الأدلة وتحديد مواقع الجناة، بالإضافة إلى التعاون ضمن الأطر الإقليمية والاتفاقيات الثنائية بين الدول²، ولا يقتصر هذا التكامل على الجانب المعلوماتي فحسب، بل يمتد ليشمل المساعدة القضائية المتبادلة التي تتيح للأجهزة الأمنية تنفيذ مهام بتكليف من السلطات القضائية، كالبحث عن المطلوبين وتنفيذ أوامر القبض الدولية³ وفي هذا الصدد، عزز القانون 04/09 هذا التوجه في مادته 16⁴، مؤكداً على إمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة الرقمية وكشف مرتكبي الجرائم المتصلة

¹ . عمر عباس العبيدي، مرجع السابق، ص 71.

² رمزي حوحو، التعاون الدولي لمكافحة جرائم الإرهاب، مجلة الحقوق والعلوم السياسية، المجلد 03، العدد 03، جامعة زيان عاشور بالجلفة، كلية الحقوق والعلوم السياسية ص 187.

³ المرجع نفسه، ص 188.

⁴ أنظر: المادة 16 من قانون رقم 04-09 السالف الذكر.

بتكنولوجيات الإعلام والاتصال، سواء نُفذت تلك الجرائم على أرض الواقع أو في الفضاء الإلكتروني.

ب/ تبادل المعلومات المتعلقة بالأشخاص و المنظمات الإرهابية

تُكرس الاتفاقيات الدولية المعنية بمكافحة الإرهاب التزاماً قانونياً على الدول الأعضاء بضرورة اتخاذ التدابير الوقائية اللازمة للحيلولة دون وقوع الجرائم الإرهابية، ويبرز "تبادل المعلومات" كأحد أهم هذه التدابير، خاصة تلك المتعلقة بهوية الجناة والمنظمات التي ينتمون إليها والإجراءات المتخذة حيالهم، ويهدف هذا التعاون المعلوماتي إلى تقويض المخططات الإرهابية وتضييق الخناق على التنظيمات النشطة؛ وهو ما أكدته الإعلان الخاص الصادر عن لجنة وزراء مجلس أوروبا عام 1978، والذي شدد على حتمية التزام الدول بمنح الأولوية لتطوير آليات الإخطار السريع وتبادل البيانات الشاملة حول الحوادث الإرهابية والظروف المحيطة بها، بما يضمن سرعة الاستجابة وفعالية الملاحقة القانونية لمرتكبيها¹.

ج/ تفعيل الإجراءات والتدابير الوقائية

يتجسد التعاون الدولي أيضاً في تبني حزمة من الإجراءات والتدابير الاحترازية المطبقة على مستوى المنافذ الحدودية، كالموانئ والمطارات، حيث يتم تكثيف عمليات الرقابة وفحص المسافرين وأمتعتهم للتحقق من طبيعة المحتويات، وفي هذا السياق، أُرست القرارات الصادرة عن الجمعية العامة للمنظمة الدولية للطيران المدني قواعد صارمة تحظر حمل الأسلحة من قبل الأفراد على متن الطائرات، كما منحت موظفي الأمن حيزاً قانونياً يسمح لهم بالتفتيش والاطلاع على جوازات السفر في أي وقت، لضمان التحقق الدقيق من هويات المسافرين وتأمين سلامة النقل الجوي².

¹ أحمد رفعت و صالح بكر الطيار، الارهاب الدولي، مركز الدراسات العربي الاوربي، سنة 1988 ص241

² بوعنادة فاطمة الزهراء، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، 2013، ص71.

الحفظ العاجل للبيانات المعلوماتية والأمر بتسليمها

يتمثل إجراء الحفظ العاجل للبيانات المعلوماتية في توجيه السلطة المختصة أمراً ملزماً لمزودي الخدمات بضرورة التحفظ المؤقت على بيانات رقمية معينة، سواء كانت مخزنة في حوزتهم أو خاضعة لسيطرتهم، وذلك ريثما يتم اتخاذ إجراءات قانونية لاحقة كالنقش أو الأمر بتقديم تلك البيانات. ويتسع نطاق هذا الإجراء ليشمل كافة أشكال المعلومات أو الصور أو الوسائط أو الأصوات التي تخضع لعمليات المعالجة والتخزين والنقل عبر الوسائل التقنية، بما في ذلك البيانات المتمثلة في الأرقام والرموز والأحرف، مما يضمن صون الأدلة الرقمية من التعديل أو الحذف وضمان جاهزيتها للاستخدام في المسار القضائي¹.

تفتيش المعلومات المخزنة

يعد تفتيش البيانات الرقمية المخزنة أو وسائط حفظها إجراءً جوهرياً لتعقب مرتكبي جرائم الإرهاب الإلكتروني واستقصاء الأدلة المتعلقة بها، حيث تستوجب الضرورة التحقيقية فحص المحتوى المعلوماتي، سواء بشكل كلي أو جزئي، ضمن الأطر التي تتيحها تقنيات المعلومات، ويشترط في تنفيذ هذا الإجراء الامتثال التام للمحددات القانونية المنظمة لعمليات التفتيش، مع الموازنة بين متطلبات العدالة وحماية حرمة الحياة الخاصة للأفراد، وفي هذا الإطار، أكدت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على إلزامية تفتيش المعلومات المخزنة كأداة قانونية فعالة لمواجهة هذا النوع من الجرائم المستحدثة².

2/ آليات التعاون القضائي لمكافحة الإرهاب الإلكتروني

أ/ تسليم المجرمين دولياً

تُعرف المعاهدة النموذجية الصادرة عن الجمعية العامة للأمم المتحدة بموجب القرار رقم 116/45 "تسليم المجرمين" بأنه إطار من الإجراءات القانونية الممنهجة، تهدف من خلاله

¹ بوعنادة فاطمة الزهراء، المرجع السابق، ص 71.

² أنظر المادة 02 من الاتفاقية العربية لمكافحة تقنيات المعلومات، القاهرة، المصادق عليها بموجب المرسوم الرئاسي رقم 86-14 مؤرخ في 20 فيفري 2014، ج ر عدد 11 مؤرخة في 26 فيفري 2014.

دولة ما إلى نقل شخص متهم أو محكوم عليه إلى سلطات دولة أخرى، وذلك لتمكينها من مقاضاته جنائياً أو تنفيذ حكم قضائي صدر بحقه مسبقاً¹، وفي إطار التعاون الإقليمي، ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأعضاء بتسليم مرتكبي الجرائم المعلوماتية، بما في ذلك المتورطين في أعمال الإرهاب الإلكتروني، ومع ذلك، أجازت الاتفاقية للدول الامتناع عن تسليم مواطنيها، مقابل التزام تلك الدول بمباشرة الملاحقة القضائية ضدهم داخلياً عن الجرائم الإلكترونية التي اقترفوها في حق دول أخرى²، وعلى صعيد التشريع الوطني، وسّعت المادة 15 من القانون الجزائري رقم 09/04 من نطاق الولاية القضائية للمحاكم الجزائرية، حيث منحتها الاختصاص الحصري للنظر في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال حتى وإن ارتكبت خارج الإقليم الوطني، شريطة أن يكون الفاعل أجنبياً وأن تستهدف الجريمة مؤسسات الدولة، أو مرافق الدفاع الوطني، أو المصالح الاقتصادية الاستراتيجية للجزائر³.

ب/ نقل الإجراءات

يُقصد بنقل الإجراءات اضطلاع إحدى الدول بمباشرة التدابير الجنائية المتعلقة بجريمة ما داخل إقليم دولة أخرى ولصالحها بناءً على سند اتفاقي، وهو إجراء مشروط بضرورة أن يشكل الفعل المنسوب للجاني جريمة معترفاً بها في تشريعات كل من الدولة الطالبة والمطلوب منها على حد سواء، مع وجوب كون الإجراءات المراد تنفيذها مقررّة قانوناً في نظام الدولة المطلوب منها بخصوص ذات الجريمة، فضلاً عن اشتراط فاعلية هذا الإجراء في الوصول إلى الحقيقة، خاصة في الحالات التي تتوفر فيها أدلة الإثبات ضمن نطاق اختصاص الدولة المطلوب منها التنفيذ⁴.

¹ قرار رقم 45/116، الجمعية العامة للأمم المتحدة، مؤرخ في 14 ديسمبر 1990، المتعلق بتسليم المجرمين.

² الاتفاقية العربية لمكافحة تقنيات المعلومات، المرجع السابق.

³ انظر المادة 15 من القانون رقم 09-04، السالف الذكر.

⁴ رمزي حوحو، المرجع السابق، ص 189.

ج/ المساعدة القضائية الدولية

تُمثل المساعدة القضائية كل إجراء قانوني يستهدف تيسير ممارسة الاختصاص القضائي لدولة ما بصدد جريمة ارتكبت في دولة أخرى، وهو ما جعل أغلب الاتفاقيات الدولية المعنية بمكافحة الإرهاب تدرج نصوصاً تقضي بضرورة اللجوء إلى هذا النوع من التعاون بين الدول المتعاقدة؛ بغية تحقيق أقصى درجات الفعالية والسرعة في إجراءات ملاحقة الإرهابيين ومعاقبته، استناداً إلى المصلحة المشتركة في مواجهة الأعمال الإرهابية، وتتجسد صور هذه المساعدة في تبادل المعلومات والوثائق التي تطلبها السلطات القضائية الأجنبية حول اتهامات وُجّهت لرعاياها أو إجراءات اتُخذت ضدهم، بالإضافة إلى تبادل البيانات المتعلقة بالسوابق القضائية للجناة، بما يُمكن الجهات المختصة من الوقوف بدقة على الماضي الجنائي للفرد المُحال إليها¹.

تتطلب المواجهة الفعّالة للإرهاب الإلكتروني ارتكازاً وثيقاً على منظومة من المعايير الدولية الأساسية؛ وفي مقدمتها الالتزام المطلق بقواعد القانون الدولي ومبادئه المستقرة، مع ضرورة إيجاد إجماع عالمي يرفض ويُدين كافة أشكال الإرهاب وصوره، وبخاصة الإرهاب الإلكتروني، ويستلزم ذلك تعزيز أطر التعاون الدولي في مجال تبادل المعلومات المتعلقة بالظواهر الإرهابية، وضمان تفعيل مبدأ المسؤولية الجنائية بحق الجناة السيبرانيين، مع السعي المستمر لتطوير ورفع كفاءة إجراءات مكافحة الإرهاب الرقمي لضمان ردعه وتطويقه².

وتبرز إشكالية الاختصاص القضائي في الجرائم الإرهابية كأحد أهم التحديات القانونية، خاصة في الحالات التي تمتع فيها الدولة المطلوب إليها التسليم عن تسليم مرتكبي الجرائم. وهنا تفرض الاتفاقيات الدولية قاعدة قانونية صارمة تقوم على مبدأ "إما التسليم أو المحاكمة"؛

¹ المرجع نفسه، ص191.

² ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد 8، العدد 1، 2021، ص42.

إذ يتعين على الدولة التي ترفض التسليم أن تتولى بنفسها محاكمة الفاعل عما اقترفه، وذلك لضمان عدم إفلات المجرمين من العقاب تحت أي ذريعة قانونية أو سيادية.

وفي هذا السياق، تضطلع المنظمات الدولية بدور محوري عبر إصدار توصيات تُلزم الدول بتقديم المساعدة القضائية المتبادلة لقمع الجرائم الإرهابية، مع حثّها على إزالة العوائق القانونية في تشريعاتها الوطنية التي قد تحول دون المحاكمة أو التسليم، وبناءً على ذلك، يمثل "الاختصاص القضائي العالمي" اليوم الركيزة الأساسية للتصدي للإرهاب عموماً والإلكتروني خصوصاً، كونه يجسد الصورة المثلى للتعاون القضائي والتكامل التشريعي بين دول العالم¹.

المطلب الثاني

اتفاقيات والمنظمات الإقليمية في مكافحة الإرهاب الإلكتروني

يشهد العالم المعاصر تحولاً جذرياً في أنماط الصراع والجريمة، حيث لم تعد الميادين التقليدية هي الساحة الوحيدة للمواجهات، بل انتقل الثقل الإجرامي إلى "الفضاء السيبراني" الذي وفر للجماعات الإرهابية بيئة خصبة للعمل بعيداً عن الرقابة المباشرة. وقد أفرز هذا التحول ما يُعرف بـ "الإرهاب الإلكتروني"، وهو نمط مستحدث من الإرهاب يتخذ من الوسائل التقنية والشبكات المعلوماتية أداة لترويع المجتمعات، وتدمير البنى التحتية الحيوية، واختراق الأمن القومي للدول.

ونظراً للطبيعة العابرة للحدود لهذه الجرائم، حيث يمكن لمنفذ الهجوم أن يتواجد في قارة بينما تقع النتائج الجرمية في قارة أخرى، أدرك المجتمع الدولي أن القوانين الوطنية القاصرة لا تكفي وحدها لردع هذا الخطر، من هنا برزت أهمية المقاربات الإقليمية كحلقة وصل حيوية بين التشريعات المحلية والاتفاقيات الدولية الشاملة.

¹ رمزي حوحو، المرجع السابق، ص 191.

تأتي أهمية دراسة الاتفاقيات والمنظمات الإقليمية في مكافحة الإرهاب الإلكتروني من كونها تعكس إرادة سياسية وقانونية موحدة لمجموعة من الدول التي تجمعها روابط جغرافية ومصالح أمنية مشتركة، وبهذا سنتطرق إلى الاتفاقيات الإقليمية لمكافحة الإرهاب الإلكتروني (الفرع الأول)، والمنظمات الإقليمية لمكافحة الإرهاب الإلكتروني (الفرع الثاني).

الفرع الأول : الاتفاقيات الإقليمية لمكافحة الإرهاب الإلكتروني

في ظل الطفرة الرقمية الهائلة التي يشهدها القرن الحادي والعشرون، انتقلت الظاهرة الإرهابية من ميادينها التقليدية إلى الفضاء السيبراني الواسع، مستغلةً خصائص الشبكة العنكبوتية في التخفي، وسرعة الانتشار، وتجاوز الحدود الجغرافية، هذا التحول النوعي جعل من "الإرهاب الإلكتروني" تهديداً وجودياً للأمن القومي للدول وللاستقرار الدولي على حد سواء. ونظراً لقصور التشريعات الوطنية المنفردة عن محاصرة هذه الجرائم العابرة للحدود، برزت الحاجة الماسة إلى صياغة أطر قانونية موحدة على الصعيد الإقليمي، وتعد هذه الاتفاقيات، اتفاقية الاتحاد الأفريقي لعام 2014 (أولا)، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات (ثانياً).

أولاً: اتفاقية الاتحاد الأفريقي لسنة 2014

أقرت هذه الاتفاقية بمباركة رؤساء دول وحكومات الاتحاد الأفريقي (AU)، ودخلت طور التنفيذ الفعلي عقب تصديق 15 دولة عضو عليها، تهدف الاتفاقية بشكل أساسي إلى إرساء إطار قانوني لمواجهة التحديات الرقمية المتنامية في القارة، بما يشمل تنظيم التجارة الإلكترونية، وحماية البيانات الشخصية، ومكافحة الجرائم الإرهابية الإلكترونية، وتعزيز الأمن السيبراني، حيث تمنح الدول الأعضاء الصلاحية لسن تشريعات وطنية رادعة للإرهاب الإلكتروني¹.

¹ دار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطر التعامل الإلكتروني، دراسة مقارنة، أطروحة الدكتوراه، كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017، ص ص 285-286.

وفيما يخص الحقوق والواجبات، تضمنت المادة (18) نصوصاً صريحة لحماية أصحاب البيانات، مؤكدة على حقهم في الإخطار المسبق قبل مشاركة معلوماتهم مع أي أطراف ثالثة، كما ربطت المادة (25/3) بين الأمن السيبراني وحقوق الإنسان، ملزمة الحكومات بضمان توافق سياساتها الأمنية مع الميثاق الأفريقي لحقوق الإنسان والشعوب، لاسيما فيما يتعلق بحرية التعبير، والحق في الخصوصية، وضمان المحاكمة العادلة.

علاوة على ذلك، ركزت المادة (26/1) على نشر الثقافة المجتمعية بالأمن السيبراني، بينما سعت المادة (28/2) لترسيخ سيادة القانون في الفضاء الرقمي، ولم يقتصر الأمر على الجوانب التشريعية الداخلية، بل حثت الاتفاقية الدول على توقيع معاهدات المساعدة القانونية المتبادلة لضمان تبادل البيانات وفق المعايير الدولية، كما اتخذت موقفاً حازماً بحظر استخدام الأنظمة الحاسوبية للإساءة للأفراد بناءً على العرق، أو الدين، أو الأصل القومي، أو الانتماء السياسي. وبموجب المادة (15)، يتعين على الدول الأعضاء (البالغ عددها 54 دولة) الإشارة إلى هذه الاتفاقية في أحكامها واعتماد القوانين المنفذة لها على المستوى الوطني¹.

ثانياً: الاتفاقية العربية لمكافحة الإرهاب الإلكتروني

1- الاتفاقية العربية لمكافحة جرائم التكنولوجيا المعلومات لعام 2010

تكللت الجهود العربية في مضمار مكافحة الإرهاب الرقمي بإبرام "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" أواخر عام 2010، والتي جاءت لتعزيز التنسيق المشترك في مواجهة الجرائم الإرهابية الإلكترونية. وتتألف هذه الاتفاقية من 43 مادة قانونية، خُصصت 21 مادة منها لتحديد الجرائم (الأحكام الموضوعية)، بينما تناولت 8 مواد الجوانب الإجرائية المتعلقة بصلاحيات السلطات في التتبع وجمع المعلومات وضبط المحتويات الرقمية المخزنة، بالإضافة إلى 14 مادة في الفصل الرابع تعنى بتنظيم التعاون الدولي وتبادل المعلومات بين

¹ دار نسيمه المرجع السابق، ص ص288-289.

الدول الأعضاء ضمن نطاق إقليمي محدد¹، وقد شملت الاتفاقية تجريم باقة واسعة من الأفعال، كالاختراق، والاعتراض، والاعتداء على سلامة البيانات والملكية الفكرية، والتزوير والاحتيال، فضلاً عن الجرائم المتعلقة بالإرهاب الإلكتروني، وغسل الأموال، والاتجار بالبشر والأسلحة، مع تشديد العقوبات على الجرائم التقنية المرتكبة².

وفي تفصيل أعمق للمواد القانونية، نصت المادة (11) على تجريم إلحاق الضرر بالمستخدمين عمداً أو الاحتيال عليهم، كما حظرت الأنشطة المتعلقة بالمحتوى الإباحي والتحريض على الدعارة، والاعتداء على خصوصية الأفراد أو التشهير بهم عبر الوسائل التقنية³، ومن جانب آخر ركزت المادة (10) على مكافحة الإرهاب الإلكتروني، حيث جرّمت نشر أفكار الجماعات الإرهابية، وتمويل عملياتها، وتسهيل الاتصالات بين تنظيماتها، بالإضافة إلى حظر نشر طرق صناعة المتفجرات أو التحريض على الفتن والنعرات والاعتداء على الأديان والمعتقدات⁴.

2- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات (2004)

توجت الدول العربية جهودها لمواكبة التحولات التكنولوجية والمعلوماتية المتسارعة بإصدار إطار قانوني موحد عُرف باسم "القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام 2004"، وقد جاء هذا القانون نتاج تعاون بين الأجهزة العربية المشتركة، حيث اعتمدته جامعة الدول العربية من خلال الأمانة الفنية لمجلس وزراء العدل العرب بموجب القرار رقم (495 / د 19 - 2003/10/8)، كما تمت المصادقة عليه من قبل

¹ صفاء كاظم، غازي الجياشي، جريمة قرصنة البريد، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة بابل، العراق، 2016، ص46.

² رامي متولي، المرجع السابق، ص75.

³ رامي متولي، مرجع سابق، ص 76.

⁴ رامي متولي، مرجع سابق، ص ص76،77.

مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (418/د21/2004)، ويتألف هذا البناء التشريعي من 27 مادة قانونية¹.

ويحدد هذا القانون مجموعة من الأفعال التي تُجرم قانوناً، بل ويذهب إلى تصنيفها ضمن جرائم "الإرهاب الإلكتروني" في حال مست مصالح محمية بموجب القانون. وتشمل هذه الجرائم الدخول غير المشروع للأنظمة بقصد العبث بالبيانات، سواء بالإلغاء أو الحذف أو التدمير أو التغيير، أو إعادة نشر المعلومات الشخصية²، كما يجرم القانون التعطيل المتعمد للشبكات المعلوماتية أو أجهزة الحاسوب، ومنع الوصول إلى الخدمات أو مصادر البيانات والمعلومات بأي وسيلة كانت³.

وتمتد الحماية القانونية لتشمل مكافحة الابتزاز والتهديد الإلكتروني، حيث يُجرم استخدام الشبكة لحمل الأشخاص على القيام بفعل أو الامتناع عنه، حتى وإن كان ذلك الفعل مشروعاً في أصله⁴، وفي سياق حماية الأموال، يمنع القانون الوصول غير المصرح به لأرقام وبيانات البطاقات الائتمانية وما يماثلها بقصد الاستيلاء على بيانات أو أموال الغير⁵، كما يتصدى القانون للممارسات التي تمس النظام العام أو الآداب العامة، مجزماً إنتاج أو إرسال أو تخزين أي محتوى يخالف هذه القيم عبر الوسائط التقنية⁶.

و فيما يتعلق بالجرائم الجسيمة العابرة للحدود، يفرض القانون رقابة صارمة على إنشاء المواقع الإلكترونية التي تهدف إلى تسهيل الاتجار بالبشر،

¹ محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت والأحكام الموضوعية والأحكام الجزائية، ط1، منشورات حلي الحقوقية، بيروت، 2011، ص 125.

² أنظر المادة 3 من القانون العربي الاسترشادي لمكافحة الجرائم التقنية، أنظمة المعلومات وما في حكمها، صادر عن الأمانة العامة لجامعة الدول العربية (القرار 2004/417).

³ انظر المادة 7 من القانون نفسه.

⁴ انظر المادة 9 من القانون العربي الاسترشادي لمكافحة الجرائم التقنية، السالف الذكر.

⁵ انظر المادة 10 من القانون نفسه.

⁶ انظر المادة 13 من القانون نفسه.

أو تلك التي تتبع لجماعات إرهابية¹، و يشمل ذلك المواقع التي تنتشر خلف مسميات تموهية لتسهيل التواصل بين القيادات الإرهابية، أو تمويلها، أو نشر الفكر المتطرف، أو تداول طرق تصنيع المتفجرات²، وأخيراً يشدد القانون العقوبة على الاختراق العمدي للمواقع والأنظمة الذي يستهدف الحصول على معلومات تمس الأمن القومي للدولة أو اقتصادها الوطني، أو يهدف إلى تدمير تلك البيانات وبث أفكار تضر بالأمن الداخلي أو الخارجي.³

الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الإقليمية

رغم تأخر التشريعات العربية والإقليمية في ملاحقة التطور العالمي لجرائم الحاسوب، إلا أن السوق الأوروبية المشتركة قادت دوراً ريادياً في المكافحة، حيث أصدر البرلمان الأوروبي قرارات مفصلية، أبرزها قرار 8/4/1979 الهادف لحماية الأفراد من تداعيات التطور المعلوماتي، سعياً لتحسين الفضاء الرقمي ضد الإرهاب الإلكتروني.⁴

يُمثل الإرهاب الإلكتروني أحد أخطر التحديات العابرة للحدود التي تواجه المجتمع الدولي في العصر الرقمي، إذ لم تعد العمليات الإرهابية تقتصر على الوسائل التقليدية، بل امتدت لتستهدف البنية التحتية المعلوماتية للدول، وخصوصية الأفراد، والأمن القومي عبر الفضاء السيبراني، وأمام هذه التهديدات المتنامية، أدركت المنظمات الإقليمية أن المواجهة الفردية من قبل الدول لم تعد كافية، مما استوجب صياغة استراتيجيات تعاونية وأطر قانونية موحدة.

وتتجلى هذه الجهود في مسارين متوازيين، يقود الاتحاد الأوروبي الذي وضع حجر الأساس للتشريعات الدولية (أولاً)، سعياً منه لخلق توازن دقيق بين الحماية الجنائية وصون الحريات الأساسية، وفي المقابل، تبرز جهود جامعة الدول العربية (ثانياً) التي سعت رغم التحديات

¹ انظر المادة 17 من القانون العربي الاسترشادي لمكافحة الجرائم التقنية، السالف الذكر.

² انظر المادة 21 من القانون نفسه.

³ انظر المادة 32 من القانون نفسه.

⁴ وليد الزبيدي، القرصنة على الانترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة لنشر والتوزيع، الأردن، 2003، ص128.

التشريعية والتقنية، إلى مواءمة نصوص ميثاقها وتطوير قوانين استرشادية واتفاقيات مشتركة تهدف إلى تحصين السيادة الرقمية العربية وملاحقة الأنماط المستحدثة للجرائم التقنية.

أولاً: الاتحاد الأوروبي في مكافحة الإرهاب الإلكتروني

تبنى الاتحاد الأوروبي استراتيجية استباقية لمكافحة الجرائم الإرهابية الإلكترونية بكافة أشكالها، حيث تجسدت هذه الجهود مبكراً في عام (1981) بتوقيع اتفاقية حماية الأشخاص تجاه المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية، تلاها خطوة محورية في عام (1985) بوضع قواعد إرشادية متخصصة لتحديد أنماط جرائم الحاسوب، وقد هدفت هذه القواعد إلى تنبيه المشرعين لضرورة صياغة نصوص قانونية تجرم الأنشطة غير المشروعة المرتبطة بالتقنية، مع التشديد على معادلة صعبة توازن بين متطلبات الحماية الجنائية الفعالة وبين صون الحق في المعلومات وحماية حريات الأفراد الأساسية من أي تعسف¹.

عزز الاتحاد الأوروبي منظومته القانونية عام (1989) بإصدار توصيات خاصة بالجرائم الإرهابية الإلكترونية أقرتها لجنة وزراء المجلس الأوروبي، حيث حددت هذه التوصيات "الحد الأدنى" من الأنشطة غير المشروعة المتعلقة بالحاسوب الواجب تجريمها، داعيةً الدول الأعضاء إلى توحيد جهودها التشريعية لمحاصرة هذه الأنماط المستحدثة من الأنشطة الإجرامية وضمان ملاحقتها قانونياً².

حدد الاتحاد الأوروبي قائمة من الأنشطة الواجب تجريمها شملت التواصل غير المرخص وتجاوز التدابير الأمنية، و"غش وتزوير الحاسوب"، وإعادة إنتاج البرامج دون إذن، متبوعاً بتشكيل لجان خبراء لتعزيز الحماية الإجرائية والموضوعية، وقد توجت هذه الجهود باجتماع "ستراسبورغ" عام (2000) الذي دعا لتجريم إتلاف البيانات والاحتتيال الرقمي، وصولاً

¹ صغير يوسف، الجرائم المرتكبة عبر الأنترنت، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري، الجزائر، 2013، ص101.

² مريم محمد حسن، المرجع السابق، ص169.

إلى الإصدار التاريخي لـ (اتفاقية بودابست عام 2001) كإطار قانوني عالمي يضمن العقوبات الرادعة وتعزيز (التعاون الدولي) وتبادل المعلومات لتحقيق الأمن الإلكتروني الشامل¹.

تجلت الجهود الأوروبية في هذا الصدد من خلال العناية البالغة التي أولتها لجنة وزراء الاتحاد الأوروبي لمواجهة معضلات الإرهاب الإلكتروني، حيث ركزت في سلسلة من توصياتها على حث الدول الأعضاء نحو تبني استراتيجيات موحدة تعزز من آليات الفهم المتبادل والتعاون المشترك في التصدي لهذه الجرائم، ومن أبرز هذه التوجيهات، التوصية رقم (10/85) المعنية بالتطبيق الفعلي للاتفاقية الأوروبية للمساعدة المتبادلة في الشؤون الجنائية، ولاسيما ما يتصل بالإنبات القضائية واعتراض الاتصالات السلكية واللاسلكية، والتوصية رقم (2/88) التي استهدفت مكافحة القرصنة في حقوق التأليف والنشر والحقوق المجاورة، كما تضمنت هذه الجهود التوصية رقم (15/87) التي وضعت ضوابط لاستخدام البيانات الشخصية في العمل الشرطي، والتوصية رقم (4/95) الهادفة لحماية الخصوصية في خدمات الاتصالات، وبشكل أخص الخدمات الهاتفية، وإضافة إلى ذلك، برزت التوصية رقم (9/89) كإطار إرشادي للمشرعين الوطنيين في صياغة تعريفات دقيقة لجرائم الحاسوب، وصولاً إلى التوصية رقم (13/95) التي عالجت الإشكالات القانونية في قانون الإجراءات الجنائية المرتبطة بتقنيات المعلومات الحديثة.²

وعلى صعيد متصل، برزت المساعي الأوروبية الرامية لمجابهة الإرهاب الإلكتروني من خلال قرارات مؤتمرات وزراء العدل، ومنها القرار الصادر عن المؤتمر الحادي والعشرين المنعقد في "براغ" عام 1997، والذي وجه دعوة للجنة الوزراء بضرورة مساندة أعمال اللجنة الأوروبية في تقريب القوانين الجنائية الوطنية لتوحيد الرؤية القانونية ضد الجرائم الإرهابية الرقمية؛ وهو ما أسهم بشكل مباشر في إتاحة توظيف أدوات تقنية متطورة في عمليات البحث والتحري. كما تواصلت هذه الجهود في مؤتمر وزراء العدل المنعقد في لندن عام 2000، والذي

¹ خالد حسن لطفي، المرجع السابق، ص 176.

² رامي متولي المرجع السابق، ص 75.

شدد على حث الدول الأوروبية لمواصلة العمل على تذليل العقبات القانونية أمام الانضمام لاتفاقية "بودابست" لعام 2001، مع التأكيد على حتمية التعاون الدولي كركيزة أساسية وشاملة لمكافحة تهديدات الإرهاب الإلكتروني.¹

ثانياً: جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني

اضطلعت جامعة الدول العربية، بصفتها منظمة إقليمية، بدور بارز في مواجهة الأنشطة غير المشروعة المرتبطة بتقنية المعلومات، فبالرغم من خلو ميثاقها من نص صريح يتناول مكافحة الإرهاب الرقمي وتفرعاته، إلا أن المادة الثانية منه حددت مقاصد المنظمة في تعزيز التعاون لحماية استقلال الدول وسيادتها، وهو ما يتماشى موضوعياً مع ضرورة التصدي للإرهاب الإلكتروني الذي ينتهك سيادة الدول عبر اختراق نظم المعلومات السيادية واستغلال البيانات الحساسة ضد المصالح العربية، وفي هذا السياق منحت المادة الثالثة من الميثاق مجلس الجامعة صلاحية إقرار آليات التعاون مع الهيئات الدولية المعنية بحفظ الأمن والسلم، مما يعزز التوجه نحو مكافحة هذه التهديدات، حيث يُصنف الاعتداء على الأنظمة المعلوماتية الرسمية أو محاولة تخريبها وبث الرعب والتحريض ضد الأنظمة القائمة عبر الفضاء الرقمي كصورة من صور العدوان التي تجرمها قواعد القانون الدولي وميثاق الأمم المتحدة.²

تبلورت جهود الجامعة العربية في مكافحة الجرائم التقنية بصدور قرار مجلس وزراء العدل العرب رقم (229 لسنة 1999)، الذي اعتمد "القانون الجزائي العربي الموحد" كنموذج استرشادي، ويُعد هذا القانون من أهم الركائز العربية لمواجهة الإرهاب الإلكتروني، خاصة لتخصيصه فصلاً كاملاً يعالج الانتهاكات المعلوماتية الموجهة ضد حقوق الأفراد.³

¹ رشيد صبحي جاسم محمد، الارهاب والقانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة بغداد، العراق، 2003، ص208.

² خالد حسن لطفي، مرجع سابق، ص177.

³ عمر عباس، خضير العبيدي، المرجع السابق، ص80.

تستمر المساعي العربية الحثيثة لسد الفجوة التشريعية في القوانين الجنائية القائمة ومواجهة الجرائم المستحدثة، حيث كرست جامعة الدول العربية الاجتماع الثاني عشر للجنة الجرائم المستحدثة عام 2009 لمناقشة قضية "تزوير بطاقات الائتمان"، وفي سياق متصل، صاغت الأمانة العامة مشروع اتفاقية عربية لمكافحة جرائم الحاسوب تنفيذًا لتوصيات سابقة، وعكفت لجنة مشتركة من مجلسي وزراء الداخلية والعدل العرب على عقد اجتماعات متتالية لصياغة المشروع في صورته النهائية بناءً على مرئيات الدول الأعضاء، إلا أن هذه الجهود لم تُقضى حتى الآن إلى الاعتماد الرسمي لهذه الاتفاقية.¹

¹ رامي متولي، مرجع سابق، ص ص 74-75.

المبحث الثاني

الجهود الوطنية لمكافحة الإرهاب الإلكتروني

أحدثت الطفرة التكنولوجية تحولاً جذرياً في بنية المجتمعات، لكنها أفرزت في المقابل ظاهرة "الإرهاب الإلكتروني" كأحد أعقد التهديدات المستحدثة، حيث استغلت الجماعات المتطرفة الفضاء السيبراني العابر للحدود لبث أفكارها، وتمويل أنشطتها، واستهداف البنى التحتية الحيوية، وأمام هذه الطبيعة الرقمية العسيرة على الملاحقة بالوسائل التقليدية، وجدت النظم القانونية نفسها أمام حتمية تطوير ترسانتها التشريعية والإجرائية لضمان الردع الأمني دون المساس بالحقوق والحريات الدستورية.

وتأسيساً على ذلك، يسلط هذا المبحث الضوء على الجهود الوطنية لمكافحة الإرهاب الإلكتروني من خلال محورين، يتناول الأول الأطر القانونية المقارنة لبعض الدول العربية والغربية (المطلب الأول) للوقوف على استراتيجياتها التشريعية والرقابية، بينما يركز المحور الثاني على جهود الجزائر في مكافحة الإرهاب الإلكتروني (المطلب الثاني)، مستعرضاً التدابير الموضوعية لتجريم هذه الأفعال، والآليات الإجرائية العامة والخاصة التي أقرها المشرع الجزائري للبحث والتحري عن الجريمة الرقمية.

المطلب الأول

الأطر القانونية لمواجهة الإرهاب الإلكتروني في بعض الدول العربية والغربية

فرض التطور التكنولوجي المتسارع نمطاً مستحدثاً من التهديدات يُعرف بـ "الإرهاب الإلكتروني"، حيث تمكنت الجماعات المتطرفة من استغلال الفضاء السيبراني وتحويله إلى ساحة لترويج الأفكار الهدامة، وتمويل الأنشطة الإجرامية، وشن هجمات رقمية تستهدف البنى التحتية للدول. هذا التحول من الإرهاب المادي إلى الرقمي العابر للحدود كشف عن عجز القوانين العقابية التقليدية عن ملاحقة الجريمة المعلوماتية، مما أوجد ضرورة ملحة لتحديث

الترسانات التشريعية وإيجاد نصوص مرنة واستباقية قادرة على ردع هذا الخطر وتأمين الأمن القومي الرقمي.

وللوقوف على نجاعة هذه المواجهة التشريعية وفلسفتها، يحل هذا المطلب الأثر القانوني والأمنية المعتمدة في بيئتين قانونيتين متميزتين من خلال فرعين رئيسيين : في الدول العربية (الفرع الأول) و الدول الغربية (الفرع الثاني).

الفرع الأول: في الدول العربية

حرصت التشريعات العربية على مجابهة التحديات الرقمية عبر استحداث أطر قانونية متطورة، تجسدت في نماذج فاعلة كالتجربة الأردنية (أولاً) في مكافحة الإرهاب الإلكتروني، والتجربة المصرية (ثانياً) التي ركزت على تحصين الفضاء المعلوماتي دستورياً وقانونياً .

أولاً: في التشريع الأردني

1- الجرائم الإرهابية المرتكبة إلكترونياً وفقاً لقانون منع الإرهاب

تضمن قانون منع الإرهاب الأردني الصادر في 2006/11/01، تعريفاً شاملاً للعمل الإرهابي يمتد ليشمل "الإرهاب بالوسائل الإلكترونية" بصفة ضمنية من خلال عبارة "بأي وسيلة كانت"، وينص القانون على أن العمل الإرهابي هو كل فعل مقصود يهدف إلى قتل الأشخاص أو إيذائهم جسدياً، أو إلحاق الضرر بالممتلكات العامة والخاصة، أو المرافق الدولية، أو البنية التحتية أو البيئة، كما يمتد هذا المفهوم ليشمل الأفعال التي تهدف إلى الإخلال بالنظام العام، أو تهديد سلامة المجتمع وأمنه، أو تعطيل أحكام الدستور والقوانين، بالإضافة إلى محاولات التأثير على سياسة الدولة أو إجبار الحكومة على القيام بعمل ما أو الامتناع عنه من خلال التهريب والعنف¹.

¹ نور الله تله، المرجع السابق، ص ص134-135.

2/ الإرهاب بالوسائل الإلكترونية بموجب نص قانون جرائم المعلومات رقم 30 لسنة 2010

نظراً لتفاقم الجرائم الإلكترونية وتمدد أبعادها، وجد المشرع الأردني نفسه أمام ضرورة ملحة لإفراد تشريع خاص ينظم هذه المسائل، وهو قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010، وبالرجوع إلى نص المادة (10) من القانون المذكور، نجدها قد قضت بفرض عقوبة الأشغال الشاقة المؤقتة على كل من سخر نظام معلومات أو شبكة إلكترونية، أو أسس موقعاً رقمياً لغايات تيسير تنفيذ ممارسات إرهابية، أو مساندة جماعات وتنظيمات إرهابية، أو التسويق لمعتقداتها وأفكارها، أو توفير الدعم المادي لها، إلا أن القراءة الفاحصة لهذا النص تكشف عن حصر المواجهة القانونية للإرهاب الإلكتروني في نطاق ضيق يتمثل في الترويج والتمويل والدعم عبر المواقع، وهو ما لا يستوعب الأشكال المتطورة والأنماط المستحدثة للنشاط الإرهابي الرقمي كافة؛ الأمر الذي يستوجب على المشرع الأردني تحديث هذه النصوص لتشمل سائر صور الاستغلال التقني في العمليات الإرهابية، وضمان تغطية تشريعية شاملة تواكب كافة جوانب الإرهاب الإلكتروني¹.

ثانياً: في التشريع المصري

1/ المرجعية الدستورية (دستور 2014)

أرسى الدستور المصري الحالي في مادته رقم (31) مبدأً جوهرياً باعتبار "أمن الفضاء المعلوماتي" جزءاً لا يتجزأ من منظومة الاقتصاد والأمن القومي الشامل، وبموجب هذا النص أصبحت الدولة ملتزمة باتخاذ كافة التدابير الوقائية والعلاجية اللازمة لحماية هذا الفضاء، وذلك وفقاً للأطر والضوابط التي يحددها القانون².

¹ نور الله تله، المرجع السابق، ص ص 135-136.

² المادة 31 من القانون رقم 175 لسنة 2018 لمكافحة جرائم تقنية المعلومات المصري، وهو القانون التنفيذي للدستور المصري لسنة 2014.

2/ الانضمام للاتفاقيات الإقليمية (الاتفاقية العربية 2010)

في إطار تعزيز التعاون الدولي والإقليمي، وافقت مصر في 19 أغسطس 2014 على الانضمام إلى "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" المبرمة عام 2010، وينبثق هذا التوجه عن قناعة بضرورة توحيد السياسات الجنائية العربية لحماية المجتمع الرقمي من التهديدات العابرة للحدود، وقد ركزت هذه الاتفاقية في مادتها رقم (15) على توصيف الجرائم المرتبطة بالإرهاب عبر الوسائط التقنية¹.

الفرع الثاني: الدول الغربية لمكافحة الإرهاب الإلكتروني

يشهد الإرهاب الإلكتروني تطورًا متسارعًا فرض على الدول الغربية تبني سياسات قانونية وأمنية متقدمة لمواجهة، نظرًا لما يمثله من تهديد مباشر للأمن القومي والبنى التحتية الرقمية. وقد اتجهت هذه الدول إلى وضع استراتيجيات شاملة تجمع بين سن التشريعات الحديثة، وتعزيز الرقابة الإلكترونية، وإنشاء هيئات متخصصة في الأمن السيبراني، إلى جانب توسيع نطاق التعاون الدولي في مجال مكافحة الجرائم الإرهابية الرقمية.

وتبرز كل من الولايات المتحدة الأمريكية (أولاً)، وفرنسا (ثانياً)، كنماذج رائدة في هذا المجال، حيث سعت كل دولة إلى تطوير منظومتها القانونية والأمنية بما يتلاءم مع طبيعة التهديدات السيبرانية المتجددة

أولاً: الولايات المتحدة الأمريكية

تُصنف الولايات المتحدة الأمريكية ضمن القوى الرائدة عالمياً في مجابهة الإرهاب الإلكتروني، حيث اعتمدت في مقاربتها على مسارات متوازية شملت تطوير الترسنة القانونية الوطنية، وتفعيل التعاون الدولي عبر الاتفاقيات الثنائية والمتعددة الأطراف، بالإضافة إلى استحداث أجهزة أمنية وعسكرية متخصصة، وقد اتسمت الرؤية الاستراتيجية الأمريكية بالنزعة الاستباقية لدرء المخاطر قبل وقوعها، حيث تركزت في بدايتها على الشق العسكري، وتجسد

¹ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، القاهرة لسنة 2010، انضمت إليه مصر سنة 2014.

ذلك عام 2005 حين استحدثت وزارة الدفاع (البنتاغون) وحدة عسكرية نوعية أنيطت بها مسؤولية حماية الفضاء السيبراني القومي وتأمين الشبكات المعلوماتية الحيوية من أي تهديدات إرهابية محتملة¹.

وفي الشق التشريعي، كانت الولايات المتحدة من أوائل الدول التي قننت مكافحة الجرائم الإرهابية الرقمية، لا سيما بعد صدور تشريعات أكتوبر 2001 التي منحت سلطات إنفاذ القانون صلاحيات واسعة في مجالات التفتيش والرقابة والتحري الإلكتروني²، ولا تزال الجهود الفيدرالية مستمرة لتحديث القوانين بما يواكب التطور المتسارع للظاهرة الإرهابية، بما في ذلك مساعي تقنين الرقابة على استخدام محركات البحث الكبرى مثل (Google، Yahoo، MSN)³ وفي إطار تدعيم هذه الجهود، اتخذت الإدارة الأمريكية جملة من الإجراءات التنفيذية والتشريعية المحورية، لعل من أبرزها⁴:

- سن قانون تعزيز أمن المعلومات لعام 2002.
- إقرار الاستراتيجية الوطنية لتأمين الفضاء الإلكتروني في عام 2003.
- تأسيس لجنة متخصصة لمكافحة الإرهاب الإلكتروني تابعة لوزارة العدل الأمريكية.
- تشكيل لجنة حماية البنى التحتية الحساسة، والتي انبثق عنها ما يُعرف بـ "مركز حرب المعلومات" المتخصص في معالجة القضايا الأمنية الرقمية.
- إرساء دعائم المركز القومي لحماية البنية التحتية، ومركز تحليل وتبادل المعلومات، إلى جانب سلسلة من البرامج والمبادرات الهادفة لتعزيز الأمن الرقمي الشامل.

¹ عبد المجيد حلاوي، المرجع السابق ص22.

² محمد سيد سلطان، الحماية الدولية والقانونية للبيئة الالكترونية من الجريمة والارهاب، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، منعقد في الرياض السعودية بتاريخ يومي 6 و 7 أفريل 2010، ص 19.

³ عبد المجيد حلاوي، المرجع السابق، ص22.

⁴ محمد سيد سلطان، المرجع السابق، ص ص 19- 20.

ثانياً: فرنسا

تُعد التجربة الفرنسية في مكافحة الإرهاب من الرواد على المستويين الإقليمي والأوروبي، متميزة باستباقيتها في مواجهة الإرهاب الإلكتروني وصياغة الآليات القانونية لتتناسب مع تطوره، وقد برز هذا النهج باكراً من خلال القانون رقم 88-19 الصادر في 5 يناير 1988 المتعلق بالجرائم الرقمية، والذي أُدرج في المادة 462 من القانون الجنائي الفرنسي، حيث جعل النفاذ غير المشروع إلى أنظمة معالجة البيانات الآلية، أو البقاء فيها دون حق، جريمة. كما فرض تشديداً على العقوبات (سجن أو غرامة) إذا أدى ذلك إلى حذف أو تعديل آلي للبيانات، وصولاً إلى تعديلات 1993 التي زادت من شمول الجرائم لتعزيز الردع¹.

وفي سياق مترابط، أصدر عام 2009 قانوناً متخصصاً بمكافحة الإرهاب منح صلاحيات واسعة لمراقبة الاتصالات والإنترنت والكاميرات في الأماكن العامة، مع إمكانية مقاضاة أي مواطن فرنسي ينضم إلى معسكرات تدريب إرهابية خارج البلاد، حتى بدون فعل مادي داخل الأراضي، تحت تصنيف "تشكيل عصابة إجرامية" لارتكاب إرهاب، بعقوبة تصل إلى 10 سنوات سجناً وغرامة 225 ألف يورو².

واستجابة لزيادة مقاتلي الخارج، عُدل القانون في نوفمبر 2014 لفرض قيود سفر ومنع الانضمام إلى جماعات متطرفة كـ"داعش"، مع صلاحية مصادرة جوازات السفر والهويات مؤقتاً، ومنع دخول المشتبهين، بالإضافة إلى رقابة مشددة على المحتوى الرقمي المتطرف وإلزام مسؤولي المواقع بحذف التحريضات تحت عقوبة الإغلاق³.

ووصلت هذه المنظومة إلى قمّتها بقانون "تعزيز مكافحة الإرهاب" في مارس 2015، الذي غيّر المشهد بمنح الاستخبارات صلاحيات اختراق ومراقبة "الإرهابيين المحتملين" عبر

¹ رائد عدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، دورة تدريبية، توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، الرياض، السعودية، 23-27، فيفري 2013، ص، ص 12-13.

² نور الله تله، مرجع سابق، ص 141.

³ . مرجع نفسه، ص 141-142.

قرارات إدارية دون حاجة لموافقة قضائية مسبقة؛ مما سمح بتقنيات التجسس الرقمي، وتركيب أجهزة تنصت، واعتراض اتصالات في مناطق محددة جغرافياً، مع إلزام شركات الاتصالات ومزودي الإنترنت بتزويد البيانات الكاملة، وخُتمت الجهود في أبريل 2015 باتفاقية بين الحكومة الفرنسية وشركات التكنولوجيا الكبرى (جوجل، فيسبوك، مايكروسوفت، أبل) لآلية مشتركة تضمن إزالة فورية للمحتويات الإرهابية وحظر المواقع المتطرفة، تحت إشراف مكتب مكافحة الجرائم الإعلامية والرقمية¹.

المطلب الثاني

جهود الجزائر لمكافحة الإرهاب الإلكتروني

يُمثل الإرهاب بشتى صوره وأبعاده أحد أخطر التحديات الأمنية المعاصرة التي تُهدد استقرار الدول والمجتمعات في ظل التسارع التكنولوجي، وقد أدى هذا التحول الرقمي إلى بروز "الإرهاب الإلكتروني" (الفرع الأول) كخطر عابر للحدود، مما يفرض على الدول والمؤسسات تبني استراتيجيات شاملة ومتكاملة لمواجهة (الفرع الثاني) والحد من مخاطره.

الفرع الأول: الإرهاب الإلكتروني في الجزائر

استناداً إلى رصيدها التاريخي الحافل في مجابهة الظاهرة الإرهابية، أرست الجزائر دعائم منظومة قانونية متطورة حظيت بإشادة المجتمع الدولي، حيث لم تتوقف الجهود عند التدابير الأمنية التقليدية، بل امتدت لتشمل تحصين الفضاء الرقمي تماشياً مع التحولات التكنولوجية المتسارعة، ويأتي هذا التوجه في ظل سعي الدولة لتبني نموذج الاقتصاد الرقمي، مما جعل من التصدي للإرهاب الإلكتروني ضرورة حتمية لحماية الاستقرار الوطني وضمان أمن التعاملات المستقبلية.

¹ نور الله تله، مرجع سابق، ص 142-143.

وفي سبيل سد الفراغ القانوني، عمد المشرع الجزائري من خلال القانون رقم 04-15¹ المعدل لقانون العقوبات إلى تجريم كافة أشكال الاعتداءات الرقمية، حيث نصت المادة 394 مكرر وما يليها على معاقبة الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، وتجريم أعمال التخريب أو الاستيلاء على البيانات، بالإضافة إلى حظر نشر المعلومات لغايات إرهابية أو تجسسية أو تحريضية، وقد تنوعت الجزاءات المقررة بين عقوبات أصلية كالحبس والغرامة، وتدابير تكميلية رادعة تشمل مصادرة الأجهزة وإغلاق المواقع أو المنشآت التي كانت مسرحاً للجريمة، شريطة ثبوت علم المالك بوقوعها.²

وتعزيزاً للمقاربة الوقائية، استحدث القانون رقم 04-09³ قواعد إجرائية تسمح بالرصد المبكر للتهديدات السيبرانية، مانحاً السلطات المختصة صلاحيات الرقابة على المراسلات الإلكترونية في حالات محددة تتعلق بحماية النظام العام أو مكافحة الأعمال الموصوفة بجرائم الإرهاب، كما تم إنشاء "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، لتكون بمثابة مركز تنسيقي وطني يسهر على تنفيذ السياسة الدفاعية الرقمية للدولة، مما جعل التشريع الجزائري مجالاً شاملاً يغطي كافة الجرائم المرتكبة عبر شبكة الإنترنت.⁴

الفرع الثاني: مواجهة الإرهاب الإلكتروني في الجزائر

تبنى المشرع الجزائري استراتيجية قانونية متكاملة لمواجهة الإرهاب الإلكتروني، حيث عزز منظومته التشريعية بالأمر رقم 04-09 المتعلق بتكنولوجيا الإعلام والاتصال، وتتوزع هذه الجهود بين إجراءات عامة (أولاً) للبحث والتحري، وإجراءات خاصة (ثانياً)، تشمل التدابير المادية والتقنية اللازمة لضبط هذه الجرائم المستحدثة.

¹ قانون رقم 04-15 مؤرخ في 10/11/2004، يتضمن قانون العقوبات، جريدة الرسمية، عدد 17، صادر في 10/11/2004.

² انظر المادة 394 مكرر، من قانون رقم 04-15 المؤرخ في 10/11/2004، من قانون العقوبات.

³ قانون رقم 04-09 السالف الذكر.

⁴ أنظر المادة 13 و14 من القانون نفسه.

أولاً: الإجراءات العامة لمتابعة جريمة الارهاب الإلكتروني

"طبق المشرع الجزائري بعض إجراءات البحث والتحري التقليدية على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب، إضافة إلى إدراجه لبعض الإجراءات الخاصة كاعتراض المراسلات وتسجيل الأصوات والتقاط الصور والمراقبة الإلكترونية، وقد عزز المنظومة القانونية بإصداره للأمر 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، إذ أبرز من خلاله توجهه نحو تسمية هذه الجرائم المستحدثة بتسمية "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"².

1- الإجراءات المادية

تتمثل الإجراءات المادية في المعاينة التقنية للمسرح الرقمي وتفتيشه لضبط الأدلة الجنائية، حيث ينتقل ضباط الضبطية القضائية للمكان الذي ارتكبت فيه الجريمة لإثبات آثارها المادية واستخلاص الدليل الرقمي.

أ/ مفهوم المعاينة التقنية

تُعرف المعاينة التقنية بأنها الإجراء المنصبّ على مسرح الجريمة، باعتباره المستودع الجوهرية الذي يضم أهم الأدلة الجنائية التي يتركها الجاني خلفه، وبموجب هذا الإجراء، ينتقل مأمورو الضبط القضائي إلى الموقع لمباشرة فحص الآثار المادية للجريمة، وتوثيق حالة الأمكنة والأشخاص، والتحفّظ على كل ما من شأنه المساهمة في استجلاء الحقيقة.

وقد كرست المواد 06، 07، 08 من قانون رقم 04-09 هذا الإجراء كخطوة أساسية ضمن مرحلة جمع الاستدلالات، حيث منحت الضبطية القضائية صلاحية تنفيذه سواء في الظروف الاعتيادية أو في حالات التلبس³ بالجريمة لضمان فاعلية المعاينة وتحقيق غاياتها،

¹ أنظر المادة 11 من قانون رقم 04-09 السالف الذكر.

² عز الدين عثمانى، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث الدراسات القانونية والسياسية، مخبر المؤسسات النظم السياسية، العدد الرابع، جانفي 2018.

³ عبد الله ماجد العكايلة، الوجيز في الضبطية القضائية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2010، ص65.

أقرت التشريعات عقوبات جنائية رادعة ضد أي شخص يعبث بمسرح الجريمة، سواء بتغيير معالم الأمكنة، أو إزالة الأدلة¹، أو إحداث أي تعديل مادي قبل مباشرة سلطات التحقيق أو الاستدلال لمعاينتها الأولية، وذلك وفقاً لما نصت عليه المادة 337 من قانون الإجراءات الجزائية² بينما تقتصر المعاينة في الجرائم التقليدية على المحيط المادي المباشر، فإن جريمة الإرهاب الإلكتروني تتطلب معاينة مزدوجة تتم على مستويين:

المسرح التقليدي ويقصد به الحيز المادي الخارجي لبيئة الحاسوب، ويشمل كافة المكونات الملموسة في موقع الجريمة، مثل:

- وحدات التخزين (الأشرطة الممغنطة).
- التوصيلات والكابلات الخاصة بالأجهزة.
- شاشات العرض ولوحات التحكم ومفاتيح التشغيل.

الجانب المادي للمعاينة يتعلق هذا الجانب بمشتملات الحاسب الآلي ذات الطبيعة الملموسة؛ وتتسم عملية المعاينة هنا بالبساطة والوضوح، لكونها تنصبُّ على مكونات مادية محسوسة كانت هي الأداة المستخدمة في الجريمة أو كانت هدفاً لها.

أما المسرح الافتراضي (البيئة الرقمية) يتمثل هذا المستوى في المحيط الداخلي للأنظمة الإلكترونية، حيث يركز على "البيانات الرقمية" المخزنة في الذاكرة أو على الأقراص الصلبة. وتشمل هذه المعاينة الجرائم التي تستهدف البرمجيات وقواعد البيانات، أو تلك التي تُرتكب عبر الشبكة العنكبوتية (الإنترنت) كما هو الحال في عمليات الإرهاب الإلكتروني، تحديات المعاينة في العالم الافتراضي خلافاً للمعاينة التقليدية، تكتنف معاينة المسرح الافتراضي صعوبات بالغة، ويعود ذلك لعدة اعتبارات جوهرية أبرزها:

¹ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في الكمبيوتر والانترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص160.

² قانون رقم 25-14 مؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، ج ر عدد 54 مؤرخة في 13 أوت 2025.

ندرة الأدلة المادية الملموسة حيث أن الآثار الناتجة عن الجرائم المعلوماتية تختلف جذرياً عن الآثار التقليدية، فهي آثار رقمية غير محسوسة يصعب اقتفاؤها أو التحفظ عليها بالطرق المعتادة¹.

ضوابط المعاينة التقنية لمسرح الجريمة

– التحفظ على الأجهزة وجوب الإبقاء على الحواسيب المضبوطة كما هي دون عبث وتوثيق حالتها الراهنة.

– تحريز المطبوعات جمع الوثائق الورقية المستخرجة من الحاسب وتصنيفها في أكياس مخصصة.

– ترقيم الوسائط حصر دعائم التخزين (أقراص، فلاشات) وترقيمها مع بيان مكان ضبطها بدقة.

– النقل الفني وضع الضبطيات في أوعية واقية من العوامل الجوية والمجالات المغناطيسية لإرسالها للمخبر².

ب/ التفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تُعد عملية التفتيش في جرائم أنظمة المعالجة الآلية للمعطيات من أدق الإجراءات القانونية وأخطرها نظراً لمساسها المباشر بالحريات الشخصية المكفولة دستورياً، وهو ما دفع المشرع لإحاطتها بضوابط صارمة تحكم سلطة مباشرته وظروف تنفيذه لضمان صون حرمة المسكن والحرية الفردية، باعتباره وسيلة تهدف حصراً للوصول إلى الأدلة المادية. وتخضع هذه العملية لنوعين من الشروط؛ "موضوعية" و"شكلية"، حيث تهدف الأخيرة إلى ضمان صدقية النتائج وحماية المتهم من تعسف الجهات القائمة على التفتيش، ومن أبرز هذه الضمانات

¹ ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، السنة الجامعية 2016/2015، ص 58.

² المرجع نفسه، ص 59.

الشكلية ما أقره المشرع الجزائري في قانون الإجراءات الجزائية بشأن "النطاق الزمني"، حيث حظر البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحاً أو بعد الثامنة مساءً¹، أجاز المشرع الجزائري بموجب المادتين 75، 76 من قانون الإجراءات الجزائية تفتيش المنازل في أي وقت، ليلاً أو نهاراً، في جرائم محددة تشمل الجرائم المتعلقة بالمعالجة الآلية للمعطيات، شريطة الحصول على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق المختص.

ورغم أن الأصل في تفتيش المساكن يستوجب حضور المتهم أو من ينوب عنه، أو شاهدين في حال تعذر ذلك طبقاً للمادتين 157، 158 من القانون رقم 25-14 الذي استثنى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من هذا القيد، حيث لم يعد ضابط الشرطة القضائية ملزماً بحضور المشتبه به أو نيل رضاه أثناء المعاينة، كما أتاح تفتيش مسكن الشخص الموقوف للنظر أو المحبوس في مكان آخر بعد استيفاء الموافقات اللازمة.²

يُعد التفتيش عملاً من أعمال التحقيق الجوهري التي استوجب المشرع الجزائري توثيقها بموجب محضر رسمي مكتوب باللغة الوطنية، يتضمن كافة الإجراءات والوقائع والأدلة المضبوطة وتاريخ تحريره وتوقيع مُصدره لضمان حجتيه، وتتحدد مشروعية هذا الإجراء بضرورة توافر شروط موضوعية، تبدأ بوجود سبب جدي يتمثل في وقوع جريمة معلوماتية فعلية، وأن ينصب محل التفتيش على المستودعات المادية أو الافتراضية للأسرار، والتي تشمل في الجرائم الإلكترونية الحواسيب والشبكات المعلوماتية ومكوناتها المادية والمعنوية، على أن يصدر الإذن بالتفتيش حصراً عن السلطة المختصة المتمثلة في قاضي التحقيق أو النيابة العامة لضمان حماية الحقوق والحريات، وغاية التفتيش الكشف عن الحقيقة وضبط الأشياء المتعلقة بالجريمة، وإلا اعتُبر الإجراء باطلاً إذا تم لأغراض أخرى.

وفي سياق ضبط الأدلة الرقمية، وعلى الرغم من سهولة التعامل مع المكونات المادية، إلا أن الصعوبة تكمن في الوسائل الفنية المستحدثة، مما دفع المشرع بموجب القانون 09-04

¹ أنظر المادتين 75، 76 من القانون رقم 25-14 السالف الذكر.

² بن مكي نجا، السياسة الجنائية لمكافحة الجرائم المعلوماتية، ط01، دار الخلدونية، الجزائر، 2017، ص215.

لإقرار آليات تقنية خاصة تشمل نسخ المعطيات على دعامات تخزين قابلة للحجز، أو تقييد الوصول إليها ومنع الدخول للمنظومة، مع إمكانية الحجز على المعدات المادية كأجهزة "المودم"¹.

كما أكدت أحكام قانون الإجراءات الجزائية على عدم جواز ضبط هذه الأدلة إلا بأمر قضائي، مع منح وكيل الجمهورية صلاحيات استثنائية في جرائم المساس بأنظمة المعالجة الآلية للمطيات للإذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور وتثبيتها دون اشتراط موافقة المعنيين، وذلك متى استدعت ضرورة التحقيق ذلك، مع سريان القواعد العامة للتحقيق والمحاكمة على ما لم يرد فيه نص خاص².

2/ الإجراءات الشخصية

أ/ الخبرة

تُعرف الإجراءات الشخصية بكونها تدابير لصيقة بالفرد، تبرز من خلال الاستجواب والخبرة القضائية؛ حيث تُسخر الخبرة الكفاءات الفنية والعلمية التخصصية التي يفتقدها رجال القضاء لفك رموز الجريمة الإلكترونية، وتحديد هوية الجاني³، واستنباط الأدلة الرقمية الدقيقة من خلال عمليات تقنية تخصصية تسهم في توضيح الجوانب الغامضة في التحقيق ويخضع إلى إجراءات قانونية هي :

– إختياره من طرف جدول الخبراء حسب المادة 240 من ق.ا.ج.ج⁴

– على الخبير أداء اليمين القانونية حسب المادة 241 من ق.ا.ج.ج⁵

¹ قانون رقم 04-09 السالف الذكر.

² أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار بلقيس، الجزائر، 2021، ص136.

³ أحمد شوقي الشلقاني، مبادئ الاجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ط5، ديوان المطبوعات الجامعية، الجزائر ص259.

⁴ أنظر المادة 240 من القانون رقم 14-25، السالف الذكر.

⁵ أنظر المادة 241 من القانون رقم 14-25، السالف الذكر.

يخضع تعيين الخبير القضائي لضوابط إجرائية تشمل الاختيار من الجدول وأداء اليمين القانونية وفقاً لقانون الإجراءات الجزائية، حيث يستعين بوسائل تقنية متطورة لتتبع أثر الجريمة وتحديد هوية فاعلها، ومن أبرزها تتبع بروتوكول الإنترنت (IP) لكشف رقم الجهاز وموقعه، واستخدام "البروكسي" كوسيط شبكي لتعزيز الأمن وإدارة الاتصال، بالإضافة إلى توظيف برامج التتبع ونظم كشف الاختراق (IDS) وأدوات التدقيق والمراجعة الحاسوبية، وهي آليات تكنولوجية تمنح التحقيق القدرة على فحص الشبكات واستنباط الأدلة الرقمية بدقة.¹

ب/ الاستجواب

عد الاستجواب في جرائم الإرهاب الإلكتروني إجراءً جوهرياً يهدف إلى مواجهة المتهم بالحقائق والأدلة المنسوبة إليه، وبينما يخضع هذا الإجراء للقواعد العامة المعمول بها في الجرائم التقليدية، فإنه يتطلب سلطة تحقيق متخصصة تمتلك الكفاءة التقنية اللازمة للإحاطة بتفاصيل هذا النوع من الجرائم المعقدة، مع الالتزام بالضمانات القانونية التي كفلها المشرع لحماية حقوق المتهم² وفي سياق التدابير الاستثنائية، خول القانون لضباط الشرطة القضائية صلاحية توقيف الأشخاص الذين تتوفر ضدهم قرائن قوية في مراكز الشرطة أو الدرك، وبالرغم من أن القاعدة العامة تحدد مدة التوقيف للنظر بـ 24 ساعة، إلا أن المشرع استثنى جرائم الإرهاب الإلكتروني نظراً لخطورتها ومساسها بالمعالجة الآلية للمعطيات، حيث أجاز تمديد فترة التوقيف لمرة واحدة وفقاً للمادة 175³، كما أباح اللجوء إلى القوة القانونية لإحضار الأشخاص طبقاً للمادة 176 من القانون 14-25 المذكور أعلاه.

¹ أحسن بوسقيعة، المرجع السابق، الوجيز في القانون الجزائي الخاص، ص 142.

² حلف فاروق، الآليات القانونية لمكافحة الجريمة المعلوماتية، مداخلة مقدمة في الملتقى حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، 16-17 نوفمبر 2015، ص ص 02، 03.

³ سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، جامعة الاخوة منتوري، قسنطينة، مجلة العلوم الانسانية، عدد 52، مجلد ب، ديسمبر 2019، ص 52.

ج/ سماع الشهود

تكتسي شهادة الشهود في الجرائم المعلوماتية طابعاً فنياً خاصاً، حيث يُعرّف الشاهد فيها بأنه الشخص ذو الخبرة المتخصصة في تقنيات وعلوم الحاسب الآلي، والمنوط به تقديم معلومات جوهرية حول كيفية الولوج إلى أنظمة المعالجة الآلية للمعطيات¹، وتتنوع فئات هؤلاء الشهود لتشمل مشغلي الحاسب الآلي المسؤولين عن إدارة الأجهزة والمعدات، والذين يمتلكون مهارة عالية في التعامل مع البيانات إدخالاً واستخراجاً ومعالجة، بالإضافة إلى خبراء البرمجة المختصين بصياغة الأوامر البرمجية وتخطيط التطبيقات والنظم²، وقد وسع المشرع الجزائري في القانون 09-04³ من هذا المفهوم ليشمل مقدمي الخدمات، وهم الكيانات (سواء كانت عامة أو خاصة) التي تتيح للمستخدمين القدرة على التواصل عبر المنظومات المعلوماتية، أو تلك التي تتولى معالجة وتخزين المعطيات الرقمية لصالحهم، على غرار ما هو منصوص عليه في قانون الإجراءات الجزائية عملاً بأحكام المادة 163 وما يليها⁴.

ثانياً: الإجراءات الخاصة لمكافحة الإرهاب الإلكتروني

1/ الإجراءات الخاصة بحماية معطيات الحاسب الآلي

-التحفظ العاجل على البيانات المخزنة

تُعتبر هذه الآلية وسيلة استقصائية مستحدثة، تهدف من خلالها السلطة المختصة إلى إلزام مزودي الخدمات بالحفاظ على البيانات المعلوماتية المخزنة لديهم وضمان عدم المساس بها، وذلك كتدبير احترازي مؤقت يسبق اتخاذ إجراءات قانونية لاحقة كالتفتيش أو الأمر بتقديم

¹ عبد الفتاح بيومي حجازي، المرجع السابق، ص339.

² خلف فاروق، المرجع السابق، ص04.

³ أنظر المادة 16 من قانون رقم 04/09 المؤرخ في 5 شعبان عام 1430، السالف الذكر.

⁴ أنظر المادة 163 من القانون رقم 14-25، السالف الذكر.

البيانات؛ إذ يمثل التحفظ العاجل خطوة تمهيدية غايتها الأساسية حماية البيانات من فقدان أو التلف قبل استكمال إجراءات التحقيق.¹

• الأمر بتقديم البيانات المعلوماتية للمشارك:

بالرغم من أن الأصل في البيانات الشخصية لمستخدمي الشبكة هو الحماية بموجب الحق في الخصوصية، إلا أن مأموري الضبط القضائي يملكون صلاحية إلزام الأشخاص بتسليم ما في حوزتهم من موضوعات يُطلب تقديمها كدليل جنائي، بما يمتد ليشمل بيانات المشتركين المودعة لدى مزودي الخدمات.²

2/ السماح بالمراقبة للاتصالات الإلكترونية:

تتمثل المراقبة الإلكترونية للاتصالات في إجراء تقني يهدف إلى رصد وتتبع المراسلات أثناء تدفقها وعبرها اللحظي، دون أن يمتد ذلك ليشمل البيانات المخزنة، وهي وسيلة حديثة استحدثها المشرع لجمع الأدلة والمعلومات المتعلقة بالمشتبه فيهم أو الأماكن والوسائل المرتبطة بهم، مما يجعلها أداة محورية في مكافحة الجرائم المعلوماتية³، وقد حددت المادة 04 من القانون 04-09 نطاق هذه المراقبة ليشمل كافة الوسائط السلكية واللاسلكية والخلوية، بالإضافة إلى البريد الإلكتروني ومنصات الدردشة والفاكس⁴، ومن الناحية الإجرائية، كرس المشرع الجزائري هذا الإجراء عبر القانون 14-25 المتضمن قانون الإجراءات الجزائية، وتحديدًا في المادة 83 منه، حيث خول لوكيل الجمهورية أو قاضي التحقيق صلاحية الإذن لضباط وأعوان الشرطة القضائية باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وذلك في حالات الضرورة التي تمليها التحريات في الجرائم المتلبس بها أو التحقيقات الابتدائية

¹ بن مكي نجا، مرجع سابق، ص 230.

² بن مكي نجا، المرجع نفسه ص 230.

³ نبيلة هبة هروال، الجوانب الإجرائية للجرائم الكمبيوتر والأترنت، في مرحلة جمع الاستدلالات، ط01، دار الفكر الجامعي، الإسكندرية، 2013، ص 204.

⁴ أنظر المادة 04 من قانون 04-09، السالف الذكر.

المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، ومع خطورة هذا الإجراء، فقد ألزم المشرع بضرورة تنفيذه في إطار من السرية التامة، مع التقيد بالضوابط القانونية والضمانات الأساسية التي تحمي حرمة الحياة الخاصة للأشخاص باعتبارها حقاً دستورياً مصوناً لا يجوز انتهاكه خارج الأطر القانونية المحددة¹.

- بالرجوع إلى نص المادة 4 من القانون 04-09 حدد المشرع الجزائري الحالات الحصرية التي يُسمح فيها باللجوء إلى آلية المراقبة الإلكترونية² المنصوص عليها في المادة 3، وهي:
- الوقاية الأمنية: التصدي للأفعال الإرهابية، التخريبية، أو تلك التي تمس بأمن الدولة.
 - حماية المنظومات المعلوماتية: عند توفر مؤشرات جدية على وجود تهديدات ضد أنظمة المعلومات من شأنها الإضرار بالنظام العام، الدفاع الوطني، مؤسسات الدولة، أو الاقتصاد الوطني.
 - الضرورة التحقيقية: عندما تقتضي متطلبات التحريات والتحقيقات القضائية ذلك، شريطة تعذر الوصول لنتائج ملموسة دون الاستعانة بالمراقبة.
 - التعاون الدولي: استجابة لطلبات المساعدة القضائية الدولية المتبادلة
- ولضمان مشروعية مراقبة الاتصالات وتجنب بطلان الإجراء (وفقاً لقانون الإجراءات الجزائية، والقانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها)، يجب الالتزام بالضوابط التالية المنصوص عليها في المادة 83 من قانون الاجراءات الجزائية³ وما يليها:

¹ قانون رقم 14-25 المتضمن قانون الإجراءات الجزائية، السالف الذكر.

² انظر: المادة 04 من قانون 04-09 السالف الذكر.

³ انظر: المادة 83 من قانون رقم 14-25 السالف الذكر.

• الإذن الكتابي: ضرورة صدور أمر مكتوب من السلطة المختصة (قاضي التحقيق أو وكيل الجمهورية)¹

• تحديد النطاق: يجب أن يتضمن الإذن كافة البيانات التي تتيح للضباط تحديد الاتصالات المعنية بالاعتراض بدقة.²

– نوع الجريمة: أن يكون موضوع البحث متعلقاً بإحدى الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات.

– المدة الزمنية: يُحدد الإجراء بفترة 4 أشهر، وتكون قابلة للتجديد بناءً على مقتضيات التحري والتحقيق.

– التوثيق المحضري: وجوب تحرير محضر رسمي يتضمن كافة المعطيات الفنية للعملية، مع تسجيل دقيق لساعة وبداية ونهاية المراقبة

أما بخصوص القواعد الإجرائية الواردة في القانون 04-09، فقد حددت المادة 04³ منه بدقة الشروط الواجب توافرها لتفعيل المراقبة الإلكترونية، والتي تتبلور في ضرورة صدور إذن مسبق من النائب العام لدى مجلس قضاء الجزائر العاصمة⁴، على أن يتولى تنفيذ هذه المراقبة ميدانياً ضباط الشرطة القضائية التابعون للهيئة المنصوص عليها في المادة 13 من نفس القانون، مع تقييد سريان هذا الإذن بمدة زمنية لا تتجاوز ستة أشهر، تظل فيها قابلة للتجديد وفق مقتضيات الحاجة.⁵

3/ الحماية التقنية للأنظمة من الاعتداءات الإلكترونية :

-برامج الحماية:

¹ أحسن بوسقيعة، التحقيق القضائي، ط10، دار هومة للنشر، الجزائر، 2009، ص124.

² أنظر: المادة 63 من القانون رقم 14-25 المتضمن قانون الإجراءات الجزائية، السالف الذكر.

³ أنظر: المادة 4 من قانون 04-09 السالف الذكر.

⁴ أنظر: المادة 04 الفقرة 03 من قانون 04-09 السالف الذكر.

⁵ أنظر: المادة 13 من قانون 04-09 السالف الذكر.

تعد هذه البرامج الركيزة الأساسية لتحقيق الأمن الرقمي، حيث تعمل على تصفية وحجب المواقع المحظورة والخطرة، وتتيح ميزة إدارة الوقت لتحديد مواعيد ومدة الاتصال بالشبكة. كما توجد إصدارات متخصصة لحماية الأطفال تهدف إلى التحكم في البرامج المستخدمة ومنع تسريب المعلومات الشخصية أثناء المحادثات، ومن أبرز الأمثلة على هذه النظم "جدار النار" إذ سعت شركات البرمجيات والخدمات المالية الكبرى لتطويره كإستراتيجية وقائية لمنع الدخول غير المشروع، ويعمل هذا النظام بمثابة ممر إلكتروني ذكي يراقب حركة البيانات الصادرة والواردة، وتؤكد الإحصائيات أن ما يزيد عن ثلث المواقع العالمية مؤمنة حالياً بواسطة أحد أشكال جدران الحماية¹.

-كشف التسلل وإساءة الاستخدام:

يرمي كشف التطفل وإساءة الاستخدام إلى رصد الأنشطة التخريبية في مهبها، ويتم ذلك عبر تتبع هذه الأنشطة ومراقبتها، حيث يتيح الكشف المبكر عنها فرصة إحباط المحاولة قبل وقوع الضرر، ورغم أن هذا المبدأ قد لا يبدو عملياً بالكامل كونه لا يضمن منع جميع الهجمات، إلا أن عملية الاكتشاف تظل هي الأسلوب العلمي المتبع².

¹ قندوشي ربيعة، الإعلام الإلكتروني، ط1، دار هومة للنشر والتوزيع الجزائر، 2012، ص114.

² نيايب البدنية، الأمن وحرب المعلومات، دار الفكر، عمان، ط1، 2012، ص390.

خلاصة الفصل:

تتضافر الجهود الدولية والوطنية لمواجهة الإرهاب الإلكتروني عبر مسارين تكامليين؛ فدولياً، تبرز اتفاقية "بودابست" (2001) كمرجع قانوني أساسي لتوحيد السياسات الجنائية وتسهيل التعاون القضائي، مدعومة بجهود الأمم المتحدة في بناء الثقافة الأمنية الرقمية. ووطنياً، تتبنى دول كالولايات المتحدة وفرنسا استراتيجيات استباقية تجمع بين الترسانة التشريعية الصارمة والقدرات التقنية المتقدمة للرصد والملاحقة. أما على المستوى الإجرائي، كما في النموذج الجزائري، فتعتمد آليات التحري على تدابير دقيقة مثل "التحفظ العاجل" على البيانات الرقمية ومراقبة الاتصالات ضمن ضوابط قانونية توازن بصرامة بين مقتضيات الأمن القومي وحماية الخصوصية الفردية.

خاتمة

بناءً على ما أسفرت عنه هذه الدراسة، نخلص إلى أن الإرهاب الإلكتروني يُشكّل جيلاً جديداً من الجرائم المعلوماتية المستحدثة التي أفرزتها طفرة العلمية الهائلة وثورة التكنولوجيا المعاصرة. ويمثّل هذا السلوك الإجرامي الامتداد الافتراضي للإرهاب التقليدي، بعد أن بدّلت الجماعات المتطرفة استراتيجيتها واعتمدت على الحواسب الآلية وشبكة الإنترنت كأدوات محورية لإدارة هجماتها والاعتداء على الأنظمة والموارد المعلوماتية للدول. وبسبب طبيعته العابرة للحدود الجغرافية والزمنية، غدا هذا النمط يُعرف بـ "إرهاب المستقبل" والمهدد الأكبر للأمن الدولي، متميزاً بقدرته على الانتشار السريع وتنامي مخاطره يوماً بعد يوم.

ولما كان الاعتماد على التحصينات التقنية وحدها عاجزاً عن توفير بيئة آمنة وحماية المجتمعات من هذه الأضرار الجسيمة التي تَمَسُّ الأفراد والدول، فإن الأمر يستدعي تكاتفاً دولياً وإقليمياً جاداً، وتضامناً تشريعياً ووطنياً لصياغة استراتيجيات وقائية وقوانين رادعة تكفل مجابهة هذا الخطر الداهم وتقويض آثاره التخريبية.

ومن خلال فصول الدراسة نستنتج الآتي:

يُعد الإرهاب الإلكتروني امتداداً افتراضياً خطيراً للإرهاب التقليدي، وجيلاً مستحدثاً من الجرائم المعلوماتية العابرة للحدود التي تستهدف الأنظمة البرمجية للقطاعات الحيوية والاستراتيجية في الدول.

على الرغم من تعدد واختلاف التعاريف المتعلقة بالظاهرة، إلا أن هناك إجماعاً قانونياً وفقهياً على تحديد غايتها الأساسية المتمثلة في بث الرعب، ونشر الذعر، وترويع المجتمعات عبر الوسائط الرقمية.

تحولت المنصات الرقمية وشبكات التواصل الاجتماعي إلى مسرح أساسي وأداة منخفضة التكلفة للتنظيمات المتطرفة لتسريب الأفكار الهدامة، وتجنيد الشباب، وتمويل الأنشطة التخريبية.

تتعدد صور هذا النمط الإجرامي وتتداخل مع جرائم بالغة الخطورة مثل غسيل الأموال الإلكتروني لتمويل الإرهاب، والتجسس السيبراني لسرقة الأسرار السيادية، والقصف الإلكتروني لتعطيل المؤسسات.

تبنت الجزائر استراتيجية تشريعية وتقنية متكاملة لمكافحة الإرهاب الإلكتروني، مرتكزة على القانون رقم 04-15 المعدل لقانون العقوبات، والأمر رقم 09-04 المتعلق بالجرائم السيبرانية، بالإضافة إلى قانون الإجراءات الجزائية (تعديل 14-25)، وذلك لخلق منظومة قانونية رادعة وإجرائية دقيقة تضمن حماية السيادة الرقمية والاستقرار الوطني.

على الرغم من الشمولية والتطور اللذين أبدتهما التشريعات الوطنية كالمرجع الجزائري، إلا أن الطبيعة المتسارعة والديناميكية للجريمة السيبرانية تفرض على المنظومات القانونية العربية مراجعة مستمرة وتحديثاً دورياً لمواكبة أبعادها المستحدثة.

أصبحت المواجهة التقنية وحدها عاجزة عن توفير بيئة آمنة، مما يحتم تكاتف المجتمع الدولي وتكامل الردع القانوني والأمني والفني من خلال تفعيل استراتيجيات وقائية وبرامج تدريبية متخصصة.

تتطوي آليات الردع الفعالة على تطبيق إجراءات حماية تكنولوجية صارمة كأنظمة الجدران النارية، وتفعيل المعاينة التقنية المزدوجة للمسرحين المادي والافتراضي لتوثيق الأدلة الجنائية وضبط المحتويات الرقمية.

ومن اهم التوصيات التي توصلنا اليها

سد ثغرات اللجوء: تعديل قوانين الهجرة واللجوء لمنع استغلال الإرهابيين لأراضي الدول في التخطيط والتجنيد.

تعريف موحد: إيجاد تعريف قانوني جامع ومانع لجريمة الإرهاب الإلكتروني.

تشريع مستقل: صياغة قانون خاص ومستقل للإرهاب الإلكتروني يحدد عقوباته وإجراءاته دون ربطه بالإرهاب العادي.

التعاون الدولي: تعزيز التعاون القضائي بين الدول وتبادل الخبرات، والانضمام للاتفاقيات الدولية لمكافحة الجرائم المعلوماتية.

خلايا أمنية جزائرية: إطلاق خلايا أمنية متخصصة وطنياً لحماية الشباب الجزائري ومواكبة الأساليب التكنولوجية المستحدثة.

التوعية الوقائية: تفعيل دور الأسرة، والمؤسسات التربوية، والإعلام للتوعية بمخاطر الظاهرة قبل وقوعها، خاصة في الدول النامية.

منهج أخلاقي: إدراج منهج تعليمي أخلاقي لتوعية الطلاب بمخاطر الإنترنت وأخلاقيات استخدامه.

البحوث والندوات: عقد مؤتمرات ودراسات دورية لبحث أسباب الإرهاب الإلكتروني وتكثيف الجهود المشتركة للحد منه.

قائمة المراجع

I- المصادر:

- ابن منظور، لسان العرب، دار المعارف، القاهرة، 1981.
- أحمد أبي الحسين، بن فارس بن زكريا، معجم مقاييس اللغة، ج 1، تح: عبد السلام محمد هارون، دار الفكر، الأردن، 1979.

II- المراجع

أولاً: الكتب

1. أحسن بوسقيعة، التحقيق القضائي، ط10، دار هومة للنشر، الجزائر، 2009.
2. أحسن بوسقيعة، الوجيز في القانون الجزائري العام، الطبعة 21، دار بلقيس، الجزائر، 2024.
3. أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، دار بلقيس، الجزائر، 2021.
4. أحسن بوسقيعة، الوجيز في القانون الجنائي العام، ط14، دار هومة، الجزائر، 2014.
5. أحمد رفعت وصالح بكر الطيار، الإرهاب الدولي، مركز الدراسات العربي الأوروبي، سنة 1988.
6. أحمد شوقي الشلقاني، مبادئ الاجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ط5، ديوان المطبوعات الجامعية، الجزائر.
7. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، مطابع جامعة نايف للعلوم الأمنية، الرياض، 2006.
8. اسماعيل عبد الفتاح عبد الكافي، الإرهاب ومحاربته في العالم المعاصر، دار الهيئة العامة لقصور الثقافة للنشر والتوزيع، مصر، 2007.
9. أنطوان نعمة وآخرون، معجم المنجد في اللغة المعاصرة، ط2، دار المشرق، بيروت، 2001.

10. إيمان بن سالم، جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2018.
11. ايهاب سمباطي، ترجمة الجديدة والكاملة، الاتفاقية المتعلقة بالجريمة الالكترونية(بودابست 2001) البروتوكول الملحق بها، دار النهضة، القاهرة، 2009.
12. بن مكي نجا، السياسة الجنائية لمكافحة الجرائم المعلوماتية، ط1، دار الخلدونية، الجزائر، 2017.
13. حسين شفيق، الإعلام الجديد والجرائم الالكترونية، التسريبات، التجسس الإلكتروني، الإرهاب الإلكتروني، دار الفكر والفن، بدون بلد النشر، 2015.
14. خالد حسن لطفي، الإرهاب الإلكتروني أفة العصر الحديث والآليات القانونية للمواجهة، ط1، دار الفكر الإسكندرية، مصر، 2018.
15. خالد حسن، أحمد لطفي، الارهاب الإلكتروني، أفات العصر الحديث والآليات القانونية للمواجهة، ط1، دار الفكر الجامعي، الاسكندرية 2018.
16. خالد حسين أحمد لوطفي، جرائم الانترنت بين القرصة الالكترونية والابتزاز الإلكتروني، ط1، دار الفكر الجامعي الاسكندرية، 2018.
17. خليل حسين، التنظيم الدولي النظرية العامة والمنظمات العالمية، ط1، دار المنهل اللبناني، بيروت، 2010.
18. ذياب موسى البدانية، دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، دورة تدريبية في كلية التدريب، قسم البرامج التدريبية بالقنصرة، المغرب، 2006.
19. رامي متولي الجرائم المعلوماتية في تشريعات المقارنة في ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة، 2011.
20. رامي متولي، مكافحة الجرائم المعلوماتية في تشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة، 2011.

21. رائد عدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، دورة تدريبية، توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، الرياض، السعودية، 23-27، فيفري 2013،
22. رشيد صبحي جاسم محمد، الإرهاب والقانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة بغداد، العراق، 2003.
23. الزين بدره هوميل، الإرهاب في القضاء الإلكتروني، رسالة دكتوراه، كلية القانون، جامعة عمان العربية، 2012.
24. سارة بوحادة، مداخل حول الأثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية للعلوم السياسية، الجزائر، 2016.
25. سليمان الطعاني الوجيز في التربية الإعلامية، ط1، دار الخليج للنشر والتوزيع، الأردن، عمان، 2020.
26. سيد أحمد عبد الخالق، الآثار الاقتصادية والاجتماعية لغسيل الأموال، د. ط، دار النهضة العربية، القاهرة، 1997.
27. صفاء كاظم، غازي الجياشي، جريمة قرصنة البريد، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة بابل، العراق، 2016.
28. عادل عبد الصادق، استخدام الارهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015.
29. عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.
30. عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في الكمبيوتر والانترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006.
31. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية (مصر)، 2002.

32. عبد الله ماجد العكايلة، الوجيز في الضبطية القضائية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2010.
33. عبد المجيد حلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الارهاب المعلوماتي - دورة تدريبية، مكافحة جرائم الارهاب المعلوماتي، المغرب، 2006.
34. علي عدنان الفيل، الاجرام الالكترونية، ط1، مكتبة زين الحقوقية والأدبية، لبنان، 2011.
35. عمر خوري، شرح قانون العقوبات، قسم العام، محاضرات جامعة الجزائر1، كلية الحقوق، السنة الجامعية 2010/2011.
36. غادة ناصر، الإرهاب والجريمة الالكترونية، العربي للنشر والتوزيع، القاهرة، 2017.
37. قندوشي ربيعة، الإعلام الإلكتروني، ط1، دار هومة للنشر والتوزيع الجزائر، 2012.
38. محمد عبيد الكعبي والجرائم المنشأة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة.
39. محمد حماد مرهج الهيتي، الجريمة المعلوماتية دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، مصر، 2014.
40. محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الأنترنت والأحكام الموضوعية والأحكام الجزائية، ط1، منشورات حلبي الحقوقية، بيروت، 2011.
41. محمد عبد الحميد عرفة، علم الإجرام والعقاب، دار المطبوعات الجامعية، الإسكندرية، بدون ذكر سنة النشر.
42. مريم محمد حسن، التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، كلية القانون، جامعة كوفة، العراق، 2016.
43. مريم محمد حسن، تنظيم القانوني لجريمة التجسس المعلومات، رسالة ماجستير، كلية القانون جامعة الكوفة، العراق، 2016.
44. مصطفى طاهر، المواجهة التشريعية لظاهرة غسيل الأموال متحصلة من جرائم المخدرات02، طبع على نفقة المؤلف، القاهرة، 2004.

45. مصطفى محمد موسى، الإرهاب الإلكتروني، دراسة قانونية، أمنية، نفسية، ط1، دار الكتب والوثائق المصرية، القاهرة.
46. منصور رحمانى، الوجيز في القانون الجنائي العام، د. ط.، دار العلوم للنشر والتوزيع، عناية 2006.
47. موسى مسعود أرحومة، إشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغربي الأول حول المعلوماتية والقانون، أكاديمية دراسات العليا، طرابلس 2009.
48. نبيلة هبة هروال، الجوانب الإجرائية الجرائم الكمبيوتر والأنترنت، في مرحلة جمع الاستدلالات، ط01، دار الفكر الجامعي، الإسكندرية، 2013.
49. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة لنشر والتوزيع، طبعة 02 ، دار وائل لنشر، الجزائر، 2010.
50. وليد الزيدي، القرصنة على الانترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة لنشر والتوزيع، الأردن، 2003.
51. يوسف شكري، المنظمات الدولية، ط1، دار الصفاء للنشر والتوزيع، عمان، 2012.
52. يونس عرب، جرائم الكمبيوتر والانترنت، ط1، اتحاد المصارف العربية ، بيروت ، 2002.

ثانيا: الرسائل والمذكرات الجامعية

أ/ دكتوراه

1. تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة دكتوراة الفلسفة الأمنية، كلية الدراسة العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

2. دار نسيم، الأمن المعلوماتي وسبل المواجهة مخاطر التعامل الإلكتروني، دراسة مقارنة، أطروحة الدكتوراة، كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017.

ب/ الماجستير

1. إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة لنيل درجة ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018.
2. عمر عباس، خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق جامعة تكريت، العراق، 2019.
3. صغير يوسف، الجرائم المرتكبة عبر الأنترنت، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري، الجزائر، 2013.
4. نور الله تله، الإرهاب بالوسائل الإلكترونية، مذكرة ماجستير في القانون الجزائي، كلية الحقوق، جامعة دمشق، 2015، 2016.
5. اسراء طارق جواد، كاظم الجابري، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، في القانون العام، كلية الحقوق جامعة النهرين، العراق، 2012.
6. أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، مذكرة لنيل درجة ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2008.
7. عمر عباس، خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2019.
8. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2017.

ج/ مذكرات الماستر

ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، السنة الجامعية 2015/2016.

ثالثا: المقالات العلمية

1. بوعنادة فاطمة الزهراء، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، 2013.
2. رمزي حوحو، التعاون الدولي لمكافحة جرائم الارهاب، مجلة الحقوق والعلوم السياسية، المجلد 03، العدد 03، جامعة زيان عاشور بالجلفة، كلية الحقوق والعلوم السياسية.
3. سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، جامعة الاخوة منتوري، قسنطينة، مجلة العلوم الانسانية، عدد 52، مجلد ب، ديسمبر 2019.
4. سلوى أحمد ميدان، الإرهاب والجهود الدولية لمكافحته، مجلة القانون للعلوم القانونية والسياسية، العراق، جامعة كركوك، العدد الخامس، 2016.
5. صالح بن محمد المسند وعبد الرحمن بن راشد المهني، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، العدد 29، المجلد 95، أبريل 2000.
6. عبد الله عبد العزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى مؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الانترنت المنعقد من 2 إلى 4 يونيو، القاهرة، مصر، 2008.
7. عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، ورقة مقدمة في الدولة التدريبية "مكافحة الجرائم الإرهابية المعلوماتية"، المغرب، 9، 13 أبريل 2006.

8. عز الدين عثمانى، اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث الدراسات القانونية والسياسية، مخبر المؤسسات النظم السياسية، العدد الرابع، جانفي 2018.
9. عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استراتيجية الأمن القومي، ورقة مقدمة الى مؤتمر الجرائم المستحدثة وكيفية اثباتها ومواجهتها ،المركز القومي للبحوث الاجتماعية والجنائية، مصر، 15/16/ديسمبر 2010.
10. عقلية هادي عيسى، اسراء جود حاتم " الارهاب المعلوماتي (الرقمي) وطرق مكافحته" ، المجلة السياسية والدولية، العراق، جامعة المستنصرية، العدد 2010.
11. محروس نصر غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، العدد 24 الاصدار 9، العراق، 2011.
12. محمد عبد المحسن سعدون، مفهوم إرهاب وتجريره في التشريعات الجنائية الوطنية والدولية، مجلة مركز الدراسات، الكوفة، العراق، جامعة الكوفة، 2008، العدد 07.
13. ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد 8، العدد 1، 2021.
14. نجيب بن عمر عوينات، الارهاب الالكتروني: مفهوم الجهود الدولية والاقليمية لمكافحته، مجلة الاستاذ الباحث لدراسات قانونية والسياسية، معهد العالي للإعلامية الكاف جامعة جندوية ، تونس، العدد 6.

رابعاً: المداخلات

1. حلف فاروق، الآليات القانونية لمكافحة الجريمة المعلوماتية، مداخله مقدمة في الملتقى حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، 16-17 نوفمبر 2015.

2. مجمع البحوث والدراسات الأكاديمية للسلطات قابوس لعلوم الشرطة ، الجريمة الإلكترونية، البحث الحائز على المركز الأول لمسابقة جائزة الأمير نايف عبد العزيز للبحوث الأمنية، عمان، 2016.

3. محمد سيد سلطان، الحماية الدولية والقانونية للبيئة الإلكترونية من الجريمة والإرهاب، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، منعقد في الرياض السعودية بتاريخ يومي 6 و 7 أبريل 2010.

رابعاً: النصوص القانونية

الاتفاقيات

1. اتفاقية مكافحة اساءة استعمال التكنولوجيا لأغراض اجرامية رقم 63/55 في 2000/04/12 الصادرة عن منظمة الأمم المتحدة، الجلسة العامة 04، 2000/12/81،
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، القاهرة لسنة 2010، انظمت إليه مصر سنة 2014.
3. اتفاقية بودابست المتعلقة بالجريمة المعلوماتية، المجلس الأوروبي، بودابست، بتاريخ 23 نوفمبر 2001.
4. الاتفاقية العربية لمكافحة تقنيات المعلومات، القاهرة، المصادق عليها بموجب المرسوم الرئاسي رقم 14-86 مؤرخ في 20 فيفري 2014، ج ر عدد 11 مؤرخة في 26 فيفري 2014.
5. قرار رقم 45/116، الجمعية العامة للأمم المتحدة، مؤرخ في 14 ديسمبر 1990،
المتعلق بتسليم المجرمين.
6. مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الأنترنت لأغراض إرهابية، لتقرير المنشور على الموقع <https://www.unodc.org>، تاريخ التصفح: 2026/04/12، الساعة 14:40.

I/ النصوص الوطنية

أ/ النصوص التشريعية

1. أمر رقم 66- 156 المؤرخ في 08 يوليو 1966 المتضمن قانون العقوبات، ج ر ، عدد 49 مؤرخ في 11 / 06 / 1966، المعدل والمتمم بموجب القانون 24-06 المؤرخ في 28 افريل 2024 ، ج.ر، عدد 30 المؤرخ في 30 افريل 2024 .
2. قانون رقم 09-04 المتعلق بالوقاية بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،الجريدة الرسمية العدد 47 الصادر في 5 اوت 2009.
3. قانون رقم 25-14 مؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، ج ر عدد 54 مؤرخة في 13 أوت 2025.
4. قانون رقم 04-15 مؤرخ في 10/11/2004، يتضمن قانون العقوبات، جريدة الرسمية، عدد 17، صادر في 10/11/2004.

II/ النصوص الأجنبية

1. القانون رقم 175 لسنة 2018 لمكافحة جرائم تقنية المعلومات المصري، وهو القانون التنفيذي للدستور المصري لسنة 2014.
2. القانون العربي الاسترشادي لمكافحة الجرائم التقنية، أنظمة المعلومات وما في حكمها، صادر عن الأمانة العامة لجامعة الدول العربية (القرار 417/2004).
3. النظام العودي لمكافحة الجرائم المعلوماتية ، الصادر بموجب المرسوم الملكي رقم (م/17 (المؤرخ 26 مارس 2007 .

فهرس المحتويات

الصفحة	العنوان
//	شكر وعرفان
//	اهداء
//	قائمة المختصرات
1	مقدمة
الفصل الأول الاطار المفاهيمي للإرهاب الإلكتروني	
8	المبحث الأول: مفهوم الإرهاب الإلكتروني
9	المطلب الأول: تعريف الإرهاب الإلكتروني
10	الفرع الأول: تعريف اللغوي والاصطلاحي
10	أولاً: التعريف اللغوي
11	ثانياً- التعريف الاصطلاحي.
13	الفرع الثاني: التعريف القانوني والفقهي
13	أولاً : التعريف القانوني
13	ثانياً: التعريف الفقهي
14	المطلب الثاني: خصائص الإرهاب الإلكتروني وتمييزه بالجرائم المشابهة
15	الفرع الأول: خصائص الإرهاب الإلكتروني
15	أولاً: الإرهاب الإلكتروني جريمة عابرة للحدود

قائمة المراجع

16	ثانيا: جرائم غير العنيفة
17	ثالثا: صعوبة الإثبات
18	رابعا: أسلوب ارتكاب الجريمة المعلوماتي
19	الفرع الثاني: تمييز الإرهاب الإلكتروني عن الجرائم المشابهة
19	أولا : الإرهاب العادي
20	ثانيا: الجريمة الإلكترونية
21	ثالثا: القرصنة
22	المبحث الثاني: أركان الإرهاب الإلكتروني وصوره
22	المطلب الأول : أركان الإرهاب الإلكتروني
23	الفرع الأول: الركن الشرعي
24	أولا : الركن الشرعي الوارد في المادة 87 مكرر
24	ثانيا: الركن الشرعي الوارد في المادة 394 مكرر
25	الفرع الثاني: الركن المادي
26	أولا: السلوك الإجرامي
27	ثانيا: النتيجة الإجرامية
28	الفرع الثالث: الركن المعنوي
28	أولا: انتفاء تصور الخطأ غير العمدى في جريمة الإرهاب الإلكتروني
29	ثانيا: القصد الجنائي العام
31	ثالثا: القصد الجنائي الخاص

31	المطلب الثاني : صور الإرهاب الإلكتروني
32	الفرع الأول: جريمة غسيل الأموال
32	أولاً: تعريف جريمة غسيل الأموال
33	ثانياً: علاقة الإرهاب الإلكتروني بجريمة غسيل الأموال
33	الفرع الثاني: جريمة التجسس الإلكتروني
35	الفرع الثالث: جريمة التهديد والقصف الإلكتروني
35	أولاً: التهديد الإلكتروني
36	ثانياً: القصف الإلكتروني
الفصل الثاني	
الجهود الدولية والوطنية لمكافحة الإرهاب الإلكتروني.	
39	المبحث الأول: الجهود الدولية والإقليمية لمكافحة الإرهاب الإلكتروني
40	المطلب الأول: الجهود الدولية لمكافحة الإرهاب الإلكتروني
40	الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية
41	أولاً: اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55 لسنة 2000
42	ثانياً: اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001
44	الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الدولية وآليات التعاون الدولي لمكافحتها
45	أولاً: مكافحة الإرهاب الإلكتروني في المنظمات الدولية

51	ثانيا: أليات التعاون الدولي لمكافحة الإرهاب الإلكتروني
56	المطلب الثاني: اتفاقيات والمنظمات الإقليمية في مكافحة الإرهاب الإلكتروني
57	الفرع الأول : الاتفاقيات الإقليمية لمكافحة الإرهاب الإلكتروني
57	أولا: اتفاقية الاتحاد الأفريقي لسنة 2014
58	ثانيا :الاتفاقية العربية لمكافحة الإرهاب الإلكتروني
61	الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الإقليمية
62	أولا: الاتحاد الأوروبي في مكافحة الإرهاب الإلكتروني
64	ثانيا: جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني
66	المبحث الثاني: الجهود الوطنية لمكافحة الإرهاب الإلكتروني
66	المطلب الأول: الأطر القانونية لمواجهة الإرهاب الإلكتروني في بعض الدول العربية والغربية
67	الفرع الأول: في الدول العربية
67	أولا: في التشريع الأردني
68	ثانيا: في التشريع المصري
69	الفرع الثاني: الدول الغربية لمكافحة الإرهاب الإلكتروني
69	أولا: الولايات المتحدة الأمريكية
70	ثانيا: فرنسا
72	المطلب الثاني: جهود الجزائر لمكافحة الإرهاب الإلكتروني
72	الفرع الأول: الإرهاب الإلكتروني في الجزائر

73	الفرع الثاني: مواجهة الإرهاب الإلكتروني في الجزائر
74	أولاً: الإجراءات العامة لمتابعة جريمة الإرهاب الإلكتروني
80	ثانياً: الإجراءات الخاصة لمكافحة الإرهاب الإلكتروني
87	خاتمة
91	قائمة المصادر والمراجع
102	فهرس المحتويات