AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW
ISSN:3006- 0605 DOI:10.58255

مكافحة النشاط الإرهابي في البيئة الرقمية "دراسة قانونية مقارنة"

Combating Terrorist Activity in the Digital Environmen" A Comparative Legal Study"

م.م كوثر عهد محمد مجيد
Assistant Lecturer Kawthar Ahed Mohammed Majid,
kawthar3hd@gmail.com

المستخلص : يتمحور هذا البحث حول مواجهة النشاط الإرهابي في البيئة الرقمية في القانونين العراقي والمصري، حيث يدرس الإطار المفاهيمي والأركان والآثار. يعرّف النشاط الإرهابي الرقمي كاستخدام تقني لتنفيذ أعمال إرهابية عبر الاختراق أو التمويل أو الدعاية، مستفيداً من خصائص الرقمية كعبور الحدود والتخفي. تقوم أركان هذه الجريمة على العنصر المادي (كالاختراق)، والمعنوي (القصد الإرهابي)، والوسيلة الرقمية، والتأثير العابر للحدود. تتنوع آثار هذا النشاط لتمس الأمن الوطني والاستقرار الاجتماعي والاقتصادي، حيث يهدد البنى التحتية ويزعزع الثقة بالخدمات الرقمية، في الوقت نفسه ينشر الرعب النفسي ويقوض الشرعية السياسية. يواجه القانونان المصري والعراقي هذه التحديات عبر تجريم هذه الأفعال وعقابها بشدة، مع السعي لموازنة متطلبات الأمن مع حماية الحريات في الفضاء الرقمي.

الكلمات المفتاحية: (الإرهاب، الرقمي، الإلكتروني، القانون، العراقي، المصري)

Abstract : This research focuses on countering terrorist activity in the digital environment under Iraqi and Egyptian law, examining the conceptual framework, elements, and implications. It defines digital terrorist activity as the use of technology to carry out terrorist acts through hacking, financing, or propaganda, leveraging digital features such as border crossing and concealment. The elements of this crime are based on the physical element (such as hacking), the moral element (terrorist intent), the digital means, and cross-border influence. The impact of this activity varies, from national security to social and economic stability, as it threatens infrastructure and undermines confidence in digital services, while simultaneously spreading psychological terror and undermining political legitimacy. Egyptian and Iraqi laws address these challenges by criminalizing and severely punishing such acts, while seeking to balance security requirements with protecting freedoms in the digital space. **Keywords: (terrorism, digital, electronic, law, Iraqi, Egyptian)**

المقدمة: تُعد البيئة الرقمية في العصر الحديث ساحة جديدة لمواجهة ظاهرة الإرهاب، التي تجاوزت الحدود المادية لتستغل الفضاء الإلكتروني في تحقيق أهدافها التخريبية. وقد أدرك كل من المشرع العراقي والمصري هذه التحولات الخطيرة، وسارعا إلى تطوير أطر قانونية متخصصة لمواجهة هذا التهديد المستحدث، يواجه القانونان تحدياً مشتركاً يتمثل في كيفية موازنة بين ضرورة الحفاظ على الأمن الوطني وسيادة الدولة من جهة، وحماية الحريات الرقمية وحقوق الأفراد من جهة أخرى. فالنشاط الإرهابي في الفضاء الإلكتروني لم يعد مجرد جرائم تقليدية، بل تحول إلى ظاهرة معقدة تتميز

بعبور الحدود وسرعة الانتشار والقدرة على الإيذاء عن بُعد، ويعتمد المشرع في كلا البلدين على مقاربة شاملة تجمع بين التجريم والعقاب من ناحية، والوقاية والمواجهة الاستباقية من ناحية أخرى، حيث يجرم القانون العراقي والمصري أنشطة مثل الاختراق بهدف إرهابي، وتمويل العمليات الإرهابية عبر الوسائل الرقمية، ونشر المحتوى المتطرف، مع فرض عقوبات مشددة تتناسب مع خطورة هذه الأفعال. تمتاز التجربة المصرية في هذا المجال بتركيزها على حماية البنى التحتية الحيوية وتعزيز التعاون الدولي، بينما تميل التجربة العراقية إلى معالجة الآثار المترتبة على الظروف الأمنية الاستثنائية التي مرت بها البلاد. ومع ذلك، يبقى كلا القانونين في تطور مستمر لمواكبة الأساليب المتغيرة للجماعات الإرهابية في الفضاء الرقمي.

أهمية البحث : يمثل البحث في آليات مكافحة النشاط الإرهابي في البيئة الرقمية أهمية بالغة على المستويين القانوني والأمني، حيث يأتي في ظل تحولات جذرية في طبيعة التهديدات الإرهابية التي لم تعد تقتصر على الفضاء المادي بل امتدت إلى العالم الافتراضي بكل تعقيداته.

مشكلة البحث: تتمحور مشكلة البحث الرئيسية حول التحديات القانونية والعملية التي تواجهها الدول في مواكبة التطور المتسارع للنشاط الإرهابي وراء البيئة الرقمية، حيث يتفوق الجناة تقنياً على الآليات القانونية التقليدية، ويتفرع عن هذه الإشكالية الرئيسة عدة أسئلة فرعية:

١- ما مفهوم مكافحة النشاط الإرهابي في البيئة الرقمية في القانونين العراقي والمصري؟

٢- ماهي أركان النشاط الإرهابي في البيئة الرقمية وما آثاره في القانونين العراقي والمصري؟

منهجية البحث: اعتمد هذا البحث على المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية ذات الصلة في كلا البلدين (قوانين مكافحة الإرهاب، الجرائم الإلكترونية، حماية البيانات)، وفهم السياق التشريعي لكل منها، مع تحليل المفاهيم الأساسية مثل "النشاط الإرهابي الرقمي" و"البيئة الرقمية"، كما اعتمدنا المنهج المقارن من خلال مُقارنة أوجه التشابه والاختلاف بين القانونين العراقي والمصري في تجريم النشاط الإرهابي الرقمي، والعقوبات المقررة، وآليات المكافحة، مع تقييم مدى مواكبة كل منهما للتحديات الحديثة.

خطة البحث: لمعالجة المشكلة الرئيسة تم تقسيم هذا البحث إلى مبحثين: المبحث الأول: مفهوم مكافحة النشاط الإرهابي في البيئة الرقمية في القانونين العراقي والمصري. المبحث الثاني: أركان النشاط الإرهابي في البيئة الرقمية وآثاره في القانونين العراقي والمصري.

المبحث الأول

مفهوم مكافحة النشاط الإرهابي في البيئة الرقمية في القانونين العراقي والمصري

يعكس مفهوم مكافحة النشاط الإرهابي في البيئة الرقمية في كل من القانون العراقي والقانون المصري تطوراً مهماً في استجابة التشريعات الوطنية للتحديات الحديثة التي فرضها عصر التكنولوجيا، ويجسد كلا القانونين إدراكاً واضحاً لتحول ساحة التهديد الإرهابي من العالم المادي إلى الفضاء الإلكتروني، حيث يتم استخدام المنصات الرقمية لأغراض متعددة وخطيرة، مثل التخطيط للهجمات، والتجنيد، ونشر الأيديولوجيات المتطرفة، وتمويل الأنشطة غير المشروعة، وتبادل

المعلومات[١] يرتكز المفهوم في كلا البلدين على ركيزتين رئيسيتين: الأولى هي التجريم، حيث يعمل القانون على تعريف الأفعال التي تشكل نشاطاً إرهابياً في الفضاء الإلكتروني وتحديد عقوبات رادعة لها. والثانية هي التمكين، حيث يمنح القانون سلطات واسعة لأجهزة الدولة المختصة (كجهاز مكافحة الإرهاب أو أجهزة الأمن الوطني) للرصد والمراقبة والتحقيق والملاحقة القضائية لهذه الجرائم[٢]، **بناءً على ما سبق، سندرس هذا المبحث في مطلبين وذلك وفق التقسيم الآتي:**

المطلب الأول

ماهية النشاط الإرهاب الرقمي وعناصره

مفهوم النشاط الإرهابي الرقمي هو مفهوم معقد يتجاوز الفكرة البسيطة عن الهجمات الإلكترونية التخريبية. فهو لا يقتصر على فعل تقني بحت، بل يُفهم على أنه تحوّل جوهري في التكتيكات والإستراتيجيات التي تتبناها الجماعات الإرهابية، حيث تصبح البيئة الرقمية فضاءً عضوياً لتحقيق أهدافها الأساسية المتمثلة في إثارة الرعب ونشر الأيديولوجيات المتطرفة وزعزعة استقرار المجتمعات والدول. في صلب هذا المفهوم تكمن فكرة الاستغلال الممنهج والشرير لإمكانيات الفضاء الإلكتروني، لا تميز الجماعات الإرهابية بين العالمين الافتراضي والمادي، بل ترى في الرقمية بيئة خصبة ومثالية لتكثيف أنشطتها بسبب طبيعتها العابرة للحدود، وسرعتها، وإتاحتها، وقدرتها على إضفاء طابع المجهولية[٣].

يتجلى هذا النشاط في عدة مستويات متداخلة تشكل دورة حياة متكاملة للعمليات الإرهابية. فهو يبدأ باستخدام المنصات الرقمية كأدوات فعالة للتجنيد والتلقين، حيث تستهدف هذه الجماعات الأفراد الضعفاء أو الباحثين عن هوية، وتغمرهم بمحتوى دعائي مصمم بعناية (مقاطع فيديو، منشورات، بث مباشر) يمجّد العنف ويشوه المعتقدات السلمية ويبني حالة من الولاء الأعمى[٤].

بالتوازي مع ذلك، يصبح الفضاء الرقمي السيناريو الرئيسي لعمليات التمويل، من خلال طرق متخفية مثل طلب التبرعات عبر منصات مشفرة، أو ابتزاز الأموال، أو حتى تنظيم عمليات نصب واحتيال مالي لتمويل عملياتها. كما تتحول غرف الدردشة الخاصة وتطبيقات المراسلة المشفرة إلى قاعات حرب افتراضية للتخطيط والتنسيق للهجمات المادية، حيث يتم تبادل التعليمات والتخطيط للعمليات وتجنيد العناصر منخفضة المستوى دون الحاجة إلى اللقاء الجسدي، مما يزيد من صعوبة اكتشافها[٥]. كما يرتكز المفهوم في البلدين على فلسفةٍ قانونيةٍ مزدوجة؛ تتمثّل الركيزة الأولى في التجريم الاستباقي والرادع، حيث يسعى المشرّع إلى تعريف الأفعال التي تشكّل جرائم إرهابية رقمية بطريقةٍ واسعةٍ وشاملةٍ لتغطية كافة الأنشطة التي يمكن أن تقع في هذا الإطار، مع فرض عقوباتٍ مشدّدةٍ تصل إلى السجن المؤبد أو الإعدام في بعض

---

[١] حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالي، بغداد، ٢٠١٣، ص٣٢٦.

[٢] حامد البياتي، الإرهاب في العراق وخطورة انتقاله إلى المنطقة والعالم، ط١، مؤسسة شهيد المحراب للتبليغ الإسلامي، بغداد، ٢٠٠٥، ص٦٤.

[٣] صالح العادلي، موسوعة القانون الجزائي للإرهاب، دار الفكر العربي، القاهرة، ٢٠٠٣، ص٢١١.

[٤] حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مرجع سابق، ص٣٢٩.

[٥] صالح العادلي، موسوعة القانون الجزائي للإرهاب، مرجع سابق، ص٢٣١.

الجرائم، انطلاقاً من اعتبار أن الجريمة الإلكترونية الإرهابية جريمةً غير عاديةٍ تستدعي عقوباتٍ غير عادية[١]، فقد أكد المشرع العراقي في قانون الجرائم الإلكترونية العراقي رقم (٥) لسنــة ٢٠٢٣: يمثل هذا القانون الإضافة الأكثر أهمية والأساس القانوني الأكثر تحديداً لمحاربة الإرهاب في البيئة الرقمية، حيث خصص فصلاً كاملاً للجرائم الإرهابية[٢]. أما المشرع المصري فقد أكد في قانون مكافحة تقنية المعلومات (الجريمة الإلكترونية) رقم (١٧٥) لسنة ٢٠١٨ على تجريم الأنشطة الأساسية التي تتم عبر الإنترنت، مثل الاختراق، وانتحال الشخصية، وإنشاء المواقع لغرض الاحتيال أو الإضرار بالأمن القومي[٣]. أما الركيزة الثانية فهي التمكين الإجرائي للأجهزة الأمنية، حيث يمنح القانون سلطاتٍ استثنائيةٍ لأجهزة مكافحة الإرهاب والأمن الوطني تتيح لها تتبع النشاط الإرهابي عبر الشبكة، ومراقبة المحتوى، وطلب بيانات المستخدمين من مقدمي الخدمة، وحظر المواقع والمنصات التي تنشر الفكر المتطرف، وذلك في إطار سعيه لموازنة متطلبات المواجهة الأمنية مع الحفاظ على الأمن القومي.

على الرغم من هذا التقاطع في الأهداف العامة، إلا أن السياقين العراقي والمصري يمنحان لهذا المفهوم نكهةً خاصةً في كل بلد. ففي العراق، يأخذ المفهوم طابعاً عملياتياً مباشراً، متأثراً بتجربته المباشرة والدامية في مواجهة تنظيمات إرهابية مثل داعش، والتي اعتمدت بشكلٍ لافتٍ على الفضاء الرقمي في الترويج والتجنيد. لذلك، يركز المنظور العراقي أكثر على حماية الوحدة الوطنية وسيادة الدولة من خلال كبح أي تحريض رقمي يمكن أن يهدد الاستقرار الأمني الهش. بالمقابل، في مصر، يتسع نطاق المفهوم ليشمل حماية الأمن المجتمعي والفكري بشكلٍ أوسع، حيث يتم التركيز على مكافحة خطاب الكراهية ونشر الشائعات الكاذبة التي من شأنها تحريض المواطنين على العنف أو النيل من هيبة الدولة ومؤسساتها. كما يظهر اهتمامٌ واضحٌ بحماية البنية التحتية المعلوماتية الحيوية من الهجمات الإلكترونية التي يمكن أن تصنف كأعمال إرهابية[٤].

بشكلٍ جوهري، يواجه التطبيق العملي لهذا المفهوم في كلا البلدين التحدي نفسه، وهو إيجاد التوازن الدقيق بين ضرورة منح الأجهزة الأمنية الأدوات الكافية لمحاربة تهديدٍ خفي ومعقّد، وواجب حماية حقوق الخصوصية والحريات الفردية التي يكفلها الدستور، مما يفتح باب نقاشٍ مجتمعي وقانوني حول حدود هذه الصلاحيات وإمكانية إساءة استخدامها.

أما عناصر النشاط الإرهاب الرقمي: يُعتبر العنصر البشري الحلقة الأكثر تعقيداً وحساسية في معادلة مكافحة النشاط الإرهابي الرقمي، فهو ليس مجرد طرف في هذه المعادلة، بل هو المحور الأساسي الذي تدور حوله كافة الجهود، سواء

---

[١] محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة ،٢٠٠٣، ص٧١.

[٢] ينظر: قانون الجرائم الإلكترونية العراقي رقم (٥) لسنــة ٢٠٢٣المادة (١١): تنص على: (أولاً): يعاقب بالسجن مدة لا تقل عن خمس عشرة سنة وبالغرامة التي لا تقل عن خمسين مليون دينار ولا تزيد على مائة مليون دينار أو بإحدى هاتين العقوبتين، كل من أنشأ أو استخدم موقعاً إلكترونياً أو حساباً أو مجموعة الكترونية لأغراض إرهابية.

[٣] ينظر: قانون مكافحة تقنية المعلومات (الجريمة الإلكترونية) رقم (١٧٥) لسنة ٢٠١٨ المادة (٧): تعاقب بالسجن مدة لا تقل عن سنتين وبغرامة لا تقل عن ١٠٠ ألف جنيه ولا تزيد على ٣٠٠ ألف جنيه كل من أنشأ أو استخدم موقعاً الكترونياً أو حساباً الكترونياً لأغراض إرهابية.

[٤] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت الأحكام الموضوعية والجوانب الإجرائية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٩٤.

كان ضحيةَ، أو جانيَ، أو مدافعاً.[١] فمن ناحية، يمثل الأفراد الهدف الأساسي للجماعات الإرهابية في الفضاء الرقمي، فهم ضحايا التجنيد والاستقطاب، حيث تستغل هذه الجماعات نقاط الضعف النفسي أو الاجتماعي أو الفكري لديها، كالشعور بالاغتراب، أو البحث عن هوية، أو اليأس الاقتصادي، لتحويلهم من مستخدمين عاديين إلى أدوات فاعلة في آلة العنف. وهنا يبرز تحدي حماية الإنسان من نفسه، أي من تأثره بالخطاب المتطرف الذي يغذي الروح العدوانية ويشوه صورة الآخر.

وفي الجهة المقابلة، يقف العنصر البشري في جهاز الدولة، من عناصر أمنية وقضائية ومحققين رقميين، كخط الدفاع الأول، هؤلاء لا يعتمدون فقط على التقنيات المتطورة في التتبع والمراقبة، بل على الذكاء البشري، والخبرة التحليلية، والفهم العميق لآليات التفكير المتطرف وسيكولوجية الإرهابي. قدرتهم على تفسير البيانات ضمن سياقها الثقافي والاجتماعي، وليس مجرد معالجتها آلياً، هي ما يصنع الفرق بين مجرد جمع المعلومات وبين تفكيك شبكة إرهابية.

كما يتسع النطاق ليشمل عنصر التمويل الرقمي، حيث يعاقب القانون على جمع أو تحويل الأموال عبر الوسائل الإلكترونية أو المشفرة عندما يكون الغرض منها تمويل الأنشطة الإرهابية، حتى لو كان ذلك تحت مسميات خداعة مثل التبرعات الخيرية. ويعتبر هذا العنصر من أخطر الأنشطة لكونه الشريان الحيوي الذي يضمن استمرارية التنظيمات الإرهابية[٢]. أيضاً، يعد التخطيط والتحريض الرقمي عنصراً جوهرياً، حيث يتم تجريم استخدام شبكات التواصل أو تطبيقات المراسلة لتخطيط هجمات إرهابية ملموسة أو التحريض المباشر على ارتكابها، حتى لو لم ينتج عن هذا التحريض فعل فوري، انطلاقاً من نظرية الجريمة غير المكتملة والتي تعاقب على البدء في التنفيذ.

لا يغفل المشرع عنصر القرصنة الإلكترونية الموجهة ضد أجهزة الدولة الحيوية أو البنية التحتية المعلوماتية، إذا كان الهدف منها إحداث ضرر يجبر الدولة على تنفيذ أمر معين أو بهدف بث الرعب بين المواطنين، كما يدخل في نطاق التجريم أنشطة أخرى مثل انتحال هوية مؤسسات الدولة أو الشخصيات العامة عبر الإنترنت لنشر أخبار كاذبة من شأنها إثارة الفتنة أو زعزعة الثقة في السلطات[٣]وهكذا، فإن العناصر لا تُفهم كقائمة منفصلة، بل كنسيج متشابك من الأفعال التي يعاقب عليها القانون لمجرد صلتها بالإرهاب،بهدف سد أي ثغرة قد تستغلها التنظيمات الإرهابية في العالم الافتراضي.

المطلب الثاني

خصائص البيئة الرقمية للنشاط الإرهابي

تتميز البيئة الرقمية التي تعمل فيها الجماعات الإرهابية بمجموعة من الخصائص الفريدة التي تجعلها بيئة خصبة للنشاط الإرهابي، **ومن أبرز هذه الخصائص:**

---

[١] علي هادي حميدي الشكراوي ،الأحزاب السياسية و حماية القواعد الدستورية ، دراسة مقارنة ، مجلة بابل للعلوم الإنسانية تصدرها كلية التربية جامعة بابل ، العدد الحادي عشر ، ٢٠٠٧، ص٢٣٣.

[٢] سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجزائي، أطروحة دكتوراه، كلية القانون، جامعة الموصل، ٢٠٠٦، ص١٦٨.

[٣] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص١٨٦.

أولاً– اللاحدودية والعالمية : تعتبر خاصية اللاحدودية والعالمية من أعمق الخصائص التي تميز البيئة الرقمية، حيث تذوب فيها الحواجز الجغرافية والسيادية التقليدية للدول، فالجريمة الإرهابية لم تعد تحتاج إلى عبور حدود مادية، بل يمكن التخطيط لها من أي مكان في العالم وتنفيذ آثارها في مكان آخر، مما يخلق إشكالية قانونية كبيرة تتعلق بالاختصاص القضائي والسيادة الوطنية[١]. في مواجهة هذا التحدي، اتجه المشرع في كل من العراق ومصر إلى تبني استراتيجية قانونية ذكية تقوم على توسيع نطاق الاختصاص القضائي لمواكبة هذا الطابع العابر للحدود. فلم يعد ارتباط الجريمة بإقليم الدولة هو المعيار الوحيد لمحاكمة مرتكبيها.

ففي القانون المصري، نجد أن المشرع قد وسع نطاق تطبيق القانون ليشمل الجرائم الإرهابية التي ترتكب خارج إقليم الجمهورية إذا كان لها آثار تمس الأمن القومي المصري أو تستهدف مصالح الدولة أو رعاياها في الخارج. كما يعاقب القانون كل مصري أو أجنبي مقيم في مصر يرتكب خارجها فعلاً إرهابياً يعاقب عليه القانون المصري[٢].

أما في القانون العراقي، والذي وُضع في ظل ظروف تهديد إرهابي عابر للحدود بشكل مباشر، فقد اعتمد على مبدأين: الأول هو اختصاص القضاء العراقي بالنظر في الجرائم الإرهابية التي تمس أمن الدولة وسلامتها، بغض النظر عن مكان وقوعها الفعلي أو جنسية الفاعل، طالما كان هناك تأثير على الأمن العراقي. والمبدأ الثاني هو التأكيد على أهمية التعاون القضائي والأمني الدولي كأداة لا غنى عنها لملاحقة العناصر الإرهابية التي تعمل من ملاذات آمنة خارج الحدود، وذلك من خلال اتفاقيات التسليم والمساعدة المتبادلة[٣].

ثانياً– إمكانية التخفي والتمويه تمثل خاصية إمكانية التخفي والتمويه في البيئة الرقمية تحدياً جوهرياً لاجهزة مكافحة الإرهاب، حيث تتيح هذه الخاصية للجماعات الإرهابية إخفاء هوياتها وأنشطتها باستخدام أدوات مثل الشبكات المظلمة، وتقنيات التشفير القوية، والهويات الوهمية، والعملات الرقمية المشفرة التي تعمل على إضفاء طابع المجهولية على المعاملات المالية[٤]. لمواجهة هذا التحدي، اتجه المشرع في كل من العراق ومصر إلى منح السلطات المختصة صلاحيات استثنائية تمكنها من اختراق هذا الحجاب من التخفي. ففي القانون المصري، تم تجريم استخدام وسائل التشفير أو التقنيات التي تساعد على إخفاء الهوية بهدف ارتكاب أو التخطيط لأعمال إرهابية. كما يلزم القانون مقدمي خدمات الاتصالات والإنترنت بالاحتفاظ ببيانات المستخدمين وتسليمها للسلطات المختصة في إطار التحقيقات الأمنية، مما يمكن الأجهزة الأمنية من تتبع هويات المستخدمين الحقيقية خلف الأسماء المستعارة.

أما في القانون العراقي، فقد تم تعزيز قدرات الجهات الأمنية في مجال المراقبة الإلكترونية والتحقيق الجنائي الرقمي، حيث يسمح القانون لها بمراقبة الاتصالات الإلكترونية واعتراضها بعد الحصول على إذن قضائي مسبق. كما يعمل القانون

---

[١] سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجزائي، مرجع سابق، ص١٨٣.

[٢] محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، مرجع سابق، ص٢١٣.

[٣] مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، بحث منشور العراق، في مجلة العلوم القانونية والسياسية، جامعة ديالى العدد الأول، المجلد الثالث، بغداد، ٢٠١٤، ص١٣٨.

[٤] محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، مرجع سابق، ص٢٢٧.

على تجريم تمويل الإرهاب عبر العملات المشفرة وغيرها من الوسائل الرقمية التي تستغل خاصية التخفي، وذلك بهدف قطع الشريان المالي للجماعات الإرهابية الذي يعتمد بشكل متزايد على هذه التقنيات.

ثالثاً– السرعة والفورية تمثل خاصية السرعة والفورية سمة محورية في البيئة الرقمية، حيث تتيح للجماعات الإرهابية نشر أفكارها وتوجيهاتها وتنفيذ عملياتها في لحظات، عبر منصات التواصل الاجتماعي وتطبيقات المراسلة الفورية. هذه السرعة تعطيها ميزة تكتيكية كبيرة، وتجعل عملية المواجهة تشبه سباقاً ضد الزمن.

لمواجهة هذا التحدي، اتجه المشرع في كل من العراق ومصر إلى اعتماد آليات استجابة سريعة وقائية واستباقية، ففي القانون المصري، تم منح السلطات المختصة صلاحية التصدي الفوري للمحتوى الإرهابي عبر طلب حظر المواقع أو الحسابات التي تنشر مواد إرهابية، أو حتى فرض حظر شامل على تطبيقات معينة في حال ثبت استخدامها بشكل مكثف في أنشطة إرهابية، وذلك بهدف كسر دائرة الانتشار السريع للمحتوى المتطرف قبل تحوله إلى ظاهرة[١].

أما في القانون العراقي، الذي يواجه تهديداً إرهابياً مباشراً ومستمراً، فقد ركز على تفعيل ما يُعرف بـ "الفرق الإلكترونية" المتخصصة في الرصد والمراقبة على مدار الساعة. تتمتع هذه الفرق بصلاحية التدخل العاجل لحذف المحتوى الإرهابي أو تعطيل حسابات نشطة تنشر خطاب الكراهية أو تخطط لهجمات، بالتعاون مع مقدمي الخدمات، مما يحد من تأثير السرعة التي تتمتع بها هذه الجماعات. كما يعمل كلا القانونين على تجريم ما يُسمى بـ "الجريمة المستمرة"، حيث يعتبر النشر المستمر للمادة الإرهابية جريمة قائمة بذاتها، مما يسمح للسلطات بالتدخل في أي لحظة طالما استمر النشاط الإجرامي، وذلك لمواكبة الطبيعة المتجددة والمستمرة للنشاط الإرهابي الرقمي.

رابعاً– التكلفة المنخفضة اتجه المشرع في كل من العراق ومصر إلى تطوير آليات قانونية تركز على تجريم ومحاصرة الأنشطة التمويلية ذات التكلفة المنخفضة التي تعتمد على الوسائل الرقمية. ففي القانون المصري، تم تجريم حيازة أو جمع أو تقديم الأموال أو المقومات المالية بأي طريقة كانت، بما في ذلك الطرق الإلكترونية البسيطة والمتاحة، إذا كان القصد منها تمويل أنشطة إرهابية. كما يعمل القانون على ملاحقة ومنع الحملات التمويلية عبر المنصات الإلكترونية التي تستغل سهولة إنشائها وانخفاض تكلفتها[٢].

أما في القانون العراقي، فقد تم التركيز على تعقب المعاملات المالية الإلكترونية المشبوهة، بما في ذلك التحويلات الصغيرة عبر القنوات الرقمية، والتي قد تستخدم لتمويل العمليات الإرهابية. كما يسعى القانون إلى تفكيك الشبكات الافتراضية التي تعتمد على موارد محدودة، من خلال تجريم إنشاء أو إدارة أي منصة رقمية أو مجموعة الكترونية بهدف دعم أو تمويل الإرهاب، حتى لو كانت تكلفة إنشائها لا تذكر[٣].

خامساً– التفاعلية والتأثير النفسي في مواجهة هذا التحدي المعقد، اتجه المشرع في كل من العراق ومصر إلى تطوير أطر قانونية تركز على تجريم العمليات النفسية والتأثيرية التي تمارسها الجماعات الإرهابية. ففي القانون المصري، تم

---

[١] سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجزائي، مرجع سابق، ص٢٦١.

[٢] أحمد كيلان عبد الله، حجية المحررات المستخرجة من الحاسوب في الإثبات الجنائي : أطروحة دكتوراه ، جامعة بغداد، كلية القانون، العراق، ٢٠٠٧، ص٩٦.

[٣] عادل يحيى، السياسة الجزائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠١٤، ص٢١٧.

تجريم ليس فقط الدعوة المباشرة للعنف، ولكن أيضاً خطاب الكراهية ونشر الشائعات والأخبار الكاذبة التي من شأنها الإضرار بالأمن الوطني أو الوحدة الاجتماعية أو النيل من هيبة الدولة. هذا يشمل المحتوى الذي يستخدم لخلق حالة من الخوف أو الذعر أوالفتنة بين أفراد المجتمع، انطلاقاً من إدراك أن الحرب النفسية هي تمهيد أساسي للتجنيد والتعبئة[١].

أما في القانون العراقي، الذي يواجه واقعاً طائفياً معقداً، فقد أولى اهتماماً خاصاً لتجريم أي محتوى رقمي يهدف إلى التحريض على العنف الطائفي أو العرقي، أو يعمل على زعزعة الثقة بين مكونات المجتمع العراقي. كما يعاقب القانون على إنشاء أو إدارة المجموعات والحسابات التفاعلية التي تستخدم للتلاعب بالوعي الجمعي أو غسل الأدمغة أو تعبئة الأفراد نحو العنف[٢].

سادساً– التطور المستمر في مواجهة هذا التحدي المتجدد، اتجه المشرع في كل من العراق ومصر إلى اعتماد منهجية مرنة في الصياغة القانونية. فبدلاً من حصر التجريم في أدوات أو تقنيات محددة، تم استخدام تعريفات واسعة وشاملة للأفعال الإرهابية الرقمية. ففي القانون المصري، يُعرف النشاط الإرهابي بتعميد ليشمل أي استخدام للتقنية المعلوماتية بهدف الإضرار بالوحدة الوطنية أو تعطيل أحكام الدستور، مما يسمح بتطبيق النص على أدوات المستقبل التي لم تكن موجودة وقت التشريع.

اعتمد القانون العراقي، على مفهوم "الجرائم الإلكترونية ذات الطابع الإرهابي" كمظلة شاملة، مع منح القضاء صلاحية تفسير النصوص وتكييف الأفعال الجديدة معها، استناداً إلى القصد الإجرامي والغاية من الفعل وليس فقط الوسيلة المستخدمة[٣]، كما عمل المشرع في البلدين على تضمين نصوص تسمح باستحداث آليات مكافحة جديدة دون الحاجة لتعديل القانون الأساسي، وذلك من خلال تفويض الجهات التنفيذية المختصة (كمجلس الأمن الوطني أو وزارة الداخلية) بإصدار بروتوكولات عمل متجددة للتعامل مع التهديدات المستجدة، في إطار السياسة العامة للدولة لمكافحة الإرهاب.

وبشكل جوهري، يمكن القول إن الاستجابة لهذه الخاصية لم تكن تقنية فحسب، بل فلسفية في جوهرها، حيث انتقل المشرع من منطق تجريم الوسائل إلى منطق تجريم الغاية والوظيفة الإرهابية لأي نشاط رقمي، مما يخلق تشريعاً حياً قادراً على مسايرة تطورات المستقبل.

المبحث الثاني

أركان النشاط الإرهابي في البيئة الرقمية وآثاره في القانونين العراقي والمصري

يتشكل النشاط الإرهابي في البيئة الرقمية من خلال عدة أركان مترابطة تبدأ بالركن المادي الذي يتمثل في الفعل الإجرامي ذاته، سواء كان ذلك بالتواصل والتخطيط للعمليات الإرهابية، أو بتجنيد الأفراد ونشر الأفكار المتطرفة، أو بجمع التبرعات وتمويل الأنشطة المحظورة، أو حتى بالهجوم المباشر على البنى التحتية المعلوماتية للدولة عبر الاختراق أو تعطيل الأنظمة. ويقوم هذا الركن على استغلال الخصائص الفريدة للفضاء الإلكتروني من سرية وانتشار عالمي وسهولة في

---

[١] مصطفى محمد موسى، الإرهاب الإلكتروني، ط١، مطابع الشرطة، القاهرة، ٢٠٠٩، ص٤١.

[٢] مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، مرجع سابق، ص١٤٩.

[٣] نضال ياسين الحاج حمو، دراسة السلوك في التشريع العراقي، بحث منشور في مجلة القضاء، العدد (١-٤)، السنة (٥٣)، بغداد، ٢٠٠٣، ص٣٣١.

الوصول لإحداث الضرر[١]. وفيما يخص الآثار القانونية، فإن التشريعين العراقي والمصري يتفقان على تجريم هذا النشاط وفرض عقوبات مشددة عليه، وإن اختلفت الصياغة والنطاق. ففي القانون المصري، ينظر إلى الجريمة الإرهابية الإلكترونية كخطر داهم على أمن الدولة القومي.[٢] أما في القانون العراقي، والذي تشكل في ظل ظروف مواجهة تنظيمات إرهابية عنيفة، فإن التأكيد ينصب على مكافحة كل أشكال الإرهاب بما فيها الرقمية، حيث يعاقب مرتكبها بعقوبات تصل إلى الإعدام أو السجن المؤبد. وعليه سندرس هذا التفصيل من خلال مطلبين وذلك وفق الاتي:

المطلب الأول

أركان النشاط الإرهابي في البيئة الرقمية

يشكل النشاط الإرهابي في البيئة الرقمية تحديًا معقدًا للأنظمة القانونية والأمنية المعاصرة، حيث يتطلب فهمه وتحليله تحديد أركانه الأساسية التي تميزه عن غيره من الأنشطة غير المشروعة في الفضاء الإلكتروني، وهذه الأركان تتمثل بالآتي:

أولاً– الركن المادي (السلوك الإجرامي) يتمثل الركن المادي للنشاط الإرهابي في البيئة الرقمية في مجموعة الأفعال الملموسة والمحسوسة التي يقوم بها الجاني باستخدام الوسائل التكنولوجية، والتي تشكل جريمة إرهابية بمفهوم القانون. لا يقتصر هذا الركن على فعل واحد بل يتسع ليشمل أي استخدام للفضاء الإلكتروني لتسهيل أو تنفيذ الأهداف الإرهابية[٣].

يتجلى هذا الركن عبر سلوكيات متعددة مثل استخدام منصات التواصل أو تطبيقات المراسلة المشفرة للتخطيط للعمليات الإرهابية وتنسيقها بين العناصر، أو إنشاء مجموعات ونشر محتوى متطرف بهدف التجنيد الفكري واستقطاب الأفراد وغسل أدمغتهم، أو إنشاء مواقع ومنتديات لتمويل الأنشطة المحظورة من خلال طلب التبرعات وتحويل الأموال بشكل سري، أو الهجوم المباشر على شبكات الحاسوب والبنى التحتية المعلوماتية الحيوية للدولة عبر اختراقها أو تعطيلها أو تدمير البيانات فيها، وهو ما يعرف بالإرهاب الإلكتروني المباشر الذي يمكن أن يسبب شللاً كاملاً لقطاعات حيوية كالطاقة والاتصالات والمال[٤].

يشمل هذا الركن أيضاً حيازة أو تطوير أو توزيع برمجيات خبيثة مصممة خصيصاً لتنفيذ هذه الهجمات، وكذلك بث الدعاية والتهديد عبر الإنترنت لنشر الرعب بين الجمهور وإرهاب الشخصيات العامة. يعتمد تحقق هذا الركن على الاستفادة من الطبيعة العابرة للحدود والسرعة والتخفي التي توفرها البيئة الرقمية، مما يجعل الفعل الإجرامي ممكناً بغض النظر عن الموقع الجغرافي للجاني. فالركن المادي يتمثل في الأفعال الملموسة التي تُرتكب باستخدام الوسائل الرقمية، مثل الاختراق، أو نشر محتوى متطرف، أو تمويل الإرهاب إلكترونيًا، أو التخطيط للهجمات عبر منصات التواصل. يعاقب القانون المصري والعراقي هذه الأفعال بعقوبات مشددة تصل إلى السجن المؤبد أو الإعدام في حالات الخطورة البالغة، خاصة إذا نتج عنها أضرار جسيمة أو وفيات.

---

[١] هاشم حسن التميمي ، دور الاعلام في مكافحة الإرهاب» مجلة العلوم السياسية العراق جامعة بغداد العدد ٤، ٢٠١٥، ص٤١٧.

[٢] أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ٢٠٠٧، ص٨٣.

[٣] مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، مرجع سابق، ص١٥٦.

[٤] طارق سرور، الجماعة الإجرامية المنظمة، دار النهضة العربية، القاهرة، ٢٠٠٠، ص٢٣٦.

ثانياً- الركن المعنوي (القصد الجنائي) يتمثل الركن المعنوي للنشاط الإرهابي في البيئة الرقمية في البنية النفسية والنية الجرمية التي تستند عليها الأفعال المادية، والتي تميز الجريمة الإرهابية عن غيرها من الجرائم الإلكترونية العادية.

فلا يكفي مجرد إثبات قيام الشخص بنشر محتوى أو اختراق نظام ما، بل يجب إثبات أن ذلك تم بعلم وإرادة وبتوجه نية خاصة. حيث يتطلب توافر القصد الجنائي الخاص، الذي يعني أن يكون هدف الجاني المقصود والرئيسي من فعله هو خدمة غاية إرهابية، كتخويد الجمهور أو زعزعة أمن البلاد أو الاستقلال بأراضيها أو تعطيل أحكام الدستور أو القوانين، أو منع مؤسسات الدولة من ممارسة عملها[١].

كما يتجلى هذا الركن في الدافع الإرهابي، وهو العنصر الذي يوضح التوجه الفكري والمعتقدي للجاني، حيث يكون مدفوعاً بأيديولوجية متطرفة تدفعه إلى استخدام الفضاء الرقمي كأداة لتحقيق أهداف تلك الجماعة أو الفكر، حتى لو لم ينتمِ لها رسمياً. وهذا يعني أن الجريمة لا تقع عمداً فحسب، بل تقع بقصد إرهابي محدد.

ويمتد ليشمل العلم والارتباط، حيث يكون الجاني على علم تام بأن نشاطه الرقمي، سواء كان التمويل أو الدعاية، يساهم في دعم عمل إرهابي، ويتوافق مع أهدافه، حتى لو كان بعيداً عن تنفيذ العمليات الميدانية مباشرة. وبذلك، فإن القصد الجرمي في الجرائم الإرهابية الإلكترونية أعمق وأخطر من مجرد القصد العام في الجرائم التقليدية، لأنه يستهدف إلحاق الضرر بالكيان الوطني والمجتمع ككل[٢]. اذاً، يشير إلى النية والدافع وراء الفعل الإجرامي، حيث يجب إثبات أن الجاني قصد من خلال نشاطه الرقمي تحقيق غاية إرهابية، مثل نشر الرعب أو زعزعة أمن الدولة، يُعتبر هذا الركن حاسمًا في التمييز بين الجريمة الإرهابية والجريمة الإلكترونية العادية، كلا القانونين (المصري والعراقي) يشددان على ضرورة توافر القصد الجنائي الخاص لوصف الفعل بأنه إرهابي[٣].

وبعد دراسة الركنين المادي والمعنوي لابد من الولوج في الرابطة السببية، حيث أنه لتكوين الرابطة السببية، يجب إثبات أن الركن المعنوي (نية الترويع أو الإضرار بأمن الدولة) هو الذي دفع بشكل مباشر إلى ارتكاب الركن المادي (الفعل الإلكتروني) الذي أنتج النتيجة الإرهابية أو ساهم فيها مساهمة جذرية[٤].

ثالثاً- الوسيلة الرقمية تُشكّل الوسيلة الرقمية العمود الفقري الذي يُميز هذا النوع من الجرائم، فهي ليست مجرد أداة محايدة بل هي البيئة التي تحتضن الفعل الإرهابي وتُضاعف من آثاره. إن جوهر الركن المادي يكمن في استغلال الخصائص الفريدة لهذه الوسائل لتحقيق الأهداف الإرهابية. تتمثل هذه الوسيلة في استثمار كل ما يتصل بالفضاء الإلكتروني من أدوات اتصال وتقنيات رقمية، حيث يعتمد الإرهابيون على منصات التواصل المغلقة والمشفرة لإجراء اتصالاتهم وتنسيق خططهم بعيداً عن أعين الرقابة، مستفيدين من خاصية التخفي والسرعة. كما يلجأون إلى إنشاء مواقع ويب ومدونات ومنتديات خفية لنشر أفكارهم المتطرفة وتجنيد المؤيدين، مستغلين قدرة الشبكة على الوصول إلى جمهور

---

[١] جمال إبراهيم الحيدري، الوافي في القسم العام، قانون العقوبات، الطبعة الأولى، مكتبة السنهوري، بغداد، ٢٠١٢، ص١٦٢.

[٢] كريم مزعل شلبي ، مفهوم الإرهاب دراسة في القانون الدولي والداخلي، مجلة أهل البيت، جامعة الكربلاء، العدد ٤، بغداد، ٢٠١٦، ص٣٤٦.

[٣] بوادي حسنين، المنظومة الأمنية في مواجهة الإرهابية، دار الفكر العربي، الإسكندرية، مصر، ٢٠٠٧، ص١٦٩.

[٤] أسامة أحمد المناعسة و جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط٢، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٤، ص١٣٢.

عالمي غير محدود[١]. وتمتد الوسيلة ليشمل استخدام تطبيقات تحويل الأموال الإلكترونية والعملات المشفرة لجمع التبرعات وتمويل العمليات بسرية تامة، علاوة على استغلال منصات مشاركة المحتوى لبث التسجيلات التهديدية والدعائية لنشر الرعب وإرهاب الآمنين. كما تتجلى في تطوير واستخدام البرمجيات الخبيثة وبرامج الاختراق لتعطيل الأنظمة الحيوية للدولة أو اختراق قواعد البيانات الحساسة، مما يحول البنية التحتية الرقمية نفسها إلى ساحة للهجوم المباشر.

رابعاً- التأثير العابر للحدود يُعد التأثير العابر للحدود السمة الجوهرية التي تطبع النشاط الإرهابي في البيئة الرقمية وتضاعف من خطورته، حيث يذوب فيه مفهوم السيادة التقليدي للدولة. فالفعل الإجرامي الذي ينشأ من نقطة جغرافية محددة يمكن أن تمتد آثاره لتطال أمن وسلامة دول أخرى بعيدة، دون أن يحتاج الفاعل إلى عبور حدود مادية.

تتجلى هذه السمة في قدرة الإرهابي على الجلوس في دولة ما لاستهداف البنية التحتية الحيوية لدولة أخرى، كاختراق شبكات الطاقة أو الأنظمة المالية، مما يخلق وضعاً يتعذر معه تطبيق القوانين المحلية وحدها. كما أن عملية التجنيد الفكري لم تعد محصورة في نطاق إقليمي ضيق، بل أصبح بإمكان الجماعات استهداف الأفراد في مختلف أنحاء العالم عبر منصات مفتوحة أو مغلقة، مما يخلق خلايا نائمة متفرقة جغرافياً لكنها موحدة فكرياً.[٢]

ويخلق هذا العبور القانوني والإقليمي إشكاليات معقدة على مستوى الملاحقة القضائية والتعاون الدولي، حيث يتطلب الأمر تنسيقاً بين جهات إنفاذ القانون في عدة دول للحصول على الأدلة الإلكترونية المخزنة على خوادم في دول أخرى، وسط تحديات قانونية وسياسية تتعلق بسيادة كل دولة على بياناتها. كما أن أثر الدعاية الإرهابية العابرة للحدود لا يقل خطراً، حيث يمكن لبث رسالة تهديد واحدة أن تصل إلى الملايين في لحظات وتسبب ذعراً عاماً يتخطى القارات.

وبالتالي، فإن البيئة الرقمية حوّلت الإرهاب من خطر محلي يمكن احتواؤه إلى تهديد عالمي متشابك، يجعل من أي دولة معرضة للخطر من أي نقطة في العالم، مما يستدعي تطوير أطر قانونية وقضائية دولية أكثر مرونة وفعالية لمواجهة طبيعة هذا الخطر الذي لا يعترف بالحدود. القانون العراقي: يواجه تحديات مرتبطة بالوضع الأمني، ويشدد على تجريم الأنشطة الرقمية التي تدعم التنظيمات الإرهابية، مع إيلاء اهتمام خاص لتمويل الإرهاب إلكترونيًا[٣]. القانون المصري: يركز على حماية أمن الدولة القومي، ويجرم أي استخدام رقمي لتسهيل الإرهاب، مع عقوبات صارمة تشمل المصادرة المالية والحبس لفترات طويلة .[٤] هذه الأركان الأربعة تُشكل إطارًا متكاملًا لفهم كيفية تحول الإرهاب إلى الفضاء الرقمي وكيفية مواجهته قانونيًا.

---

[١] عقيلة هادي عيسى ، وإسراء جواد حاتم، الإرهاب المعلوماتي الرقمي وطرق مكافحته، المجلة السياسية والدولية، الجامعة المستنصرية، العدد ١٦، بغداد، ٢٠١٠، ص٤٧٣.

[٢] علي حسين الخلف ، الشاوي، سلطان عبد القادر، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، ٢٠٠٦، ص٨١.

[٣] كاظم عبد جاسم، صعوبات مواجهة الجرائم المعلوماتية، جريدة الصباح العراقية، العدد الثامن، الجزء ١٣، بغداد، ٢٠١٩، ص٥١٢.

[٤] محمد عبدالله أبو بكر سلامة ،جرائم الكمبيوتر والأنترنيت ، ط١، منشأة المعارف ، الإسكندرية، مصر، ٢٠٠٦، ص١٢٦.

المطلب الثاني

آثار النشاط الإرهابي في البيئة الرقمية

يخلِّف النشاط الإرهابي في البيئة الرقمية آثاراً خطيرة وسوف نقوم بتناول هذه الآثار كل على حدى بشيء من التفصيل وذلك وفق التقسيم الآتي:

أولاً- الآثار الأمنية يُخلِّف النشاط الإرهابي في البيئة الرقمية آثاراً أمنية بالغة الخطورة، تمثل تحديًا مباشراً لاستقرار الدول وسلامة مواطنيها. فمن خلال استغلال الفضاء الإلكتروني، تنجح الجماعات الإرهابية في خلق بيئة من التهديد المستمر الذي يتجاوز القدرات الأمنية التقليدية.

تتمثل هذه الآثار في تقويض الأمن القومي عبر اختراق البنى التحتية الحيوية للدولة، مثل شبكات الطاقة والاتصالات والأنظمة المالية، مما يهدد بشل حركة الحياة اليومية وإحداث اضطراب اقتصادي واجتماعي واسع. كما يعمل النشاط الإرهابي الرقمي على تعزيز التطرف من خلال نشر الأفكار المتطرفة بسرعة هائلة وتجنيد الأفراد عبر منصات مغلقة، مما يوسع القاعدة البشرية لهذه الجماعات ويخلق خلايا نائمة يصعب كشفها.

ثانياً- الآثار الاجتماعية يُخلِّف النشاط الإرهابي في البيئة الرقمية آثاراً اجتماعية عميقة تمتد إلى نسيج المجتمع نفسه، حيث يعمل على تفكيك الروابط الإنسانية وتدمير الثقة بين الأفراد ومؤسسات الدولة. فتلك الأنشطة لا تستهدف فقط البنى التحتية المادية، بل تهاجم الكيان المعنوي للمجتمع وقيمه الأساسية[١].

يتجلى ذلك في نشر ثقافة الخوف والشك بين أفراد المجتمع، حيث يصبح الفضاء الرقمي – الذي من المفترض أن يكون مساحة للتواصل والمعرفة – مصدراً للتهديد والترهيب، مما يدفع الكثيرين إلى العزلة وتجنب المشاركة في الحياة العامة خوفاً من الاستهداف أو الاصطدام بالمحتوى المتطرف. كما يعمل على استغلال الفوارق الاجتماعية والطائفية عبر بث خطاب الكراهية والإقصاء، مما يزيد من حدة الانقسامات الداخلية ويُضعف الوحدة الوطنية[٢].

ثالثاً- الآثار الاقتصادية يُحدث النشاط الإرهابي في البيئة الرقمية آثاراً اقتصادية مدمرة تمتد إلى قطاعات اقتصادية حيوية وتُعطل مسار التنمية الوطنية. فبالإضافة إلى التكاليف المباشرة الناجمة عن الهجمات الإلكترونية، تظهر تداعيات غير مباشرة تطول استقرار الأسواق والثقة العالمية بالاقتصاد المحلي. من أبرز هذه الآثار الخسائر الفادحة الناتجة عن تعطيل البنية التحتية الرقمية للدولة والقطاع الخاص، حيث تستهدف الهجمات الأنظمة المصرفية والمالية مما يؤدي إلى اختلاس الأموال أو تعطيل الخدمات المالية وإرباك حركة الأسواق. كما أن عمليات الابتزاز الإلكتروني ضد الشركات والمؤسسات الكبرى تُلحق أضراراً مالية كبيرة وتدفعها إلى دفع فديات مالية لاستعادة بياناتها أو حماية أنظمتها[٣].

رابعاً- الآثار السياسية يُحدث النشاط الإرهابي في البيئة الرقمية آثاراً سياسية خطيرة تمسّ استقرار النظام السياسي وشرعيته، حيث يستهدف هذا النشاط مؤسسات الدولة وسيادتها وعلاقاتها الدولية. فمن خلال استغلال الفضاء الإلكتروني،

---

[١] إسراء طارق جواد كاظم الجابري، الإرهاب الإلكتروني، مطبعة العاني، بغداد، ٢٠١٧، ص٥٤.

[٢] سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجزائي، أطروحة دكتوراه، كلية القانون، جامعة الموصل، العراق، ٢٠٠٦، ص١٣٨.

[٣] حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالي، بغداد، ٢٠١٣، ص١١٧.

تنجح الجماعات الإرهابية في زعزعة الثقة بين المواطنين وحكومتهم، حيث تعمل على تشويه صورة الدولة ومؤسساتها عبر حملات التشكيك المنظمة التي تهدف إلى إضعاف الشرعية السياسية وتقويض هيبة الدولة[١].

كما يمتد تأثير هذا النشاط إلى العلاقات الدولية، حيث يصبح الفضاء الإلكتروني ساحة لاستهداف الدول الأخرى أو استخدامه كذريعة لاتهام الدولة بعدم القدرة على ضبط أنشطة الإرهاب المنطلقة من أراضيها، مما يخلق توترات دبلوماسية ويؤثر على التحالفات الإستراتيجية. وفي الوقت نفسه، تدفع هذه التهديدات الحكومة إلى تبني سياسات أمنية أكثر تشدداً، والتي قد تؤدي إلى تقييد الحريات العامة وفرض رقابة مكثفة على المحتوى الرقمي، مما يثير جدلاً حول التوازن بين متطلبات الأمن وضرورات الحفاظ على الحقوق الأساسية[٢].

خامساً– الآثار التكنولوجية يُحدث النشاط الإرهابي في البيئة الرقمية آثاراً تكنولوجية عميقة تُغيّر من طبيعة التعامل مع المنظومة التقنية وتُعيد تشكيل أولويات التطوير التكنولوجي على المستوى الوطني، فالهجمات الإرهابية الرقمية تدفع الدول والشركات إلى تبني استراتيجيات دفاعية أكثر تعقيداً تتضمن تطوير أنظمة أمن سيبراني متقدمة قادرة على مواجهة التهديدات المتطورة، مما يؤدي إلى استنزاف موارد مالية وبشرية هائلة كان من الممكن توجيهها نحو مشاريع تنموية مبتكرة.[٣]

سادساً– الآثار النفسية يتجلى هذا التأثير في المعاناة النفسية للضحايا المباشرين للتهديدات الإلكترونية، حيث يعيشون في حالة ترقّب دائم وخوف من التعرض للاستهداف الشخصي أو الإساءة الرقمية، مما قد يؤدي إلى اضطرابات نفسية مثل القلق المزمن والاكتئاب واضطراب ما بعد الصدمة، كما يمتد هذا الأثر إلى المجتمع ككل، حيث يخلق مناخاً من الشك والريبة بين الأفراد، مما يقوّض الثقة في التواصل الرقمي ويحدّ من حرية التعبير والمشاركة في الفضاءات الإلكترونية خوفاً من الاحتكاك بالمحتوى المتطرف أو الوقوع ضحية للاستهداف[٤].

وبالتالي، فإن هذه الآثار النفسية لا تقتصر على الجانب الفردي، بل تتحول إلى ظاهرة جماعية تُضعف المرونة النفسية للمجتمع وتزيد من حالة الانكفاء الاجتماعي، مما يتطلب تدخّلات نفسية واجتماعية متخصصة لمواجهة هذا النوع من الحرب النفسية الرقمية التي تستهدف العقل الجمعي قبل استهداف المنشآت المادية.

الخاتمة

يُمثّل النشاط الإرهابي في البيئة الرقمية تحديًا معاصرًا خطيرًا يهدد أمن الدول واستقرارها، متخطيًا بخصائصه الفريدة كل الحدود الجغرافية والتقليدية، وقد جاء هذا البحث ليعالج هذه الإشكالية من خلال دراسة مقارنة بين القانونين العراقي والمصري، وسعى إلى بيان مفهوم هذا النوع المستجد من الإرهاب وعناصره، وتحليل أركانه وآثاره المدمرة على الأمن القومي والمجتمعي، وقد توصلنا لمجموعة من النتائج والمقترحات:

---

[١] رشيد صبحي جاسم محمد، الإرهاب والقانون الدولي، رسالة ماجستير، كلية القانون، جامعة بغداد، ٢٠٠٣، ص٧٦.

[٢] عصام عبد الفتاح عبد السميع مطر، الجريمة الإرهابية، دار الجامعة الجديدة، الإسكندرية، مصر، ٢٠٠٥، ص٣١٢.

[٣] عبد الفتاح بيومي حجازي، الدليل الجزائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر، ٢٠٠٩، ص١٣٧.

[٤] حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالي، بغداد، ٢٠١٣، ص١٧٣.

النتائج

١. أكدت الدراسة أن مفهوم الإرهاب الرقمي في القانونين العراقي والمصري قد تجاوز الفعل المادي ليشمل أفعالاً غير ملموسة تنفذ في الفضاء الإلكتروني، مثل اختراق الأنظمة الحيوية، وتعطيل المواقع الإلكترونية للدولة، والتمويل الإلكتروني للجماعات الإرهابية.

٢. نستنتج أنه على الرغم من اختلاف النصوص، فإن كلا القانونين يشترطان لقيام جريمة الإرهاب الرقمي ركنين أساسيين: ركناً مادياً يتمثل في أي فعل أو شروع في فعل باستخدام الوسائل التقنية (كالاختراق، أو التعطيل، أو النشر)، و ركناً معنوياً يستلزم القصد الجنائي والغاية الإرهابية من الفعل (كترويع السكان أو المساس بأمن الدولة).

٣. أدت الطبيعة العابرة للحدود، والسرعة، والتخفي، واللاتماس التي تتمتع بها البيئة الرقمية إلى تضخيم آثار النشاط الإرهابي، مما جعل آثاره الاقتصادية (تخريب البنية التحتية المالية والرقمية) والاجتماعية (تفكيك النسيج المجتمعي عبر نشر الكراهية) والأمنية أكثر خطورة وأصعب في المكافحة.

المقترحات

١. نقترح بتطوير التشريعات وضرورة مراجعة وتحديث القوانين الوطنية بشكل دوري لمواكبة المستجدات التقنية وأساليب المجموعات الإرهابية المتطورة.

٢. نقترح بناء وتدريب فرق متخصصة في الشرطة والقضاء على التحقيق في الجرائم الإلكترونية وتتبع الأدلة الرقمية وتحليلها.

٣. نقترح بنشر الوعي المجتمعي بمخاطر الإرهاب الرقمي وطرق الوقاية منه، خاصة بين الشباب، لتحصينهم ضد عمليات التجنيد الإلكتروني ونظريات التطرف.

قائمة المصادر والمراجع

أولاً- الكتب:

١. أسامة أحمد المناعسة و جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط٢، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٤.

٢. إسراء طارق جواد كاظم الجابري، الإرهاب الإلكتروني، مطبعة العاني، بغداد، ٢٠١٧،

٣. أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ٢٠٠٧.

٤. بوادي حسنين، المنظومة الأمنية في مواجهة الإرهابية، دار الفكر العربي، الإسكندرية، مصر، ٢٠٠٧.

٥. جمال إبراهيم الحيدري، الوافي في القسم العام، قانون العقوبات، الطبعة الأولى، مكتبة السنهوري، بغداد، ٢٠١٢

٦. حامد البياتي، الإرهاب في العراق وخطورة انتقاله إلى المنطقة والعالم، ط١، مؤسسة شهيد المحراب للتبليغ الإسلامي، بغداد، ٢٠٠٥.

٧. صالح العادلي، موسوعة القانون الجزائي للإرهاب، دار الفكر العربي، القاهرة، ٢٠٠٣.

٨. طارق سرور، الجماعة الإجرامية المنظمة، دار النهضة العربية، القاهرة، ٢٠٠٠.

٩. عادل يحيى، السياسة الجزائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠١٤.

١٠. عبد الفتاح بيومي حجازي، الدليل الجزائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر، ٢٠٠٩.

١١. عصام عبد الفتاح عبد السميع مطر، الجريمة الإرهابية، دار الجامعة الجديدة، الإسكندرية، مصر، ٢٠٠٥.

١٢. علي حسين الخلف ، الشاوي، سلطان عبد القادر، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، ٢٠٠٦،
١٣. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت الأحكام الموضوعية والجوانب الإجرائية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٤.
١٤. محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة ،٢٠٠٣.
١٥. محمد عبدالله أبو بكر سلامة ،جرائم الكمبيوتر والأنترنيت ، ط١، منشأة المعارف ، الإسكندرية، مصر، ٢٠٠٦.
١٦. مصطفى محمد موسى، الإرهاب الإلكتروني، ط١، مطابع الشرطة، القاهرة، ٢٠٠٩.

ثانياً– الرسائل الجامعية:

١. أحمد كيلان عبد الله، حجية المحررات المستخرجة من الحاسوب في الإثبات الجنائي : أطروحة دكتوراه ، جامعة بغداد ، كلية القانون، العراق، ٢٠٠٧،
٢. رشيد صبحي جاسم محمد، الإرهاب والقانون الدولي، رسالة ماجستير، كلية القانون، جامعة بغداد، ٢٠٠٣.
٣. سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجزائي، أطروحة دكتوراه، كلية القانون، جامعة الموصل، العراق، ٢٠٠٦.

ثالثاً– المجلات والبحوث العلمية:

١. حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالي، بغداد، ٢٠١٣.
٢. حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالي، بغداد، ٢٠١٣.
٣. عقيلة هادي عيسى، وإسراء جواد حاتم، الإرهاب المعلوماتي الرقمي وطرق مكافحته، المجلة السياسية والدولية، الجامعة المستنصرية، العدد ١٦، بغداد، ٢٠١٠،
٤. علي هادي حميدي الشكراوي، الأحزاب السياسية و حماية القواعد الدستورية، دراسة مقارنة ، مجلة بابل للعلوم الإنسانية تصدرها كلية التربية جامعة بابل ، العدد الحادي عشر ، ٢٠٠٧.
٥. كاظم عبد جاسم، صعوبات مواجهة الجرائم المعلوماتية، جريدة الصباح العراقية، العدد الثامن، الجزء ١٣، بغداد، ٢٠١٩.
٦. كريم مزعل شلبي ، مفهوم الإرهاب دراسة في القانون الدولي والداخلي، مجلة أهل البيت، جامعة الكربلاء، العدد ٤، بغداد، ٢٠١٦،
٧. مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، بحث منشور العراق، في مجلة العلوم القانونية والسياسية، جامعة ديالى العدد الأول، المجلد الثالث، بغداد، ٢٠١٤،
٨. نضال ياسين الحاج حمو، دراسة السلوك في التشريع العراقي، بحث منشور في مجلة القضاء، العدد (١-٤)، السنة (٥٣)، بغداد، ١٩٩٩،
٩. هاشم حسن التميمي، دور الاعلام في مكافحة الإرهاب» مجلة العلوم السياسية العراق جامعة بغداد العدد ٤، ٢٠١٥

رابعاً– القوانين:

١. قانون الجرائم الإلكترونية العراقي رقم (٥) لسنــة ٢٠٢٣
٢. قانون مكافحة تقنية المعلومات (الجريمة الإلكترونية) رقم (١٧٥) لسنة ٢٠١٨.