مجلة القرار للبحوث العلمية المحكّمة | العدد 20، المجلد 7، السنة الثاني | آب (أغسطس) 2025 | صفر 1447
ISSN 3006-7294

استخدام البلوك تشين لتمويل المنظمات الإرهابية دراسة تحليلية في ضوء القوانين الإماراتية

إعداد: الباحث / عبد الله يوسف آل ناصر | دولة الإمارات العربية المتحدة

طالب دكتوراه في الحقوق والعلوم السياسية – القانون العام | الجامعة الإسلامية في لبنان

E-mail : a.alnasser@araalaw.com | https://orcid.org/0009-0007-3228-7391

https://doi.org/10.70758/elqarar/7.20.10

تاريخ الاستلام: 2025/7/8	تاريخ القبول: 2025/7/19	تاريخ النشر: 2025/8/15

للاقتباس: آل ناصر، عبد الله، استخدام البلوك تشين لتمويل المنظمات الإرهابية – دراسة تحليلية في ضوء القوانين الإماراتية، مجلة القرار للبحوث العلمية المحكّمة، المجلد السابع، العدد 20، السنة 2، 2025، ص-ص: 222-249. https://doi.org/10.70758/elqarar/7.20.10

المُلخص

يشهد العالم تطورًا متسارعًا في مجال التقنيات الرقمية، ولعلّ من أبرز هذه التقنيات هي «البلوك تشين»، التي فرضت نفسها كأداة فعالة في عدة قطاعات حيوية أبرزها المال والأعمال. غير أن هذه التقنية، بفضل خصائصها الفريدة كعدم المركزية، وإخفاء الهوية، والتشفير المعقّد، باتت أيضًا وسيلة محتملة لارتكاب الأفعال الإجرامية، وعلى رأسها تمويل الإرهاب وتنظيم العمليات الإرهابية العابرة للحدود. فقد استغلت التنظيمات الإرهابية هذه البيئة الرقمية لتجاوز النظم الرقابية التقليدية، وخلق شبكات مالية غير مرئية يصعب تتبّعها. ويهدف هذا البحث إلى دراسة العلاقة بين تقنية البلوك تشين والأعمال الإرهابية، من خلال تحليل مظاهر استغلالها لأغراض إجرامية، مع التركيز على مدى قدرة القانون الجنائي الإماراتي على التصدي لهذه الظاهرة المعقّدة. كما يسعى البحث إلى إبراز أوجه القصور التشريعي المحتملة، واقتراح حلول قانونية من شأنها تعزيز الفعالية الجنائية في مواجهة هذا التحدي.

اعتمدت الدراسة على مناهج متعددة، أبرزها المنهج التحليلي لفهم طبيعة البلوك تشين وإسقاطها على قواعد المسؤولية الجنائية، والمنهج المقارن لاستعراض تجارب بعض الدول في هذا المجال. وتوصّل البحث إلى أن هناك ضرورة مُلحّة لتطوير الإطار القانوني الإماراتي بما يراعي التطور

The Use of Blockchain Technology in Financing Terrorist Organizations An Analytical Study in Light of UAE Legislation

التكنولوجي المتسارع، مع الحفاظ على التوازن بين حماية الحقوق الرقمية ومكافحة الاستغلال الإجرامي لهذه التقنيات.

كلمات مفتاحية: بلوك تشين، عملات مشفرة، إرهاب رقمي، تمويل إرهاب، إطار تشريعي

Author: Researcher / Abdullah Yousef Al Nasser | United Arab Emirates
PhD Candidate in Law and Political Science – Public Law | Islamic University of Lebanon
E-mail : a.alnasser@araalaw.com | https://orcid.org/0009-0007-3228-7391

https://doi.org/10.70758/elqarar/7.20.10

Received : 8/7/2025	**Accepted :** 19/7/2025	**Published :** 15/8/2025

Cite this article as: Al Nasser , Abdullah , The Use of Blockchain Technology in Financing Terrorist Organizations-An Analytical Study in Light of UAE Legislation*, ElQarar Journal for Peer-Reviewed Scientific Research, vol 7, issue 20, 2025, pp. 222-249. https://doi.org/10.70758/elqarar/7.20.10*

Abstract

The world is witnessing rapid advancements in digital technologies, among which "Blockchain" stands out as a prominent tool that has established itself as an effective mechanism across several vital sectors, most notably finance and business. However, due to its unique characteristics such as decentralization, anonymity, and complex encryption this technology has also emerged as a potential means for committing criminal acts, foremost among them the financing of terrorism and the organization of transnational terrorist operations. Terrorist organizations have exploited this digital environment to bypass traditional regulatory systems and to establish invisible financial networks that are difficult to trace. This research aims to examine the relationship between blockchain technology and terrorist activities, through analyzing the manifestations of its exploitation for criminal purposes,

with a particular focus on the extent to which the UAE's criminal law is capable of addressing this complex phenomenon. The study also seeks to highlight potential legislative shortcomings and propose legal solutions aimed at enhancing the effectiveness of criminal law in confronting this challenge.

The study adopted multiple methodologies, most notably the analytical method to understand the nature of blockchain technology and its application within the framework of criminal liability, and the comparative method to review the experiences of other jurisdictions in this field. The research concludes that there is an urgent need to develop the UAE's legal framework in a manner that accommodates rapid technological advancements, while maintaining a balance between the protection of digital rights and combating the criminal exploitation of these technologies.

Keywords: Blockchain , Cryptocurrencies , Digital Terrorism , Terrorism Financing , Legislative Framework.

مقدمة

لم تنته الثورة التكنولوجيا عند حدود ما توصلت إليه في مطلع الألفية الثالثة، لا سيما بعد ظهور شبكة الإنترنت[1] وما خلفته من تغيير في نمط الحياة الإنسانية على كافة الأصعدة الاجتماعية والثقافية والمالية والتجارية. بل أبرزت لنا تلك الثورة تكنولوجيا جديدة التي ما لبثت أن بدأت تنتشر بين المتعاملين على نطاق واسع تُسمى تقنية البلوك تشين[2].

وإلى جانب الاستخدام الإعلامي والدعائي، فقد شكّلت التكنولوجيا وسيلة متقدمة للتنظيمات الإرهابية في مجال التمويل، وهو ما يُعد أحد أخطر التحديات أمام المجتمع الدولي. تاريخيًا، اعتمدت الجماعات الإرهابية على وسائل تقليدية في تمويل أنشطتها مثل التبرعات الفردية، الأنشطة التجارية غير المشروعة، والتحويلات المصرفية المشفّرة. غير أن التحول الرقمي العميق الذي شهده العالم، سمح بظهور وسائل أكثر تعقيدًا في هذا المجال، أبرزها العملات المشفّرة وتطبيقات البلوك تشين[3].

فقد مكنت تقنية البلوك تشين هذه التنظيمات من تنفيذ المعاملات المالية بشكلٍ لا مركزي، يصعب تتبعه من قبل الجهات الرقابية، بما يُعرف باسم «التمويل غير الملموس». ومن خلال استخدامها لمحافظ رقمية وهمية، يمكنها نقل الأموال وتوزيعها عبر شبكات غير خاضعة للسلطات التنظيمية، وهو ما يخلق بيئة مالية «مظلمة» تساعد على غسل الأموال وتمويل الأعمال غير المشروعة[4].

ولعلّ الأخطر في هذا السياق، أن تقنية البلوك تشين لا تُستخدم فقط كوسيلة تمويل، بل تُستغل أيضًا كأداة لتنفيذ العمليات نفسها، مثل: استخدام العقود الذكية (Smart Contracts) في التنسيق بين أعضاء التنظيمات دون الحاجة لتواصل مباشر، أو اعتماد الرموز غير القابلة للاستبدال (NFTs) في نقل رسائل مشفّرة. وهذه الاستخدامات تؤكد أن التحول الرقمي لم يكن مجرد تطوّر تقني، بل شكل تحولًا نوعيًا في البنية العملياتية للإرهاب العالمي[5].

(1) رأت التنظيمات الإرهابية في شبكة الإنترنت بيئة مواتية وفعالة لتوسيع أنشطتها، لا سيما في مجالات التجنيد، التحريض، والتنسيق، حيث استغلت الطبيعة المفتوحة والمجهولة للشبكة في الإفلات من الرقابة التقليدية، مما مكّنها من توسيع نطاق خطابها وتجنيد الأتباع في بيئات يصعب الوصول إليها بالوسائل الأمنية التقليدية. لقد أضحت الإنترنت، بتعدد منصاتها وشبكاتها الاجتماعية، وسيلة استراتيجية بيد تلك التنظيمات، سواء في نشر الأيديولوجيات المتطرفة أو في بث مواد دعائية عالية التأثير، بما يعزز ثقافة العنف والكراهية، ويوجه الأفراد نحو تنفيذ عمليات إرهابية انتحارية أو فردية دون ارتباط تنظيمي مباشر.

(2) *UNODC,* The Use of the Internet for Terrorist Purposes*,* United Nations Office on Drugs and Crime, 2012, pp. 17-22.

(3) FATF*,* Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, Financial Action Task Force, October 2020.

(4) Europol*,* Internet Organised Crime Threat Assessment (IOCTA), 2021, p. 36.

(5) Scott J. Shackelford*,* Blockchain and the Future of Cybersecurity, Cambridge University Press, 2020, pp. 159-166, O. Kharif, «Crypto Terrorism Funding Is Growing More Sophisticated», Bloomberg 17 january 2020.

ولا شك أن الثورة التكنولوجية التي تسارعت منذ مطلع الألفية الثالثة، وبخاصة بعد ظهور شبكة الإنترنت، قد أحدثت تحولًا عميقًا في طبيعة التفاعل الإنساني على مختلف الأصعدة الاجتماعية والثقافية والاقتصادية. غير أن هذه الثورة لم تتوقف عند هذا الحد، بل أفرزت تكنولوجيا أحدث وأكثر تعقيدًا، مثل البلوك تشين، والتي سرعان ما بدأت تجد طريقها إلى الاستخدامات غير المشروعة، ومنها الإرهاب الرقمي[1].

بلوك تشين أو «سلسلة الكتل» هي «قاعدة بيانات أو سجل يجمع قائمة بجميع التبادلات التي تمت بين مستخدميها منذ إنشائها». ويمكن مقارنتها في هذا الصدد بسجل يتم فيه تسجيل وإدراج جميع التبادلات التي حدثت بين عدة أفراد.

كما تُعرف البلوك تشين بأنها «تقنيات لتخزين ونقل المعلومات، تسمح بتكوين سجلات مكررة وموزعة، بدون هيئة مركزية للتحكم، ومؤمنة بفضل التشفير، ومُهيكلة بواسطة كتل مترابطة مع بعضها البعض على فترات زمنية منتظمة»[2]. فهي هيكل لا مركزي ينتشر في الفضاء الرقمي، حيث يمكّن المستخدمين من إدخال معلومات واستخدامها لأغراض مختلفة، مثل المعاملات، تخزين البيانات، إنشاء الرموز، وتنفيذ العقود الذكية[3]. ويعتمد عمل ونزاهة هذه السجلات بشكل خاص على استخدام وسائل التشفير، التي تُعرَّف بأنها مجموعة من العمليات التي تسمح بجعل المعلومات غير مفهومة في غياب مفتاح فك التشفير المناسب[4].

تعتبر تقنية البلوك تشين من أبرز الابتكارات التي أحدثت ثورة في عالم التكنولوجيا الرقمية، باعتمادها على نظام رقمي غير مركزي يقوم بتسجيل البيانات وحفظها بطرق مشفرة تضمن أمن وسرية المعلومات. مع تطور العالم الرقمي والاعتماد المتزايد على الحلول التكنولوجية في مختلف المجالات، أصبحت البلوك تشين حلاً موثوقاً للعديد من التطبيقات العملية، ليس فقط في القطاع المالي، ولكن في العديد من المجالات الأخرى كالصحة، القانون، والأعمال التجارية[5].

في الواقع، يمكن القول بأن تقنية البلوكشين، على الرغم من كونها ثورية من الناحية النظرية، لا

(1) Mahmoud Abdalla, "Blockchain Technology and Security Challenges," Journal of Digital Forensics, Vol. 11, No. 2, 2022, pp. 88.

(2) مصطفى البنا، البلوك تشين وتحديات القانون الجزائي العربي." المجلة القانونية الخليجية، العدد 9، 2023، ص 33–56.

(3) د. أحمد عمّار، بلوك تشين – التقنية الثورية، عرض وتطبيقات. القاهرة: دار النهضة العربية، 2022، ص 10، ود. فهد العبدالله. تكنولوجيا البلوك تشين ومستقبل المعاملات المالية. جدة: دار الخليج للنشر، 2022، ص 70 وما يليها.

(4) د. فهد العبدالله، المرجع السابق، ص 102، مصطفى البنا، البلوك تشين وتحديات القانون الجزائي العربي." المجلة القانونية الخليجية، مرجع سابق، ص 33–56.

(5) د. سامي جمال، الأمن السيبراني وتقنية البلوك تشين. الرباط: دار المغرب العربي، 2021، ص56، د. أحمد عمّار، بلوك تشين – التقنية الثورية، المرجع السابق ص112.

تحدث تغييرًا على مستوى فهم الجريمة بالشكل الذي يبرر إعادة النظر فيها. قد يكون من الممكن تطبيق المعايير التقليدية للجريمة السيبرانية مع تعديلها بشكل طفيف بحيث تشمل هذه الأساليب الجديدة في ارتكاب الجرائم، أو يمكن اعتبارها تجسيدًا لشكل جديد من الجريمة. وعليه، تعتبر البلوكشين في الواقع سلاحًا للجرائم السيبرانية التي من حيث المبدأ يمكن لمجرمي الإنترنت إتقان استخداماتها المختلفة. حيث يمكن لهؤلاء استخدام البلوك تشين لارتكاب الجريمة مع اقتناعهم بإمكانية الإفلات من المساءلة[1].

إشكالية البحث

شهد العالم في السنوات الأخيرة تحولًا رقميًا متسارعًا، برزت من خلاله تقنية البلوك تشين كإحدى أبرز الابتكارات التكنولوجية التي تتمتع بخصائص فريدة، لا سيما على صعيد السرية، اللامركزية، وغياب الهوية الشخصية للمستخدمين. ورغم ما تقدّمه هذه التقنية من فرص هائلة في ميادين الاقتصاد والخدمات، إلا أنّها أصبحت أيضًا أداة مزدوجة الاستخدام، تسمح بارتكاب أفعال غير مشروعة دون إمكانية التتبع الفعّال.

فطبيعة المعاملات المجهولة والمشفّرة ضمن شبكة البلوك تشين تطرح تحديات جسيمة أمام السلطات الجنائية، خصوصًا في ما يتعلق بتعقيد مسارات تتبّع الأموال والروابط بين الفاعلين، وهو ما يؤثر سلبًا على فعالية التحقيقات الجنائية. وفي هذا الإطار، يثور التساؤل الجوهري التالي، والذي يشكّل جوهر الإشكالية التي يعالجها هذا البحث: إلى أي مدى يملك القانون الجنائي الإماراتي أدوات فعّالة لمكافحة الاستخدام غير المشروع لتقنية البلوك تشين، لا سيما في ما يتعلق بتمويل الأعمال الإرهابية وتنفيذها؟

أهمية البحث

تبرز أهمية هذا البحث في مقاربة تقنية البلوك تشين من منظور قانوني جزائي، وذلك من خلال تسليط الضوء على المخاطر الأمنية والجنائية المرتبطة بهذه التكنولوجيا، باعتبارها بيئة خصبة يمكن استغلالها من قبل الجماعات الإرهابية والفواعل الإجرامية العابرة للحدود. كما تسعى الدراسة إلى توضيح أوجه القصور التشريعي التي قد تحدّ من قدرة المنظومة القانونية على التصدي لهذا النوع المستحدث من الأفعال الجرمية، مع التركيز على ضرورة إدماج أدوات التكنولوجيا الجنائية الحديثة ضمن النظام القانوني، بما يضمن حماية المجتمع من التهديدات الرقمية المتنامية.

أهداف البحث

يهدف هذا البحث إلى تحقيق ما يلي:

(1) Zohar, Aviv. "Blockchain Technology and its Implications on Criminal Law Enforcement." Journal of Digital Law & Policy, Vol. 18, No. 3, 2022, pp. 120–141

1. تحليل الطبيعة القانونية لتقنية البلوك تشين، واستجلاء مدى توافقها مع المبادئ التقليدية للقانون الجنائي.

2. تحديد أبرز صور الجرائم التي يمكن ارتكابها من خلال البلوك تشين، مع التركيز على الجرائم الإرهابية وتمويلها.

3. استعراض وتحليل الإطار القانوني الإماراتي في هذا المجال، والكشف عن مدى قدرته على ضبط هذه الظاهرة وملاحقتها جنائيًا.

4. تقديم مقترحات تشريعية وتوصيات عملية من شأنها تعزيز فعالية النظام الجزائي الإماراتي في التصدي لاستخدامات البلوك تشين غير المشروعة، دون الإخلال بالضمانات القانونية المستقرة.

منهجية البحث

نظرًا لطبيعة الموضوع التقنية والقانونية المعقّدة، فقد اعتمد هذا البحث على مقاربة منهجية متعددة تتيح الإحاطة بأبعاده المختلفة، وفق الآتي:

- المنهج التحليلي–الاستنباطي: لتحليل النصوص القانونية الوطنية والدولية ذات الصلة، وفهم كيفية انطباقها على جرائم ترتكب باستخدام البلوك تشين، بالإضافة إلى تفسير الاجتهادات القضائية ذات الصلة.

- المنهج الاستقرائي: لرصد الوقائع والأمثلة العملية التي تكشف عن مدى استغلال هذه التقنية في العمليات الإرهابية، وبالتالي استخلاص نتائج علمية يمكن البناء عليها في المجال التشريعي.

خطة البحث:

المبحث الأول: كيفية تمويل الإرهاب بواسطة تطبيقات البلوك تشين .

المبحث الثاني: موقف القانون الإماراتي من عمليات تمويل الإرهاب بواسطة البلوك تشين .

المبحث الأول

كيفية تمويل الإرهاب بواسطة تطبيقات البلوك تشين

تُعد البلوك تشين تقنية ثورية تعمل على إحداث انقطاع في الأنظمة التقليدية، حيث إنها تجلب معها مجموعة من الآليات الجديدة وغير المعروفة سابقًا. ومع ذلك، فإن سرعة تطور التكنولوجيا لا تتوافق دائمًا مع سرعة تطوير القوانين والتشريعات، مما يخلق فجوة زمنية وتقنية بين المنظمات الإجرامية والسلطات الحكومية. تستغلَ الجريمة هذه الثغرات في أنظمة العقاب وتتقن استخدام الأشكال الجديدة لارتكاب الجرائم، وكجماعة، يمثل الإرهابيون شكلاً معينًا من الجريمة المنظمة. وبالتالي، لديهم القدرة على استخدام الأساليب المبتكرة للجريمة، خاصة في إطار تمويلهم.

وتكون استجابة السلطات الحكومية غالبًا بطيئة وغير مكتملة بسبب الطبيعة السرية والمعقدة لتمويل الإرهاب التي تجعل من الصعب التعرف على التهديدات بشكل كامل وفي الوقت المناسب. هذا التأخير في التحديد والتحليل يؤدي إلى استجابات غير متناسبة مع حجم التهديد، مما يمنح الإرهابيين ميزة في استخدام تقنيات مثل البلوك تشين لتمويل أنشطتهم دون اكتشافها بسهولة ومن أبرز التطبيقات الناتجة عن البلوك تشين والتي تستخدم في تمويل المنظمات الإرهابية هي:

العملات المشفرة (المطلب الأول) والحوالات المالية المستحدثة (المطلب الثاني) إضافة إلى الأصول غير القابلة للاستبدال (المطلب الثالث) والميتافيرس (المطلب الرابع) .

المطلب الأول

العملات المشفرة وسيلة للتمويل

باعتبارها قائمة على تقنية البلوك تشين تشكّل العملات المشفرة أداة جذب للمنظمات الإرهابية، حيث تعتبر الوسيلة الأكثر فعالية لتمويل نشاطاتها، حيث تسمح لهم هذه التقنية التحرّر من الموجبات التي يفرضها القانون والقيود الإلزامية التي تستوجبها المعاملات المصرفية.

تتميز العملات المشفّرة بخصائص تحول دون قدرة سلطات انفاذ القانون الكشف عن هوية المتعاملين بهذه العملات، وبالتالي صعوبة تعّقب التدفقات المالية. مما جعلها الطريقة المثلى والمفضلة لإنجاح عملياتهم المتعلقة بتبييض الأموال أو تمويل العمليات الإرهابية.

من خلال تجاوز الوسائط، يمكن أن تصبح المعاملات عبر العملات المشفرة شكلاً من أشكال التبرع شبه غير قابل للتتبع ويمكن أن تأتي من أي بلد. إن «الاسم المستعار» الذي توفره العملات

المشفرة للأطراف، رغم أنه ليس ضمانًا مطلقًا للإفلات من العقاب، يسمح للمعاملات بأن تمر دون أن تلتقطها رادارات السلطات الرقابية. إن لامركزية تقنية البلوك تشين تعقّد تحديد مصدر الأموال ووجهتها، مما يزيد من صعوبة عمل المحققين. سرعة المعاملات بالعملات المشفرة تعني تزايدها واندماجها في مجموعة من التدفقات المالية المعقدة التي يصعب تحليلها. وأخيرًا، فإن عدم قابلية هذه التحويلات للتغيير بفضل استخدام تقنية البلوك تشين يعد ضمانًا أمنيًا للجماعات الإرهابية حيث يمنع أي تراجع من قبل المرسل ويقلل بالتالي من الخسائر[1].

وتسهّل تقنية البلوك تشين تبادل ونقل الأصول المشفّرة، إذ إنّها تمنح المجرمين والمنظمات الإرهابية القدرة على إمكانية إخفاء هوية الأصول الناتجة عن أنشطة غير قانونية عن طريق خوارزميات خاصة تسهل تبييض الأموال وذلك من خلال خلط الأصول المشفّرة المستمدة من أنشطة إجرامية مع الأصول المشفّرة المشروعة العائدة لمستخدمين آخرين من أجل طمس مسار ومعالم العملات المشفّرة القذرة وتبييضها عن طريق إخفاء هويتها ومصدرها بعد عملية الخلط هذه تعمد خدمة خلط الأصول المشفّرة إلى توزيع العملات المشفّرة على مستخدميها "أصحابها" في محافظ جديدة بالشكل الذي تبدو فيه كما لو أنّها عُملات شرعيّة فيصبح من الصعوبة الوصول ومعرفة مصدرها غير المشروع، علماً أنّه يمكن للمجرمين إنشاء العديد من المحافظ واستخدامها لإخفاء معاملاتهم وأنشطتهم على البلوك تشين.

فعملية خلط الأصول المشفّرة هذه من شأنها أن تحول دون إمكانية تتبع المسار بين المشتري والبائع وتجعل من المستحيل تقريباً تحديد أصل الدفعة ووجهتها.

بالإضافة إلى ما تقدّم، هناك فئة من العملات المشفّرة ك Monero و Zcash يصعب تتبع مسارها لأنها تتمتع بخصائص تمكّن إخفاء هوية مالكها ومستخدمها بالكامل كما أنها تسمح بإخفاء قيمة التحويلات وهوية موقّع المعاملة أو إمكانية تعقبها.

هذا وقد تلجأ المنظمات الإرهابية بغية غسل الأموال إلى وسطاء العملات المشفّرة الذين لهم دور رئيسي في عمليات غسل الأموال ذلك أنّه بعد تلقيهم العملات المشفّرة القذرّة الناتجة عن نشاط إجرامي يعمدون إلى نقلها بإسمهم الشخصي إلى منصات لمبادلتها بعملات مشفرّة ليتم بعد ذلك تحويلها إلى عملةٍ حقيقية وسحبها.

ومن أبرز القضايا التي أثارت انتباه السلطات الدولية كانت تلك المتعلقة باستخدام كتائب القسام، الجناح العسكري لحركة حماس، للعملات الرقمية، لا سيما البيتكوين، كوسيلة لتجنّب الحصار المالي والتدقيق المصرفي. ففي عام 2019، قامت الحركة بنشر رابط خاص على منصاتها الرقمية يمكّن المتبرعين من إرسال الأموال باستخدام رموز QR تربط مباشرة بمحافظ إلكترونية مشفّرة،

(1) A. Brill, L. Keene, "Cryptocurrencies: the next generation of terrorist financing? ", Defence Against Terrorism Review Vol. 6, No. 1, Spring Fall 2014, pp. 7-30.

الأمر الذي دفع وزارة الخزانة الأميركية إلى فتح تحقيق واسع النطاق أسفر عن مصادرة أكثر من 150 حسابًا مشفّرًا وحوالى 2 مليون دولار، في واحدة من أكبر عمليات المصادرة الرقمية المتعلقة بتمويل الإرهاب حتى ذلك الوقت.[1]

وفي سياق مماثل، اعتمد تنظيم الدولة الإسلامية (داعش) على قنوات غير تقليدية لجمع الأموال وتمويل عملياته من خلال العملات المشفرة، مستخدمًا شبكات لامركزية ومنصات تبادل غير خاضعة للرقابة. وقد تم كشف إحدى هذه الشبكات في عام 2020، حيث أظهرت التحقيقات أنّ التنظيم لجأ إلى استخدام عملات مثل الإثيريوم واللايتكوين، فضلًا عن عملة البيتكوين، في حملات دعائية تدّعي العمل لأغراض إنسانية، مستهدفًا بها جمهورًا غربيًا عبر وسائل التواصل الاجتماعي. هذه الأموال نُقلت إلى محافظ افتراضية ثم تم توجيهها إلى عناصر داخل سوريا وتركيا، وقد استعملت عمليات تحويل متعددة وطبقات تشفير معقدة لتجنّب التتبع. في ضوء ذلك، تمكّنت وزارة العدل الأميركية من مصادرة الأموال وضبط البنية الرقمية للشبكة عبر عمليات تعقّب دقيقة للبلوك تشين . [2]

أما بالنسبة لتنظيم القاعدة، فقد أظهرت البيانات الجنائية لعام 2020 قيام التنظيم بإدارة شبكة رقمية لجمع التبرعات تتضمن محافظ إلكترونية وأدوات «خلط" (mixers) تعيق تتبّع المصدر الحقيقي للمعاملات. تم في هذا السياق ضبط أكثر من 300 حساب مشفّر، إضافة إلى الكشف عن استخدام عقود ذكية تمكّن من إعادة تدوير الأموال داخل النظام دون إثارة الشبهات. وقد اعتُبرت هذه القضية نقطة تحوّل في إدراك الأجهزة الأمنية لمستوى التعقيد الذي بلغه استخدام الجماعات المتطرفة للبلوك تشين، ليس فقط كوسيلة للدفع، بل كآلية تشغيلية متكاملة .[3]

(1) U.S. Department of Justice. (2020, August 13). Global disruption of three terrorist financing cyber-enabled campaigns. [Press release]. https://www.justice.gov/opa/pr/global-disruption-three-terrorist-financing-cyber-enabled-campaigns, Chainalysis. (2020, August). How terrorists are leveraging cryptocurrency. https://blog.chainalysis.com/reports/terrorism-cryptocurrency-hamas-al-qaeda-august-2020 MEMRI (Middle East Media Research Institute). (2019, January 31). Hamas launches Bitcoin fundraising campaign on its Telegram channel. https://www.memri.org/reports/hamas-launches-bitcoin-fundraising-campaign-its-telegram-channel

(2) Wall Street Journal. (2021, June 2). Hamas sees surge in Bitcoin donations amid Israel conflict. https://www.wsj.com/articles/hamas-bitcoin-donations-israel-conflict-11622565712 , Chainalysis. (2023). Crypto crime report 2023. https://www.chainalysis.com/reports/2023-crypto-crime-report/

(3) Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA). https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2021, Financial Action Task Force (FATF). (2022). Targeted , update on implementation of the FATF standards on virtual assets and virtual asset service providers. https://www.fatf gafi.org/en/publications/Fatfrecommendations/Targeted-Update-Implementation-Standards-Virtual-Assets.html

المطلب الثاني

نظام الحوالة الجديد

وعادة ما تعتمد الحوالات المالية الإلكترونية على وسيط أو طرف ثالث موثوق به –غير المرسل أو المرسل إليه – لإنجازها، فالعميل مثلًا يفوّض المصرف أو أي مؤسسة مالية أخرى بإجراء عمليات الدفع الإلكترونية وإتمامها حتى تصل إلى الشخص المستفيد. ولذلك فإن كل تلك العمليات تكون مسجّلة ومنظمة وفقًا للأصول وخاضعة للقيود التي تفرضها القوانين الصادرة عن الدول التي تجري عبرها تلك العمليات.

ومن هنا تظهر ميزة العملات المشفّرة والتي بموجب طبيعتها لا يحتاج التعامل بها إلى وجود وسيط، بل تتم مباشرة بين المرسل والمستفيد. فتتم المعاملة بينهما عبر اعتماد نظام دفع الكتروني يقوم على التشفير وباعتماد تقنية من الند للند Peer to peer (P2P) في إرسال المدفوعات عبر شبكة الانترنت[1].

فتصبح إمكانية إخفاء المصدر غير المشروع للأموال سهلة التحقق. وعليه فإن العملية تتم عبر تحويل الأموال إلى عملات مشفرة باستخدام تقنية البلوك تشين ويتم نقلها إلى المستفيد بعد ذلك، وبالتالي تتم العملية دون معرفة المرسل أو المستفيد.

لكن حتى ولو أن البلوك تشين تحتفظ بأثر جميع المعاملات بطريقة لامركزية وآمنة وشفافة وبالتالي يمكن التحقق من كل معاملةٍ مالية من شأنها التغطية على النشاط غير القانوني تسجيل كل معاملة في دفتر الأستاذ العام ومن الممكن دائماً إعادة استرجاع جميع العمليات السابقة، فإنه يمكن للجناة استخدام وسائل معينة من شأنها أن تتيح لهم التعامل بالعملات المشفرة بأسماء وهمية.

كما أن يمكن للمنظمات الإرهابية اللجوء إلى مشغلي منصات السوق السوداء Black market على الشبكة المظلمة Dark web التي تسمح بالولوج إلى مواقع لا يمكن الوصول إليها من خلال المتصفح العادي مثل Explorer أو Chrome أو Safari ... أو متصفح خاص مثل The Onion Router (Tor) أو Invisible Internet Project (I2P) الذي يعتمد نظام تشفير يحول دون كشف هويات الأشخاص في معاملاتهم إذ بإمكانهم ممارسة الأنشطة غير المشروعة مع بقاء هوياتهم مجهولة بالكامل. وخير مثال على الويب المظلم Dark Web موقع طريق الحرير Silk Road الذي كان يشكّل سوق سوداء كبيرة على الإنترنت تسمح بأعمال القرصنة وتجنيد القتلة المأجورين لقاء مبالغ تدفع حصرًا بالبتكوين.

لكي تستمر الحوالات، «تمكنت من إعادة تكييف النظام عبر التكيف مع عصر تكنولوجيا المعلومات والاتصالات الجديدة لتجاوز القيود المالية للنظام المصرفي والتكاليف التي قد تترتب

(1) O. Kharif, “Crypto Terrorism Funding Is Growing More Sophisticated”, Bloomberg 17 january 2020

على القواعد التي تحكم المؤسسات المالية الحديثة.» تُعد مسألة تأثير البلوك تشين على عمل الحوالات محورًا أساسيًا. بالفعل، يمكن تصور أن هذه التكنولوجيا قد تُستخدم لتحسين كفاءة وأمان الحوالات.

إذا كان النظام التقليدي يتضمن إرسال مبالغ نقدية أو عبر تحويل بنكي، فمن الممكن بالتالي تصور دفع بواسطة العملات المشفرة. ستكون هوية المرسل غير معروفة ليس فقط للمستفيد، ولكن أيضًا للوسيط.

هذا الغموض المزدوج يجعل من المستحيل تحديد هوية ممول العملية وكذلك المستلم. بالإضافة إلى ذلك، يمكن للبلوك تشين أن تحل أحد مخاطر الحوالة وهو خطر اختلاس الأموال من قبل الوسيط من خلال استبدالهم.

أوجه التشابه بين البلوك تشين والحوالة نظرًا لأنها تربط بين شخصين على الأقل بغض النظر عن موقعهما الجغرافي، يمكن تطبيق البلوك تشين بين الجماعات الإرهابية وأفرادها الأجانب على غرار نظام الحوالة. من خلال طبيعتها اللامركزية، تفي أيضًا بمتطلبات التغلب على غياب المؤسسات المصرفية. كما أن السرية تعد محورًا أساسيًا في كلا النظامين، حتى وإن لم تكن مبنية على عملية مماثلة: وجود طرف ثالث في الحوالة واستخدام عنوان مجهول في البلوك تشين. يمكن اعتبار مصادقة المعاملة من قبل أعضاء البلوك تشين بمثابة تسليم نهائي للأموال من قبل الوسيط بعد التحقق من هوية المستفيد الحقيقية، وأخيرًا، يلتقي هذان النظامان في إمكانية تحقيق أهداف مشروعة أو غير مشروعة.

مع ذلك، فإن خصائص البلوك تشين تسمح بتجاوز الفهم التقليدي للحوالة، من خلال الاستغناء عن أي وسيط، تتيح البلوك تشين الوصول بالثقة إلى أقصى درجاتها. المفهوم المعروف باسم «الكود هو القانون» والذي يستخدم أحيانًا للدلالة على قوة التقنيات الرقمية في تجاوز أساليب التنظيم التقليدية للمجتمعات، يجد هنا تأكيدًا. إنشاء وإدارة بلوك تشين خاصة من قبل الجماعات الإرهابية قد يفي بالمتطلبات التي كانت تفي بها الحوالة، مع تحسين أمان العمليات.

المطلب الثالث

تمويل الإرهاب عبر استخدام الرموز غير القابلة للاستبدال (NFT)

تم تصميم التمويلات الجماعية لدعم المشاريع المجتمعية الطموحة التي تفتقر إلى الدعم الحكومي. وقد تطورت في جميع القطاعات مثل البيئة، والعقارات، والمساعدات الإنسانية. يعتمد التمويل الجماعي على الأعمال الخيرية، حيث يتم تجميع مبالغ صغيرة من عدة مصادر وقد تأتي من عدة

دول. يشترك المانحون عادةً في نفس الهدف ويشاركون في دعمهم. ومع ذلك، يمكن أن يُستخدم هذا التمويل اللامركزي لأغراض غير قانونية، بل وإجرامية. أدى تطور وسائل التواصل الاجتماعي إلى زيادة انتشار هذه الدعوات المستهدفة للتبرع، وساهم رسوخ الدارك ويب في ممارسات بعض المستخدمين في ولادة تمويلات مخفية. وقد استغل الإرهاب هذا الوسيط بالنظر إلى المبالغ الصغيرة المتداولة أحيانًا، فإن «هدف السلطات العامة ليس محاولة منع هذا النوع من التمويل بقدر ما هو تحديده لرسم خريطة حقيقية للتدفقات المالية بين الأشخاص المتورطين في الجماعات السورية أو في أعمال إرهابية». هذه الخريطة قد تكون أكثر صعوبة في رسمها مع استخدام التمويلات عبر الرموز غير القابلة للاستبدال (NFT).[1]

تُنتَج الرموز غير القابلة للاستبدال (NFT) من خلال العقود الذكية التي تعتمد على تقنية البلوك تشين. يتم إنشاؤها من العدم، ويمكن أن تحتوي على معلومات متنوعة، بما في ذلك تمثيل صورة موجودة مثل عمل فني. تُعتبر العروض الأولية للعملات (ICOs) مثالاً على إمكانية تنفيذ دعوات للتبرع من خلال الـNFT. تُعرَّف هذه العملية بأنها «عملية جمع تمويل تتم من خلال نظام تسجيل إلكتروني مشترك، وهو بلوك تشين يؤدي إلى إصدار رموز تستخدم حسب الحالة للحصول على منتجات، خدمات، أو حقوق من الشركة المصدرة.» تُدفع هذه الرموز بالعملات المشفرة مثل البيتكوين أو الإيثيريوم، وتمر عبر البلوك تشين، مما يضمن سرية هوية المشتري والبائع.[2]

وإذا كان تمويل الإرهاب عبر الرموز غير القابلة للاستبدال (NFT) يمكن أن يحدث في العالم الحقيقي، فإنه يمكن أيضًا أن يتم بطريقة غير مادية من خلال الاستعانة بالعالم الافتراضي الذي يمثله الميتافيرس.

المطلب الرابع

التحويل غير المادي لتمويل الإرهاب في الميتافيرس

يتميز الميتافيرس بقدرته على إعادة خلق بيئة واقعية في عالم افتراضي. فهو يوفر جميع الخدمات المتاحة في العالم الخارجي، حيث يمكن للمستخدمين التجارة، والاستثمار في العقارات، والمشاركة

(1) Reuters. (2024, May 29). U.S. Treasury says regulators should consider NFT guidance, given fraud risks. Reuters. https://www.reuters.com reuters.com, Notiones. (2023, January 10). NFTs as emerging terrorism financing threat. https://www.notiones.eu notiones.eu+1coinweb.com+1 Gluck, R., & Bindner, L. (2023, July 10). Are jihadists profiting from NFTs? GNET. https://gnetresearch.org gnet-research.org, ACFCS. (2022). It Starts with Art – NFTs, money laundering and terrorist financing. https://www.acfcs.org i-aml.com+14acfcs.org+14notiones.eu+14

(2) U.S. Department of the Treasury. (2024, May 29). Nonfungible token illicit finance risk assessment [Press release]. https://home.treasury.gov/news/press-releases/jy2382 notiones.euen.wikipedia.org+2home.treasury.gov+2reddit.com+2

في الفعاليات الاجتماعية، أو حتى تنظيم تجمعات. إنه عالم موازٍ، دائم، ومتجاوز. وبالتالي، كما هو الحال في العالم الحقيقي، تعتبر المالية والاقتصاد السوقي من الأساسيات في الميتافيرس. وقد طوّر مؤيدو الميتافيرس هياكل مالية حقيقية تشبه المؤسسات المالية التقليدية، ولكنها تحتوي على ميزات جذابة للأفراد الصادقين كما للمسيئين.

المنظمات اللامركزية الذاتية Decentralized Autonomous Organizations (DAO) في الميتافيرس تشبه من حيث التمويل الجماعي في تلك المنظمات في العالم الحقيقي، حيث تُنشأ كيانات تمويلية دون أن تكون مؤسسات ائتمانية تقليدية. بدلاً من ذلك، تعمل كمجتمع من الأفراد (أو الرموز التجسيدية) الذي ينظم نفسه. تُشكل DAO من مجموعات من الأفراد المرتبطين بقواعد تشغيل مسجلة في البلوك تشين، تم تصميمها لتمويل المشاريع داخل البلوك تشين، ولكن يمكن أن تتجاوز استخدامها لهذا الإطار فقط. تعتبر DAO مثيرة للاهتمام بسبب طبيعتها اللامركزية والذاتية، بمجرد تسجيل قواعد التشغيل في كتلة، مثل شروط الحصول على NFT، تصبح غير قابلة للتغيير. يسمح هذا بشكل خاص بجذب الاستثمارات في الأصول الرقمية الموجودة في الميتافيرس ضمن هذه DAO، دون تدخل خارجي، وذلك بين مجتمع من الأفراد الذين يشتركون في نفس الأهداف. في هذا السياق، توفر مزيج DAO والميتافيرس دعماً محتملاً لتمويل الإرهاب، الأولى تسمح بالتمويل الجماعي بين أعضاء نفس المجموعة، بينما الثانية تشكل منصة لهذه الاستثمارات، سواء كانت NFTs، أو عقارات، أو عملات مشفرة.

يُعد الميتافيرس في حد ذاته منطقة مظلمة يمكن أن تُستَغل من قبل الجماعات الإرهابية لتنفيذ عملياتها، وكذلك لتمويل أنشطتها. إمكانية وصول المستخدمين إلى هذا العالم من أي مكان على الكرة الأرضية وظهورهم بملابس رمزية بسيطة، قد تُستغل من قبل الإرهابيين لتنظيم الاجتماعات والمعاملات دون إثارة أي شكوك. سيكون من المستحيل في الواقع معرفة من يملك أي رمز تجسيدي وأصل الأصول المشفرة، رغم أنه لا يمثل بحد ذاته وسيلة جديدة لتمويل الإرهاب، فإن الميتافيرس يُشكل دعماً مؤكداً لهذا التمويل، حيث يُموَّل ويُفَكَّر في الهجمات داخل الميتافيرس، لكنها تُنفَّذ في العالم الحقيقي وتستهدف ضحايا حقيقيين.

المبحث الثاني

موقف القانون الإماراتي من عمليات تمويل الإرهاب بواسطة البلوك تشين

تمويل الإرهاب هو أحد الركائز التي يجب التصدي لها لوقف خطره على البشرية. وبما أن البلوك تشين تعتبر شكلاً جديدًا من أشكال التمويل الذي يمكن القول إنه قد يتعزز مع تراجع مركزية التنظيمات الإرهابية، فإنها تخلق مخاطر تجد السلطات الحكومية الحالية صعوبة في استيعابها.

جعلت خطورة الجرائم الإرهابية معظم دول العالم تتضافر مع بعضها البعض لرسم إطار لمكافحة الإرهاب الدولي ومعالجة كافة الأسباب المؤدية إلي ذلك الإرهاب وتجريم أفعاله، وعقاب مرتكبيها من أجل التخفيف من آثارها الجسيمة والخطرة على البشرية، وتعزيز فرض السلام وتدعيمه بين الشعوب[1]. ويزداد الأمر تعقيدًا نظرًا لعدم وجود تعريف متفق عليه حول مفهوم الإرهاب. حيث يكتسب تعريف الإرهاب الدولي أهمية كبيرة فى إطار العلاقات الدولية، لأن تعريف الظاهرة وبيان الأفعال والتصرفات التي تعتبر من قبيل الإرهاب الدولي أو التي تخرج عن هذا المضمون يعد نقطة البداية نحو أى جهود دولية تساهم في مكافحة الظاهرة واقتلاع جذورها وقمع مرتكبيها.

توجد علاقة وثيقة الصلة ورابطة ما بين قدرة الجماعات الإرهابية على التدمير وبين قوتها وقدرتها المالية والاقتصادية، حيث تبيّن أن قوة الجماعات الإرهابية ترجع في الأساس الى قدرتها المالية والتى عن طريقها تستطيع الجماعات الإرهابية ممارسة الجرائم الإرهابية والعمل على تخطيط وتنظيم وتدريب وتنفيذ لعمليات الإرهابية، يستوي فى ذلك أن تكون الجماعات الإرهابية جماعات دولية أو جماعات محلية. وهذا يتطلب بالضرورة الاعتماد على الموارد المادية من خلال إمداد الجماعات والتنظيمات الإرهابية بالأموال والأدوات والمعدات لتنفيذ أعمالهم الإجرامية . وعليه سوف نرى الإجراءات التي اتخذها المشرّع الإماراتي فيما خص جرائم تمويل الإرهاب (المطلب الأول) على أن نبحث مدى تطابق الوسائل الجديدة الناتجة عن استخدام تقنية البلوك تشين مع أركان جريمة تمويل الإرهاب التي يتطلبها المشرّع (المطلب الثاني).

(1) د.أحمد محمد رفعت، القانون الدولي العام، مركز جامعة القاهرة للتعليم المفتوح، مطبعة جامعة القاهرة، طبعة 1999، ص 579.

المطلب الأول

الإجراءات التشريعية والتنظيمية المتخذة في الإمارات بشأن جريمة تمويل الإرهاب

لقد أولى المشرّع الإماراتي اهتمامًا بالغًا بجريمة تمويل الإرهاب، فكرّس لها أحكامًا واضحة وصارمة ضمن الفصل الرابع من القانون الاتحادي رقم (7) لسنة 2014 بشأن مكافحة الجرائم الإرهابية. وقد نصّت المادة 29 من هذا القانون على أن كل من قدم أو جمع أو أعد أو حصل أو سهّل الحصول على أموال بقصد استخدامها، أو بعلمه أنها ستُستخدم، كليًا أو جزئيًا، في ارتكاب جريمة إرهابية، يُعاقب بالسجن المؤبد أو بالسجن المؤقت الذي لا تقل مدته عن عشر سنوات. وامتد نطاق هذه المادة ليشمل كل من قدّم تمويلًا لتنظيم إرهابي أو لشخص إرهابي، أو تعامل مع أموال يعلم أنها متحصلة من جريمة إرهابية، سواء بالحيازة أو النقل أو الإيداع أو التصرف.

أما المادة 30، فقد شدّدت العقوبة على من كان عالمًا بأن الأموال متحصلة من جريمة إرهابية أو مملوكة لتنظيم أو شخص إرهابي، وقام بأفعال مثل تحويلها، أو إخفاء حقيقتها، أو تمويه مصدرها، أو التعامل بها بأي شكل من الأشكال، بقصد إخفاء حقيقتها أو غرضها غير المشروع. وقد تميز المشرّع الإماراتي في هذين النصين بتوسيع دائرة أفعال التمويل لتشمل ليس فقط التقديم أو الجمع، بل أيضًا الاكتساب، النقل، الاستثمار، والإيداع، مما يعكس حرصه على تجفيف كافة منابع تمويل الإرهاب.

وعلى الرغم من أن نصوص القانون رقم 7 لسنة 2014 لم تخضع لتعديلات مباشرة حتى الآن، إلا أن منظومة مكافحة تمويل الإرهاب في دولة الإمارات شهدت تطورات تشريعية مهمة، عزّزت من فاعلية هذه النصوص، ووسّعت من إطارها المؤسسي والتنفيذي.

ففي عام 2018، صدر مرسوم بقانون اتحادي رقم (20) لسنة 2018 بشأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب، والذي جاء ليشكّل الإطار التشريعي المكمّل والأساسي في هذا المجال، حيث وضع تعريفات دقيقة لمفهوم تمويل الإرهاب، وحدد الجهات المختصة، وألزم المؤسسات المالية وغير المالية بتطبيق إجراءات العناية الواجبة والإبلاغ عن المعاملات المشبوهة. وقد تم إحالة العديد من الأفعال المجرّمة في القانون رقم 7 لسنة 2014 إلى هذا القانون الجديد من حيث آلية الملاحقة والتنفيذ.

لاحقًا، وفي عام 2021، صدر مرسوم بقانون اتحادي رقم (26) لسنة 2021 لتعديل بعض أحكام المرسوم السابق، حيث تم تعزيز صلاحيات الجهات المختصة في مجال المصادرة والتجميد، وتوسيع نطاق المسؤولية الجنائية، بل واعتبار بعض التصرفات باطلة قانونيًا إذا هدفت إلى عرقلة

تنفيذ تدابير الحجز والمصادرة.

وفي عام 2024، توّجت هذه السلسلة التشريعية بإصدار مرسوم بقانون اتحادي رقم (7) لسنة 2024، الذي لم يعدّل نصوص قانون 2014 مباشرة، لكنه أسس لبنية مؤسسية جديدة، أبرزها إنشاء اللجنة الوطنية لمكافحة غسل الأموال وتمويل الإرهاب، ومجالس إشرافية تتولى تنسيق الجهود بين الجهات الرقابية والمالية والقضائية، في سبيل تحقيق الالتزام بالمعايير الدولية.

وإلى جانب هذه القوانين، أصدرت الدولة عددًا كبيرًا من القرارات الإدارية والتنظيمية والتعاميم الوزارية الداعمة، من أبرزها: قرار رئيس مجلس إدارة هيئة الأوراق المالية والسلع رقم 17 لسنة 2010، وقرار هيئة التأمين رقم 1 لسنة 2009، فضلًا عن تعاميم صادرة عن وزارتي العدل والاقتصاد والجمارك والبنك المركزي، جميعها تهدف إلى منع استخدام النظام المالي في تمويل الإرهاب[1].

من خلال هذا النسق التشريعي المتكامل، يتبيّن أن دولة الإمارات تعتمد مقاربة وقائية شاملة تقوم على رصد المخاطر ومواجهتها استباقيًا. ومع ذلك، فإن هذه المقاربة تواجه تحديات عند التعامل مع الوسائل الحديثة مثل تقنية البلوك تشين والعملات المشفّرة، التي تصعّب تعقب المعاملات ومصادر الأموال بسبب خاصية اللامركزية والمجهولية. فبالرغم من أن القانون لم يذكر البلوك تشين صراحة، إلا أن نطاق التجريم الواسع قد يسمح بإدراج هذه الوسائل ضمن الآليات المستخدمة في تمويل الإرهاب، خاصة مع تزايد لجوء التنظيمات الإرهابية إلى استخدام العملات الرقمية في عملياتهم. [2]

وعليه، يظهر أن المشرّع الإماراتي، من خلال تراكم تشريعي وتنظيمي مدروس، قد بنى منظومة قانونية صارمة لمكافحة تمويل الإرهاب، تراعي الإلتزامات الدولية لدولة الإمارات العربية المتحدة ، وتتكيف تدريجيًا مع التحديات التقنية المعاصرة، ولو أن الحاجة لا تزال قائمة لتعزيز الأدوات الرقابية التقنية على استخدام التكنولوجيا المالية الجديدة.

(1) وتجدر الإشارة إلى أن المشرّع الإماراتي لم يقتصر على حماية المصالح الداخلية فحسب، بل تبنّى مبدأ «العينية» في الاختصاص القضائي الجنائي، كما ورد في المادة 21 من قانون العقوبات الاتحادي، التي تخوّل الدولة ملاحقة مرتكبي جرائم الإرهاب الدولي حتى ولو ارتكبت خارج حدودها. وهذا ما يعززه نص المادة 43 من قانون مكافحة الإرهاب، التي تعتبر الجرائم المنصوص عليها فيه جرائم تمس الأمن الداخلي والخارجي للدولة.

(2) د .أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام ،النظرية العامة للجريمة و العقوبة، مركز التعليم المفتوح بكلية الحقوق جامعة بنها، ط 2009، ص 59،
د.حسني الجندي ، قانون العقوبات الاتحادي في دولة الامارات العربية المتحدة ، الكتاب الاول ،الطبعة الاولى ،دار النهضة العربية ، القاهرة ، سنة 2009–2008 ،ص 119،
النيابة العامة لدولة الإمارات العربية المتحدة. التقرير السنوي حول مكافحة الجرائم الإلكترونية والرقمية 2023. أبوظبي: إدارة مكافحة الجرائم التقنية، 2024.

المطلب الثاني

مدى توافق أركان جريمة تمويل الإرهاب مع تقنية البلوك تشين

تتكون جريمة تمويل الإرهاب من عنصرين: مادي **(أ)** ومعنوي **(ب)** وسوف نتكلم عن كل منهما بالتفصيل ونرى مدى توافق تلك الأركان مع تطبيقات تقنية البلوك تشين.

أ. **الركن المادي**

الجريمة لا تتحقق إلا بتوافر الركن المادي، حيث يعد هذا الركن عنصرًا أساسيًا لا يمكن تصور قيام الجريمة بدونه. القاعدة العامة تقتضي عدم معاقبة الشخص ما لم يتوفر هذا الركن، والذي يتألف من ثلاثة عناصر رئيسية: السلوك الإجرامي للفعل، النتيجة الإجرامية، وعلاقة السببية التي تربط بينهما. وعندما تتكامل هذه العناصر، يكتمل الركن المادي وتصبح الجريمة مكتملة. بالتالي، يُقصد بالركن المادي لجريمة التمويل البعد المادي للجريمة، أو الطريقة التي تظهر بها الجريمة للعالم الخارجي.

نصت المادة 32 من المرسوم بقانون اتحادي رقم 31 لسنة 2021 بإصدار قانون الجرائم والعقوبات على تعريف الركن المادي للجريمة بقولها: «يتكون الركن المادي للجريمة من نشاط إجرامي متمثل في ارتكاب فعل أو الامتناع عن فعل إذا كان هذا الارتكاب أو الامتناع مجرّما قانونًا.» وفيما يلي سيتم توضيح عناصر الركن المادي للجريمة بشكل متتابع.

السلوك الإجرامي الذي يهتم به القانون هو النشاط الإرادي للفاعل. ويعني هذا النشاط أي فعل ملموس يقوم به الفاعل، سواء كان ذلك من خلال فعل إيجابي أو امتناع عن تنفيذ واجب قانوني يقع تحت طائلة العقوبة. ويعتبر السلوك بهذا المفهوم شرطًا أساسيًا في كافة الجرائم، بما في ذلك جرائم تمويل العمليات الإرهابية على وجه الخصوص.

في معظم الجرائم، يمكن دائمًا ملاحظة العنصر المادي أو الطبيعي الذي تتم به الجريمة. فالمشرع، عند سن القوانين التي تجرم أفعالًا معينة، يأخذ في اعتباره الظواهر المادية التي تشكل تهديدًا أو ضررًا على مصالح الدولة التي يسعى إلى حمايتها.

وقد يتخذ السلوك الإجرامي لفعل التمويل شكل فعل إيجابي، وهو ما يعني أنه فعل مادي محسوس، يتمثل في الحركات أو الأفعال التي تصدر عن الفاعل بقصد تحقيق آثار مادية معينة[1].

(1) ومن بين الأفعال الإيجابية التي وردت في المادة 29 من قانون مكافحة الجرائم الإرهابية الإماراتي ما يلي:
1. تقديم أموال أو جمعها أو إعدادها أو الحصول عليها أو تسهيل حصول الغير عليها، بقصد استخدامها أو

ومن أمثلة الأفعال التي قد تندرج تحت نطاق تمويل العمليات الإرهابية ما يلي: القيام بأي شكل من أشكال جمع الأموال أو تقديمها بنية الاستخدام الفعلي الكلي أو الجزئي لتلك الأموال في تمويل العمليات الإرهابية. مما يعني أن الفعل الإجرامي يتحقق من خلال تقديم أو جمع الأموال وتوصيلها إلى الجماعات الإرهابية سواء بشكل مباشر أو غير مباشر.[1]

كما أن تحويل الأموال والنقل يتضمنان مضمونًا وهدفًا واحدًا يتمثل في نقل عائدات إحدى الجرائم المتعلقة بتمويل الأنشطة الإرهابية، بهدف إخفاء أو تمويه المصدر غير المشروع لهذه العائدات أو لمساعدة أي شخص متورط في ارتكاب مثل تلك الجرائم.

وبالإضافة إلى ذلك، يمكن أن يحدث السلوك الإجرامي من خلال التمويه أو الخلط، وذلك عبر إبرام صفقات مالية متتابعة لإخفاء مصدر المال غير المشروع بعد إيداعه في المؤسسات المالية. كما يمكن أن تتم عملية الإخفاء باستخدام وسائل متعددة مثل تكرار عمليات التحويل بين حسابات بنكية مختلفة، أو استخدام وسائل التحويل الإلكتروني للأموال، أو شراء الأوراق المالية، أو أدوات الاستثمار القابلة للتحويل بسهولة. ومن أبرز أساليب الخلط والتمويه هي عمليات التحويل الإلكتروني التي تتجنب النقل المادي للأموال، مما قد يقلل من إمكانية اكتشافها[2].

مع العلم بأنها ستُستخدم، كلها أو بعضها، في ارتكاب جريمة إرهابية.

2. تقديم أموال لتنظيم إرهابي أو لشخص إرهابي، أو جمعها أو إعدادها له، أو تسهيل حصوله عليها، مع العلم بغرض التنظيم أو الشخص الإرهابي.

3. اكتساب الأموال أو أخذها أو إدارتها أو استثمارها أو حيازتها أو نقلها أو إيداعها أو حفظها أو استخدامها أو التصرف فيها، أو القيام بأي عملية مصرفية أو مالية أو تجارية، مع العلم بأن تلك الأموال متحصلة من جريمة إرهابية أو مملوكة لتنظيم إرهابي، أو معدة لتمويل تنظيم إرهابي أو شخص إرهابي أو لارتكاب جريمة إرهابية تندرج ضمن الأفعال الإجرامية كل من يعلم بأن الأموال، كلياً أو جزئياً، متحصلة من جريمة إرهابية أو مملوكة لتنظيم إرهابي، أو غير مشروعة ومملوكة لشخص إرهابي، أو مخصصة لتمويل تنظيم إرهابي أو جريمة إرهابية، وذلك من خلال القيام بأحد الأفعال التالية:

1. تحويل أو نقل أو إيداع أو استبدال الأموال بغرض إخفائها أو تمويه حقيقتها أو مصدرها أو غرضها غير المشروع.

2. إخفاء أو تمويه حقيقة الأموال غير المشروعة، أو مصدرها، أو مكانها، أو طريقة التصرف فيها، أو حركتها، أو ملكيتها، أو الحقوق المتعلقة بها.

3. اكتساب الأموال أو حيازتها أو استخدامها أو إدارتها أو حفظها أو استثمارها أو استبدالها أو التعامل بها بغرض إخفاء أو تمويه حقيقتها أو مصدرها أو غرضها غير المشروع. ويلاحظ أن النشاط والفعل الإجرامي في جريمة تمويل الإرهاب يتجلى في تنفيذ العمليات المصرفية، حيث يصعب تحديد هذه العمليات بدقة، نظراً لتنوعها وتعقيدها وسرعة تطورها نتيجة التغيرات في الظروف والأوقات والمكان. فقد بدأت المصارف في شكلها البسيط ثم توسعت مثل معظم الأنشطة التجارية

(1) د. على حسين الخلف ، د. سلطان عبد القادر الشاوي ، المبادئ العامة ي قانون العقوبات، العاتك لصناعة الكتاب، القاهرة ، بدون سنة نشر ،ص 308

(2) تمييز دبي ، جلسة 29/3/2003 ، مجموعة الاحكام عام 2003 ،العدد 14 ج2 ،رقم 16 ، ص 84

ويثار التساؤل حول مدى توفر عنصر النتيجة الإجرامية في السلوك أو الفعل الإجرامي. وفي رأينا، تندرج جرائم تمويل الإرهاب ضمن فئة الجرائم الشكلية، حيث يتكون ركنها المادي من السلوك الإجرامي فقط، دون الحاجة لحدوث نتيجة ضارة. هذه الجرائم قد تحمل ضرراً معنوياً دون أن تترتب عليها نتائج مادية ملموسة. كما أن الفعل والنتيجة في هذه الجرائم يتداخلان بشكل يجعل ارتكاب الفعل يُعتبر فعلاً يؤدي إلى وقوع النتيجة في الوقت نفسه[1].

تعتبر جرائم التمويل من جرائم الخطر، حيث يكتفي المشرع لاحتمال تحقق نتيجة ضارة أو وجود تهديد واضح لسلامة المال الذي يحميه القانون الجنائي. بمعنى آخر، لا تنتج هذه الجرائم عادةً أي نتائج مادية ضارة، إذ أن أهداف عمليات تمويل الإرهاب قد تشمل الإخلال بالنظام العام أو تعريض سلامة المجتمع للخطر، مما قد يمكن الجماعات الإرهابية من تنفيذ أعمال تضر بالأفراد أو تثير الرعب بينهم، أو تهدد حياتهم وحرياتهم وأمنهم، أو تلحق الضرر بالبيئة أو الاتصالات أو المواصلات.

ومع ذلك، لا يشترط حدوث الإخلال بالنظام العام أو وقوع ضرر فعلي على المجتمع، بل يكفي أن تتوفر لدى الإرهابيين النية أو ما يعرف بالقصد الخاص نحو ذلك. وهذا يدل على أن الإرهاب يُعتبر جريمة من جرائم الخطر، حيث يكفي أن يحدث زعزعة للطمأنينة بين الناس أو بث الرعب في نفوسهم.

وبناءً على ما سبق، لا يمكن تصور الشروع في ارتكاب هذه الجريمة، لأنها إما أن تُرتكب بالكامل عند حدوث السلوك الإجرامي، أو لا تحدث على الإطلاق في حال عدم وقوع هذا السلوك. كما أنه لا مجال لبحث علاقة السببية في هذه الجرائم، إذ أن النقاش حولها يُثار فقط إذا أدى الفعل إلى نتيجة. علاقة السببية تشير إلى الصلة بين السلوك الإجرامي والنتيجة الضارة، بحيث يُثبت أن السلوك هو الذي أدى إلى حدوث تلك النتيجة. وأخيراً، لا يمكن تصور الخطأ غير العمدي أو غير المقصود في سياق الجرائم الشكلية.

وأخيرًا يمكن أن نستخلص أن الركن المادي للجريمة التي ينص عليها المشرّع الإماراتي لا يثير مشكلة في إمكانية تطبيقه على عمليات تمويل الإرهاب المرتكبة عبر البلوك تشين[2]. فتمويل الإرهاب يمكن أن يشمل أكثر الأشكال ابتكارًا لتمويل المشاريع الإرهابية، بما في ذلك تلك التي تستخدم الأصول المشفرة التي تعتبر بحسب الفقه القانوني منقولة غير ملموسة[3].

(1) د. يسر أنور على، شرح قانون العقوبات «النظريات العامة "، الكتاب الأول، القاهرة، سنة 1992 ص101.

(2) فايز رابح النفيعي، دور مؤسسة النقد العربي السعودي في مكافحة تمويل الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، طبعة 1432هـ-2011، ص202،
د فهد العبدالله، تكنولوجيا البلوك تشين ومستقبل المعاملات المالية، جدة: دار الخليج للنشر، 2022، 58

(3) ورشة عمل وزارة الخارجية الإماراتية والتعاون الدولي – المكتب التنفيذي للرقابة وحظر الانتشار (2023,نوفمبر 17 . ورشة عمل "مكافحة تمويل الإرهاب – التحقيقات والتقنيات الحديثة، وزارة الخارجية والتعاون الدولي –

ب. **الركن المعنوي**

يتطلب تحقيق الجريمة قانوناً وجود ركنين أساسيين هما الركن المادي والركن المعنوي. يمثل الركن المادي الأفعال التي تشكل الجريمة، بينما يتعلق الركن المعنوي بفكرة الخطأ لدى مرتكب الجريمة، والذي يُعرف على أنه العلاقة التي تربط بين ماديات الجريمة وشخصية الفاعل. هذا الركن يتضمن عنصرين أساسيين: العلم والإرادة، بالإضافة إلى القصد الجنائي العام والقصد الجنائي الخاص[1].

في حالة جريمة تمويل الإرهاب، يجب أن يتواجد عنصر العلم بأن جمع المال أو تقديمه يتم بغرض استخدامه في تمويل الإرهاب. وهذا يتطلب إثبات فعلي، وليس مجرد افتراض.[2]

ويؤكد النص على أهمية القصد الجنائي في تحديد المسؤولية الجنائية، وأن جريمة تمويل الإرهاب تتطلب الوعي الكامل بعناصر الجريمة والنية وراء الأفعال المرتكبة، مما يسلط الضوء على الأبعاد النفسية والقانونية المرتبطة بالجريمة.

يعتبر عنصر الإرادة هو العنصر الثاني من عناصر القصد الجنائي، حيث يتجلى في رغبة الفاعل في تنفيذ الفعل الذي يشكل الجريمة، بالإضافة إلى إرادته في تحقيق النتيجة التي تتضمن الاعتداء على الحق الذي يحميه القانون. كما تتعلق الإرادة بكل واقعة تحدد المعنى الإجرامي للفعل، مما يجعلها جزءًا من العناصر المادية للجريمة.

وتعرف الإرادة بأنها نشاط نفسي يهدف إلى تحقيق هدف معين. فإذا كانت نية الجاني هي تحقيق نتيجة إجرامية، فإن إرادته تتجه نحو السلوك الذي سيؤدي إلى تلك النتيجة. ويعتبر الهدف القريب هو الغرض الذي تسعى إليه الإرادة، بينما الغاية تمثل الهدف البعيد الذي يسعى الفاعل إلى تحقيقه لإشباع حاجة معينة، مما يجعل الغاية هي الهدف النهائي للإرادة. أما الباعث، فهو الدافع الذي يحث الفاعل على إشباع الحاجة، ويكون هذا الدافع ذو طبيعة نفسية، على عكس الغاية التي تتمتع بطبيعة موضوعية.

«الاستراتيجية الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسلح 20242027". (2024, سبتمبر 5

(1) يعتبر القصد الجنائي العام هو الصورة الأولى للركن المعنوي للجريمة، حيث تتجه إرادة الفاعل إلى القيام بفعل معين أو الامتناع عنه، وبالتالي إحداث النتيجة الإجرامية. تتجلى أهمية القصد الجنائي العام في كونه العامل الأساسي في فهم نفسية المجرم، حيث يتم التحقق من جوانب الخير والشر في شخصيته، بغض النظر عن جسامة الفعل المادي. يتمثل عنصر العلم في القصد الجنائي بالمعرفة بالوقائع المكونة للجريمة، وتوقع النتيجة، ومن ثم توجيه الإرادة نحو ارتكاب الفعل. في جريمة تمويل العمليات الإرهابية، يتطلب الأمر العلم بعناصر الواقعة المادية التي تتوافق مع النص التجريمي، وكذلك إدراك تعارض هذه الأفعال مع النظام القانوني. القانون يفترض العلم بالقانون حتى لو كان هناك بعض الالتباس أو الشك، ولا يمكن للمتهم الاحتجاج بجهله بالقانون.

(2) كامل السعيد، شرح الاحكام العامة في قانون العقوبات «دراسة مقارنة «، دار الثقافة للنشر والتوزيع، عمان، سنة 2011م، 1432هـ، ص105

فيما يتعلق بجريمة التمويل، يظهر عنصر الإرادة من خلال الرغبة في تحقيق الواقعة المادية المطابقة للسلوك الإجرامي. أما في حالة وجود إكراه، فإن النوع الذي يؤثر على الإرادة هو الإكراه المعنوي، حيث أن الإكراه المادي يؤدي إلى إلغاء الإرادة بالكامل، مما يعني أن سلوك الجاني لا يُعتبر عنصرًا من عناصر الركن المادي للجريمة. وبالتالي، فإن الأشخاص الذين يقومون بعمليات التمويل في سياق الأنشطة الإجرامية قد لا يتحملون المسؤولية الجنائية عن ارتكاب جريمة تمويل الإرهاب، إذا كان التهديد بالضرر هو ما اضطرهم لارتكاب السلوك الإجرامي.

القصد الجنائي الخاص يشير إلى اتجاه نية الفاعل لتحقيق هدف معين من خلال ارتكاب الجريمة. يُعتبر هذا النوع من القصد دافعًا محددًا يتواجد لدى الجاني، وعلى الرغم من أن الأصل هو عدم الاعتداد بالدافع وراء وقوع الجريمة، إلا أن بعض الجرائم تتطلب وجود هذا النوع من القصد لقيامها.[1]

فيما يتعلق بجريمة تمويل العمليات الإرهابية، يظهر القصد الجنائي الخاص بوضوح، حيث يتطلب الأمر أن يكون الفاعل على علم بأن الأموال التي يقدمها ستستخدم لتحقيق أهداف إرهابية، مثل إلحاق الأذى بالأشخاص أو تدمير الممتلكات. كما تنص الاتفاقية الدولية لقمع تمويل الإرهاب بوضوح على أن أي شخص يقوم بتقديم أو جمع أموال بنية استخدامها في الأنشطة الإرهابية يعد مخالفًا للقانون.

بعض الفقهاء يرون أن الركن المعنوي في جريمة تمويل الإرهاب يتمثل في القصد الإجرامي العام، مما يعني أن الجريمة لا يمكن أن تقع بالخطأ غير العمدي. كما أن المشرع لم يتطلب وجود دافع ثانوي أو نية خاصة للقيام بهذه الجريمة. وبالتالي، فإن الجريمة يمكن أن تتم بوجود أي هدف أو غاية، بخلاف جرائم الإرهاب التي تتطلب قصداً خاصاً[2].

يدعم هذا الرأي العديد من الفقهاء، حيث يشيرون إلى أنه ليس من الضروري استخدام الأموال فعلياً في تنفيذ العمل الإرهابي لكي تتحقق الجريمة، بل يكفي أن تكون الأموال قد تم جمعها أو تقديمها بنية استخدامها في تمويل العمليات الإرهابية. وتطالب الاتفاقية الدولية لقمع تمويل الإرهاب الدول الأعضاء بتجريم مجرد الشروع في ارتكاب جريمة تمويل الإرهاب، وكذلك التحريض والمساعدة، حتى لو لم يتم تنفيذ الفعل الأصلي. كما تطالب الاتفاقية بتجريم تنظيم حملات لجمع الأموال بغرض تمويل الإرهاب، حتى لو لم تنجح تلك الحملات في جمع الأموال.

وعليه، بالنسبة للعنصر المعنوي لتمويل الإرهاب فهو لا يثير الكثير من الإشكاليات. حيث يكفي

(1) غنام محمد غنام، شرح قانون العقوبات الاتحادي لدولة الامارات العربية المتحدة «القسم العام»، الطبعة الاولى، مطبوعات جامعة الامارات العربية المتحدة، سنة 2003 م، ص106

(2) فايز رابح النفيعي، دور مؤسسة النقد العربي السعودي في مكافحة تمويل الإرهاب، مرجع سابق، ص232

فقط أن يكون لدى الجاني «نية رؤية هذه الأموال أو القيم أو الممتلكات تُستخدم أو مع معرفة أنها مخصصة للاستخدام، كليًا أو جزئيًا، لارتكاب أي من أفعال الإرهاب.

لكي يُدان مرتكب فعل تقديم أو تجميع أو إدارة القيم المخصصة لتمويل الإرهاب، يجب أن يكون لديه نية أو على الأقل إدراك بوضوح أنه يقوم بفعل في إطار مشروع إرهابي. ومع ذلك، فإن مبدأ البلوك تشين نفسه هو عدم السماح بمعرفة هوية الأطراف في المعاملة، باستثناء بعض الاستثناءات. ومن الناحية الافتراضية، يمكن للفرد الذي قام بشراء NFT الذي قد يحمل شكل عمل فني عادي أو رمز مميز دون أن يكون لديه وعي أو نية واضحة بأنه يشارك في تمويل الإرهاب، أو غيرها من الرموز المميزة، بشكل تطبيقي بحت. إذا لم يكن الشخص على علم بأن هذا الرمز يُستخدم في الواقع لتمويل عملية إرهابية، فلا يمكن تحميله المسؤولية عن رغبة أو علمه بالمساهمة في ذلك. بالتالي، لن يكون من الممكن إثبات العنصر المعنوي ضده. في مواجهة هذه المعضلة في تحديد العنصر المعنوي، قد يكون من الممكن أن تقوم المحكمة بافتراض بالعلم بالأنشطة الإرهابية متى كان الشراء أو الاستثمار محاطًا بظروف تدل على أن الفاعل لم يكن يمكنه أن يجهل طبيعة عمله.

الخاتمة

لقد بيّن هذا البحث أن جريمة تمويل الإرهاب تمثّل أحد أبرز التحديات الأمنية والقانونية التي تواجهها الدول في العصر الحديث، نظراً للدور المحوري الذي يلعبه المال في تنفيذ العمليات الإرهابية وتوسّع التنظيمات المتطرفة. ومع تطور الوسائل التكنولوجية، خصوصاً اعتماد تقنية البلوك تشين والعملات الرقمية، باتت عمليات التمويل أكثر تعقيدًا، وأشد غموضًا، نتيجة الخصائص الفريدة لهذه التقنية مثل عدم المركزية، والمجهولية، وصعوبة التتبع.

في هذا الإطار، يظهر جلياً أن التشريعات التقليدية، رغم صرامتها، قد لا تكون كافية وحدها لردع أو منع هذا النمط من الجرائم، ما يستوجب تحركاً تشريعياً وتقنياً متقدماً يتلاءم مع طبيعة المخاطر الرقمية المعاصرة. وقد حاولت دولة الإمارات العربية المتحدة، من خلال القانون الاتحادي رقم 7 لسنة 2014 والمراسيم المكملة له، أن تواكب هذه التحديات، إلا أن التطور المتسارع لتقنيات البلوك تشين يفرض ضرورة مراجعة دائمة وشاملة لأطر المواجهة.

النتائج

1. توسّع نطاق تمويل الإرهاب ليشمل وسائل تقنية غير تقليدية مثل العملات المشفّرة والعقود الذكية، وهو ما يخلق فراغاً تشريعياً جزئيًا في بعض الجوانب.

2. تقنية البلوك تشين تُستخدم كأداة فعالة في إخفاء مصدر الأموال وهوية الأطراف، مما يعيق آليات التتبع والرقابة المالية التقليدية.

3. التشريعات الإماراتية، خاصة القانون رقم 7 لسنة 2014 والمراسيم المرتبطة به (مثل مرسوم 20/2018)، تُشكّل قاعدة متقدمة في مكافحة تمويل الإرهاب، لكنها لا تُشير صراحة إلى «البلوك تشين» أو «العملات المشفرة» في هذا السياق.

4. هناك قصور في الأنظمة التنفيذية والتقنية فيما يتعلق بمتابعة التدفقات المالية على شبكات البلوك تشين بشكل فعّال، ما يضعف فعالية التدابير الوقائية.

5. لا تزال الممارسات القضائية في المنطقة محدودة في التعامل مع قضايا تمويل الإرهاب عبر البلوك تشين، مما يخلق حاجة إلى تراكم اجتهادي وقضائي.

التوصيات

1. تعديل التشريعات الجنائية والتنظيمية لتشمل الإشارة الصريحة إلى الوسائل الرقمية والافتراضية المستخدمة في تمويل الإرهاب، بما في ذلك تقنيات البلوك تشين والعقود الذكية.

2. تعزيز قدرات الجهات الرقابية (مثل وحدة المعلومات المالية والهيئات المصرفية) على رصد وتتبع الأنشطة المشبوهة عبر شبكات البلوك تشين، من خلال التعاون مع منصات تحليل السلاسل (blockchain forensics) .

3. وضع ضوابط قانونية صارمة على منصات تداول العملات الرقمية المرخّصة في الدولة، وإلزامها بتطبيق معايير العناية الواجبة والإبلاغ الفوري عن المعاملات المشبوهة.

4. تطوير التعاون الدولي القضائي والتقني في مجال مكافحة تمويل الإرهاب عبر العملات المشفرة، وتبادل المعلومات مع الدول التي تملك تقنيات متقدمة في هذا الإطار.

5. إطلاق برامج تدريبية متخصصة للقضاة والنيابة العامة والجهات الأمنية حول الجرائم المرتبطة بتقنية البلوك تشين والتطبيقات التي تبنى عليها .

قائمة المراجع

أولًا: المراجع العربية

أ- مراجع عامة

1. د. أحمد محمد رفعت، القانون الدولي العام، مركز جامعة القاهرة للتعليم المفتوح، مطبعة جامعة القاهرة، 1999.

2. د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، مركز التعليم المفتوح، كلية الحقوق – جامعة بنها، 2009.

3. د. حسني الجندي، قانون العقوبات الاتحادي في دولة الإمارات العربية المتحدة – الكتاب الأول، دار النهضة العربية، القاهرة، 2009–2008.

4. د. على حسين الخلف، د. سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، العاتك لصناعة الكتاب، القاهرة، بدون سنة نشر.

5. د. يسر أنور علي، شرح قانون العقوبات – النظريات العامة، الكتاب الأول، القاهرة، 1992.

6. كامل السعيد، شرح الأحكام العامة في قانون العقوبات – دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2011.

7. غنام محمد غنام، شرح قانون العقوبات الاتحادي لدولة الإمارات – القسم العام، الطبعة الأولى، مطبوعات جامعة الإمارات، 2003.

ب- مراجع متخصصة

8. د. فهد العبدالله، تكنولوجيا البلوك تشين ومستقبل المعاملات المالية، جدة: دار الخليج للنشر، 2022.

9. د. أحمد عمار، بلوك تشين – التقنية الثورية، عرض وتطبيقات، القاهرة: دار النهضة العربية، 2022.

10. د. سامي جمال، الأمن السيبراني وتقنية البلوك تشين، الرباط: دار المغرب العربي، 2021.

11. د. سارة النجار، البلوكتشين وتطبيقاتها في العالم العربي، الرياض: دار الفكر السعودي، 2023.

12. د. هاني مصطفى، تحديات تنظيم البلوك تشين في الدول العربية، القاهرة: دار الشروق، 2023.

13. مصطفى البنا، «البلوك تشين وتحديات القانون الجزائي العربي"، المجلة القانونية الخليجية، العدد 9، 2023، ص 33–56.

ج- تقارير ومصادر رسمية

14. النيابة العامة لدولة الإمارات العربية المتحدة، التقرير السنوي حول مكافحة الجرائم الإلكترونية والرقمية، أبوظبي: إدارة مكافحة الجرائم التقنية، 2024.

15. وزارة الخارجية والتعاون الدولي – المكتب التنفيذي للرقابة وحظر الانتشار، ورشة عمل «مكافحة تمويل الإرهاب – التحقيقات والتقنيات الحديثة"، نوفمبر 2023.

16. وزارة الخارجية – الإمارات، الاستراتيجية الوطنية لمواجهة غسل الأموال وتمويل الإرهاب وتمويل انتشار التسلح 2024 – 2027، سبتمبر 2024.

17. فايز رابح النفيعي، دور مؤسسة النقد العربي السعودي في مكافحة تمويل الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص 202، 232.

18. تمييز دبي، جلسة 29/3/2003، مجموعة الأحكام، 2003، العدد 14، ج2، رقم 16، ص 84.

ثانيًا: المراجع الأجنبية

1. Scott J. Shackelford, Blockchain and the Future of Cybersecurity, Cambridge University Press, 2020, pp. 159–166.

2. Mahmoud Abdalla, "Blockchain Technology and Security Challenges," Journal of Digital Forensics, Vol. 11, No. 2, 2022, p. 88.

3. Zohar, Aviv. "Blockchain Technology and its Implications on Criminal Law Enforcement." Journal of Digital Law & Policy, Vol. 18, No. 3, 2022, pp. 120–141.

4. Brenner, Susan W. Cybercrime and the Law: Challenges, Issues, and Outcomes. Boston: Northeastern University Press, 2020.

5. A. Brill, L. Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?" Defence Against Terrorism Review, Vol. 6, No. 1, Spring–Fall 2014, pp. 7–30.

6. UNODC, The Use of the Internet for Terrorist Purposes, United Nations Office on Drugs and Crime, 2012, pp. 17–22.

7. FATF, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, October 2020.

8. Europol, Internet Organised Crime Threat Assessment (IOCTA), 2021, p. 36.

9. FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, 2022.

10. Chainalysis, Crypto Crime Report 2023, August 2023.

11. O. Kharif, "Crypto Terrorism Funding Is Growing More Sophisticated", Bloomberg, January 17, 2020.

12. Wall Street Journal, "Hamas Sees Surge in Bitcoin Donations Amid Israel Conflict", June 2, 2021.

13. U.S. Department of Justice, Global Disruption of Three Terrorist Financing Cyber-Enabled Campaigns, Press Release, August 13, 2020. https://www.justice.gov/opa/pr/global-disruption-three-terrorist-financing-cyber-enabled-campaigns

14. Chainalysis, How Terrorists Are Leveraging Cryptocurrency, August 2020. https://blog.chainalysis.com/reports

15. MEMRI, Hamas Launches Bitcoin Fundraising Campaign on its Telegram Channel, January 31, 2019. https://www.memri.org/reports

16. U.S. Department of the Treasury, Non-Fungible Token Illicit Finance Risk Assessment, May 29, 2024. https://home.treasury.gov/news/press-releases/jy2382

17. Reuters, U.S. Treasury Says Regulators Should Consider NFT Guidance, May 29, 2024. https://www.reuters.com

18. Notiones, NFTs as Emerging Terrorism Financing Threat, January 10, 2023. https://www.notiones.eu

19. Gluck, R., & Bindner, L., Are Jihadists Profiting from NFTs?, GNET, July 10, 2023. https://gnet-research.org

20. ACFCS, It Starts with Art – NFTs, Money Laundering and Terrorist Financing, 2022. https://www.acfcs.org