ElQarar Journal for Peer-Reviewed Scientific Research | Issue 21, Vol 7, Year 2 | September 2025 | Rabi al-Awwal 1447
ISSN 7294-3006

الجرائم المرتكبة ضد الأشخاص عبر الدارك ويب

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/7.21.19

تاريخ الاستلام: 2025/7/8	تاريخ القبول: 2025/7/22	تاريخ النشر: 2025/9/15

للاقتباس: آل ناصر، عبد الله، الجرائم المرتكبة ضد الأشخاص عبر الدارك ويب، مجلة القرار للبحوث العلمية المحكّمة، المجلد السابع، العدد 21، السنة 2، 2025، ص-ص: 425-443. https://doi.org/10.70758/elqarar/7.21.19

المُلخص

تتناول هذه الدراسة مدى قدرة القانون الجنائي الإماراتي على مواجهة الاعتداءات الواقعة على الأشخاص من خلال استخدام تقنية البلوك تشين، لا سيما في بيئات رقمية مغلقة مثل «الدارك ويب». وتُبرز الدراسة كيف أن الطبيعة اللامركزية والمشفّرة للبلوك تشين، إلى جانب التطبيقات الإجرامية في الشبكة المظلمة، قد مكّنت من ارتكاب أفعال جرمية جسيمة مثل الابتزاز الجنسي، استغلال الأطفال، والاتجار بالبشر، دون إمكانية التتبع أو المحاسبة الفعّالة. وقد كشفت الدراسة عن قصور تشريعي واضح في قانون العقوبات الإماراتي، سواء من حيث عدم وجود نصوص خاصة تواكب تطور الوسائل الجرمية الرقمية، أو من حيث صعوبة تطبيق قواعد المسؤولية الجنائية التقليدية على جرائم ترتكب بواسطة أدوات لامركزية مثل العقود الذكية أو العملات المشفّرة. ومن خلال تحليل مفاهيمي وقانوني وتقني، خلصت الدراسة إلى ضرورة إعادة بناء إطار قانوني متخصص يوازن بين حماية الابتكار وحماية الإنسان، مع التركيز على تعزيز أدوات التحقيق، وتوسيع الاختصاص القضائي، وتجريم أنماط الجريمة المستحدثة بشكل صريح.

الكلمات المفتاحية: الدارك ويب، الابتزاز الجنسي الرقمي، استغلال الأطفال، الاتجار بالبشر، الجرائم السيبرانية، المسؤولية الجنائية، الأدلة الرقمية، التشفير، اللامركزية، التعاون القضائي الدولي.

مجلة القرار للبحوث العلمية المحكّمة | العدد 21، المجلد 7، السنة الثانية | أيلول (سبتمبر) 2025 | ربيع الأول 1447
ISSN 3006-7294

Crimes Committed Against Persons via the Dark Web

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/7.21.19

Received : 8/7/2025	**Accepted :** 22/7/2025	**Published :** 15/9/2025

Cite this article as: Al Nasser , Abdullah , Crimes Committed Against Persons via the Dark Web*, ElQarar Journal for Peer-Reviewed Scientific Research, vol 7, issue 21, 2025, pp. 425-443. https://doi.org/10.70758/elqarar/7.21.19*

Abstract

This study examines the extent to which UAE criminal law is capable of addressing assaults against individuals committed through blockchain technology, particularly within closed digital environments such as the Dark Web. The research highlights how the decentralized and encrypted nature of blockchain, combined with its criminal applications in the dark web, has facilitated the commission of serious offenses—such as sexual extortion, child exploitation, and human trafficking—without effective traceability or accountability. The study reveals significant legislative shortcomings within the UAE Penal Code, both in terms of the absence of specific provisions addressing the evolving methods of digital crime, and the challenges of applying traditional criminal liability frameworks to offenses perpetrated using decentralized tools such as smart contracts or cryptocurrencies. Through conceptual, legal, and technical analysis, the study concludes that there is a pressing need to reconstruct a specialized legal framework that balances innovation protection with human protection, emphasizing the enhancement of investigative tools, the expansion of judicial jurisdiction, and the explicit criminalization of emerging forms of cybercrime.

Keywords: Dark Web, Digital Sexual Extortion, Human Trafficking, Digital Evidence, International Judicial Cooperation.

مقدمة

لم تعد الثورة الرقمية مجرّد مرحلة عابرة في تاريخ تطور البشرية، بل شكّلت منعطفًا جذريًا في أساليب التفاعل البشري، وأعادت صياغة مفاهيم العمل، والمعرفة، والسلطة، والتواصل، بشكل غير مسبوق. فقد أحدثت شبكة الإنترنت منذ ظهورها في تسعينيات القرن الماضي تحولًا واسع النطاق على الصعد الاجتماعية، والاقتصادية، والثقافية، والأمنية، مما مهّد الطريق أمام موجة من الابتكارات التقنية التي غيّرت بنية المجتمعات والدول.

وفي هذا السياق، برزت تقنية البلوك تشين بوصفها إحدى أكثر صور التطور الرقمي تعقيدًا وتأثيرًا، حيث تقوم على مبدأ تسجيل المعاملات والبيانات ضمن شبكة موزعة لا مركزية، تتمتع بدرجة عالية من الشفافية في الشكل، والسرية في المضمون. ويُنظر إلى البلوك تشين على أنها تكنولوجيا ثورية فتحت آفاقًا جديدة في مجالات متعددة مثل التمويل، وسلاسل الإمداد، والعقود القانونية، والصحة، وحتى الانتخابات، وذلك بفضل خصائصها الفنية الفريدة، وأبرزها التشفير، عدم قابلية التعديل، وإخفاء الهوية.

لكن في مقابل هذه الإيجابيات، أظهرت التجربة العملية أن البلوك تشين، كغيرها من الأدوات التقنية، يمكن أن تتحول إلى سلاح بيد المعتدين، خصوصًا عندما يتم استغلال بنيتها الموزعة والمجهولة لأغراض إجرامية تمسّ سلامة الإنسان وحقوقه الأساسية .فقد ظهرت خلال السنوات الأخيرة تقارير ومؤشرات مقلقة حول استخدام هذه التقنية في ارتكاب أفعال اعتداء على الأشخاص، سواء بشكل مباشر، كما في حالات نشر المواد الإباحية التي تستهدف الأطفال، أو الإتجار غير المشروع بالبشر والبيانات البيومترية، أو بشكل غير مباشر من خلال استغلال العقود الذكية لتسيير شبكات إجرامية محصّنة ضد الملاحقة.

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»[1]. فهي هيكل لا مركزي ينتشر في الفضاء الرقمي، حيث يمكّن المستخدمين إدخال معلومات واستخدامها لأغراض مختلفة، مثل المعاملات، تخزين البيانات، إنشاء الرموز، وتنفيذ العقود الذكية[2]. ويعتمد عمل ونزاهة هذه السجلات بشكل خاص على استخدام وسائل التشفير، التي تُعرَّف بأنها مجموعة من العمليات التي تسمح بجعل المعلومات مفهومة في

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

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

غياب مفتاح فك التشفير المناسب.

كما يمكن أن تكون البلوك تشين خاصة وتعتمد على نظام مركزي تديره جهة معينة ويمكنها التحكم في الوصول باستخدام هوية محددة، هذه الفئة تختلف عن الأولى بأنها لم تعد تقنية مفتوحة المصدر بل تقنية مغلقة المصدر. على سبيل المثال، يمكن استخدامها من قبل شركة خاصة للحفاظ على وتبادل البيانات الداخلية[1].

على الرغم من النجاحات الكبيرة التي حققتها الإمارات العربية المتحدة لا سيما إمارة دبي في تبني تقنية البلوك تشين، إلا أن هناك بعض التحديات التي واجهتها الإمارة خلال مسيرتها في هذا المجال تمثلت بأن تقنية البلوك تشين ما تزال حديثة نسبيًا، وهناك حاجة إلى تشريعات متكاملة تتناسب مع سرعة التطور التكنولوجي، سواء على المستوى المحلي أو العالمي، لا سيما أن هذه التقنية كغيرها من الوسائل التكنولوجية عرضة لتكون بيئة خصبة للأفعال غير المشروعة وارتكاب الجرائم[2].

فالجريمة باعتبارها فعل فردي أو جماعي تتطور وتتكيف بطبيعتها مع الابتكارات المجتمعية، حيث شكلّت التكنولوجيا بالنسبة للجريمة وسيلة لتعزيز ارتكابها وتطوير إفلات مرتكبيها من العقاب. في هذا الصدد، ظهر مصطلح الجريمة الإلكترونية لفهم ظاهرة تتزايد باستمرار.

فالجريمة الإلكترونية تُعرف بأنها «كل جريمة جنائية تُحاول أو تُرتكب باستخدام أو ضد نظام المعلومات والاتصالات، وخاصة الإنترنت. يعتمد هذا الشكل الخاص من الجريمة على سيطرة تكنولوجيا المعلومات على مختلف مجالات الحياة البشرية. تستغل الجريمة الإلكترونية الثغرات الموجودة في هذه التكنولوجيا أو تُحرفها عن غاياتها. يعكس مصطلح الجريمة الإلكترونية مدى هذه الأفعال التي تؤثّر على مليار شخص تقريبًا حول العالم لذا يحاول المشرعون حول العالم والسلطات القضائية تكييف القانون بشكل عام والقانون الجنائي بشكل خاص ليكونا قادرين على مواجهة ومعاقبة هذه الأفعال. الأول من خلال زيادة النصوص القانونية الخاصة، والثاني من خلال العمل على تفسير وتوصيف النصوص الموجودة لتتلاءم مع الواقع الجديد.

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

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

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

البلوكشين في الواقع سلاحًا للجرائم السيبرانية التي من حيث المبدأ يمكن لمجرمي الإنترنت إتقان استخداماتها المختلفة. حيث يمكن لهؤلاء استخدام البلوكشين لارتكاب الجريمة مع اقتناعهم بإمكانية الإفلات من المساءلة[1].

تُشكّل اللامركزية التي تتميز بها البلوك تشين تحديًا قانونيًا من الدرجة الأولى، إذ أنها تُعقّد من عمليات التتبع والتحقيق، وتحول دون إمكان تحديد هوية الفاعلين أو الجهات المسيطرة على الشبكات أو المنصات المشبوهة. وهذا بدوره يعمّق الفجوة بين الواقع التكنولوجي المتسارع، والبنية القانونية التقليدية التي صُمّمت في الأصل للتعامل مع جرائم واضحة المعالم، محصورة في المكان، وخاضعة لسلطة مركزية محددة.[2]

إن الاعتداء على الأشخاص، في شكله الجديد ضمن الفضاء الرقمي المدعوم بتقنية البلوك تشين،

(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

(2) كانت الجرائم المالية التي ترتكب عبر البلوك شين قد ظهر أوجّها عام 2023 عندما تمّ الاستيلاء على خوادم شركة هيدرا التي تعتبر أكبر سوق في الشبكة المظلمة في العالم وذلك من قبل الشرطة الألمانية، فلم تسهل هيدرا مبيعات المخدرات فقط، بل قدمت أيضاً خدمات غسل الأموال للمجرمين الإلكترونيين. وأيضًا، موقع غارانتيكس وهو موقع لتبادل عملات مشفرة عالي المخاطر ومقره في روسيا، حيث تمّ فرض عقوبات عليه في نفس الوقت الذي تمت فيه معاقبة هيدرا بسبب أنشطة غسل الأموال المشابهة. وهناك أيضًا تورنادو كاش وهي خدمة مزج لامركزية على شبكة إيثيريوم التي تم فرض عقوبات عليها في أغسطس 2022 (مرة أخرى في نوفمبر) لتسهيل غسل الأموال، بشكل رئيسي فيما يتعلق بالأموال المسروقة في اختراقات العملات المشفرة من قبل مجرمين إلكترونيين مرتبطين بكوريا الشمالية. تعد تورنادو كاش حالياً البروتوكول الوحيد في مجال التمويل اللامركزي DeFi الذي تم فرض عقوبات عليه من قبل OFAC – وفي عام 2023 تزايدت أحجام العملات الرقمية غير المشروعة تصل إلى أعلى مستوياتها على الإطلاق وسط زيادة في تصنيفات العقوبات والقرصنة وكان العام الماضي2022 واحدًا من أكثر الأعوام اضطرابًا في تاريخ العملات الرقمية، حيث انهارت عدة شركات كبيرة، بما في ذلك Celsius و Three Arrows Capital وFTX، وغيرها، وسط مزاعم بالاحتيال. من بين الدولة العربية التي قامت بالمبادرة الاولى لاستخدام هذه التقنية هي دولة الامارات العربية المتحدة، حيث أنشات مؤسسة دبي للمستقبل المجلس العالمي للتعاملات الرقمية في فبراير 2016 الذي يضم أكثر من 47 جهة متخصصة من شركات وحكومات لتكون المرجع وصاحبة الخبرة للجهات التي تستخدم مثل هذه التقنيات. أما فيما يتعلق بالقانون الفرنسي فقد شهد على اعترافين لهذه التقنية الاولى بمقتضى القانون الصادر بموجب الأمر رقم 520_2016 في ابريل 2016. والثاني في المرسوم التنفيذي الصادر بموجب الامر رقم 1674_2017 تاريخ 8 ديسمبر 2017. أنظر بهذا الخصوص، د. سارة النجار، البلوكتشين وتطبيقاتها في العالم العربي. الرياض، دار الفكر السعودي، 2023. د. هاني مصطفى، تحديات تنظيم البلوك تشين في الدول العربية. القاهرة: دار الشروق، 2023، ص55، مصطفى البنا، البلوك تشين وتحديات القانون الجزائي العربي." المجلة القانونية الخليجية، مرجع سابق، ص 33–56. النيابة العامة لدولة الإمارات العربية المتحدة. التقرير السنوي حول مكافحة الجرائم الإلكترونية والرقمية 2023. أبوظبي: إدارة مكافحة الجرائم التقنية، 2024.

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

لا يقتصر فقط على انتهاك الخصوصية أو المسّ بالسمعة، بل يمتد ليشمل تهديد الأمان الجسدي والنفسي، وتسهيل ارتكاب جرائم ضد الكرامة الإنسانية، الأمر الذي يفرض تحديات غير مسبوقة أمام القوانين الجنائية الوطنية، وفي مقدمتها القانون الإماراتي.

ومن هنا، تنبع الحاجة الملحّة لدراسة معمقة تستجلي مدى قابلية القانون الجنائي الإماراتي لمواجهة هذه الظواهر الجديدة، وتحليل مدى كفاءة النصوص الحالية في التصدّي لاستخدامات البلوك تشين التي تؤدي إلى انتهاكات تمس الأفراد في ذواتهم وحقوقهم الأساسية، مع اقتراح حلول قانونية وتشريعية تضمن التوازن بين تشجيع الابتكار التقني، وحماية الإنسان وكرامته في البيئة الرقمية.

إشكالية البحث

تبرز الإشكالية الجوهرية لهذا البحث من خلال السؤال التالي:

إلى أي مدى يمتلك القانون الجنائي الإماراتي أدوات فعالة لمكافحة الاعتداءات الواقعة على الأشخاص من خلال تقنية البلوك تشين، سواء من حيث الوقاية أو التجريم أو الملاحقة؟

وتنطلق هذه الإشكالية من ملاحظة مركزية مفادها أن تقنية البلوك تشين، بما تتيحه من أدوات خفيّة وغير قابلة للتلاعب، قد أصبحت أداة محتملة لانتهاك حقوق الأفراد، في غياب أو ضعف التشريعات التي تواكب هذا التحول التقني. كما تسعى هذه الدراسة إلى الوقوف على مكامن القصور القانونية في مواجهة هذه الظاهرة، ومحاولة تقديم إطار قانوني متوازن قادر على حماية الأفراد من هذه الاعتداءات، دون المساس بمبادئ العدالة والتقدم الرقمي.

أهمية البحث

تكتسب هذه الدراسة أهميتها من واقع تزايد التهديدات التي تمس الأفراد وسلامتهم في ظل التطور التقني السريع، لا سيما من خلال استغلال تقنية البلوك تشين في تنفيذ اعتداءات خطيرة على الأشخاص، سواء بصورة مباشرة كالإيذاء البدني والتشهير ونشر المحتوى المؤذي، أو بوسائل غير مباشرة كالمساس بالخصوصية والإتجار غير المشروع بالبيانات الشخصية، واستغلال العقود الذكية لتسيير أنشطة تنتهك الكرامة الإنسانية.

أهداف البحث

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف الأساسية، وهي:

1. تحليل الإطار المفاهيمي لتقنية البلوك تشين وخصائصها الفنية التي قد تسمح باستغلالها في الاعتداءات على الأشخاص.

2. تحديد أبرز صور الجرائم الماسة بالأشخاص التي يمكن أن تُرتكب باستخدام البلوك تشين، مثل الابتزاز الجنسي والإتجار بالبشر

3. اقتراح تعديلات أو إضافات تشريعية من شأنها تعزيز الحماية القانونية للأشخاص من الاعتداءات التي تتم من خلال استغلال تقنيات البلوك تشين، بما يحقق التوازن بين التحوّل الرقمي وحقوق الإنسان.

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 الاعتداءات على الأشخاص، وبالتالي استخلاص نتائج علمية يمكن البناء عليها في المجال التشريعي.

خطة البحث:

يلحظ قانون العقوبات الإماراتي جرائم عديدة ضد الأشخاص كجرائم الإبتزاز ودعارة الأطفال والإتجار بالبشر وغيرها. فهي ليست جديدة على عالم القانون بل موجودة منذ زمن طويل، لكن يمكن الأمر أن يثير الانتباه عندما تقع هذه الجرائم بأساليب جديدة وبطرق مختلفة عن ما يعرفه عالم القانون. لذلك سوف نحاول في هذه الدراسة التركيز على الجرائم المذكورة أعلاه التي باتت تقنية البلوك تشين «منصة» أو محطة لانطلاقها إلى العالم المادي عبر أهم تطبيقات البلوك تشين وهي الدارك نت « Dark Net »

المبحث الأول: الابتزاز الجنسي واستغلال الأطفال عبر الدارك ويب

المبحث الثاني: عمليات الإتجار بالبشر عبر الدارك ويب

المبحث الأول

الابتزاز الجنسي واستغلال الأطفال عبر الدارك ويب

التعرض للأطفال واستغلالهم جنسيًا أفعال دنيئة عُرفت منذ زمن طويل، حتى قبل انتشار تكنووجيا المعلومات. فهذه الأخيرة لم تكن إلا وسيلة متطورة لهؤلاء الجناة التي وفرت لهم وسائل جديدة للوصول إلى مبتغاهم.

جلب ظهور الإنترنت معه فرصًا جديدة لهؤلاء الأفراد. بعد نجاح «نابستر» Napster، وهو شبكة تبادل ملفات نظير إلى نظير Peer–to–Peer ، أتاحت للمستخدمين البحث في الأقراص الصلبة لأجهزة الكمبيوتر المجاورة وتحميل الملفات الموسيقية، ظهرت شبكات نظير إلى نظير أخرى أكثر تطورًا، والتي سهلت أيضًا مشاركة الصور ومقاطع الفيديو الرقمية. وشملت هذه الصور والمقاطع المواد الإباحية المتعلقة باستغلال الأطفال جنسيًا، ومع صعود وسائل التواصل الاجتماعي، ظهرت منتديات متخصصة على الإنترنت تركز على ما يُسمى «حب الأطفال» Child Love[1]، حيث سمحت للأفراد بالتواصل مع آخرين ذوي ميول جنسية مشابهة من مختلف أنحاء العالم.

مؤخرًا أصبح الجناة يستغلون وسيلة جديدة وهي ما تعرف بال» دارك ويب»، فهو جزء من الإنترنت غير المفهرس والذي يتطلب أدوات خاصة للوصول إليه، مثل متصفح تور. يُستخدم الدارك ويب في العديد من الأنشطة، بعضها قانوني وآخر غير قانوني. العلاقة بين البلوك تشين والدارك ويب تتجلى في الاستخدامات التي يتم بها توظيف هذه التقنية في البيئات المظلمة. على الرغم من أن البلوك تشين تم تصميمه لتعزيز الشفافية والأمان، إلا أنه يُستخدم أيضًا في تسهيل المعاملات غير المشروعة على الدارك ويب.

فالدارك ويب، ببساطة، هي شبكة متاحة على الإنترنت ولكنها تتطلب برامج خاصة وإعدادات محددة للجهاز المستخدم للوصول إليها. حاليًا، يستخدم حوالي 5.07 مليار شخص[2] شبكة الإنترنت يوميًا في حين تقدر نسبة مستخدمي الدارك ويب بحوالي 0.04% من إجمالي الاستخدامات اليومية للإنترنت، وهذا يعادل تقريبًا 2.5 مليون مستخدم يوميًا.

الدارك ويب أُنشئت في الأصل لتعزيز حرية التعبير، لا سيما في المناطق ذات الصراعات السياسية، فإن الواقع يشير إلى أن الكثير من هذه المواقع قد أصبحت سوقًا إجراميًا. ووفقًا لتقرير

(1) Goldman J, Ronken C (2000) The concept of childhood. https:// www.ccc.qld.gov.au/sites/default/files/2020-02/Project-AXIS- Volume-4-Selected-research-papers-Report-2000.pdf.

(2) Datareportal (2022) Digital around the world. https://datareportal. com/global-digitaloverview#:~:text=A%20total%20of%205.07%20billion,12%20months%20to%20October%202022.

صادر عن «اللجنة العالمية لإدارة الإنترنت»[1] Global Commission on Internet Gov– ernance فإن الدارك ويب تمثل «الجوانب السيئة للإنترنت». وقد وصفت طبيعتها المظلمة في بعض القصص حول تجارة المخدرات، والاغتيالات، والتنمر، واستغلال الأطفال.

تعمل شبكة الدارك ويب على إخفاء هوية مستخدميها من خلال إعادة توجيه حركة المرور عبر مجموعة عشوائية من الخوادم «سيرفير» المنتشرة حول العالم، هذا الإخفاء لهوية المستخدمين جعل الدارك ويب وسيلة جاذبة للعديد من الفئات، بما في ذلك الصحفيين، والمعارضين السياسيين، وكذلك الأفراد الذين يسعون لارتكاب الجرائم، فمنذ عام 2008، أصبح الوصول إلى هذا العالم أكثر سهولة بفضل متصفح «تور» (The Onion Router – TOR)، الذي أتاح لأعداد متزايدة من الجمهور استخدام هذه الشبكة.

تنتشر هذه الأنشطة في العالم المادي ولكن بشكل أكبر في العالم الافتراضي، حيث يتم تسهيلها مرة أخرى بفضل عدم الكشف عن الهوية والتواجد خارج الحدود القانونية للمشاركين، ويعتبر الـ«دارك ويب» صدى مقلقًا لهذه الظاهرة، حيث يستخدم مستهلكو الصور أو الفيديوهات ذات الطابع الإباحي للعملات المشفرة في الغالب،. هذه الجريمة ذات طبيعة افتراضية حيث أنها تجد في الـ«دارك ويب» وسيلة مثالية[2]. مع ذلك، فإن تصنيف هذه الجريمة لا يطرح صعوبة في التفسير عندما يتم على الـ«دارك ويب» عرض أو اقتناء صور أو فيديوهات ذات طابع بيدوفيلي من قبل فرد مقابل العملات الافتراضية، إنها طريقة محددة لتنفيذ الجريمة لا تغير من طبيعتها الأصلية. ولكن، على غرار تجارة المخدرات، قد يكون من الصعب جدًا تتبع آثار الجناة في هذه الجريمة المخفية. ومع ذلك، فإن أمثلة اكتشاف ومعاقبة مواقع بيع المواد الإباحية الخاصة بالأطفال من قبل السلطات تشير إلى أن التكيف مع القمع جارٍ، وأن الإفلات من العقاب لهذه الشبكات سيكون في النهاية أكثر نسبية.

توجد عشرات الآلاف من المواقع التي تلبي الاحتياجات الإجرامية لملايين المستخدمين يوميًا على شبكة الدارك ويب، من بين هذه المواقع، يوجد مئات مخصصة بشكل خاص لتبادل المواد الإباحية المتعلقة باستغلال الأطفال جنسيًا Child Sexual Abuse Material – CSAM[3] . وقد يواجه الممارسون العاملون في مجال الطب النفسي الجنائي وعلم النفس الجنائي الأفراد الذين ارتكبوا جرائم جنسية عبر هذه الشبكة، سواء جزئيًا أو كليًا.

بهدف وصف تنظيم هذه المواقع والأنشطة التي يقوم بها أعضاء هذه الشبكة لتُظهر هذه المواقع

(1) Owen G, Savage O (2015) The Tor Darknet. Global Commission on Internet Governance, London

(2) L.H Newman, "How a Bitcoin Trail Led to a Massive Dark Web Child-Porn Site Takedown", The Wired,

(3) Insoll T, Ovaska AK, Nurmi J, Aaltonen M, Vaaranen-Valkonen N (2022) Risk factors for child sexual abuse material users contact- ing children online: results of an anonymous multilingual survey on the dark web. J Online Trust Saf 1(2). *https://doi.org/10.54501/ jots.v1i2.29*

أن لديها عضوية كبيرة ومتعددة الجنسيات، حيث يتفاعل الأعضاء بشكل منظم عبر الإنترنت، وهذا التفاعل المستمر يساهم في إنشاء مجتمعات إلكترونية كبيرة يتبادل فيها الأفراد ذوو الاهتمامات المماثلة المواد الإباحية المتعلقة بالأطفال مع الحد الأدنى من مخاطر الكشف عن هويتهم.

في مايو 2021، ألقت الشرطة القبض على خمسة رجال ألمان، تتراوح أعمارهم بين 40 و64 عامًا، يُشتبه في أنهم كانوا يديرون موقع «بويزتاون» Boystown، وهو أحد أكبر المواقع المتعلقة باستغلال الأطفال جنسيًا على الدارك ويب. وفقًا للشرطة، كان الموقع نشطًا لمدة عامين، وعند إيقافه كان يحتوي على أكثر من 400,000 عضو مسجل. اتُّهم ثلاثة من الرجال المؤسسين بإدارة الموقع، في حين أن أحدهم وُصف بأنه كان من أكثر الأعضاء نشاطًا بمساهمته بأكثر من 3500 مشاركة[1].

أظهرت دراسة أجريت في عام 2015 أن هناك حوالي 900 موقع مشابه لـ «بويزتاون» كانت نشطة على الدارك ويب آنذاك، وكانت تتلقى مجتمعة حوالي 168,152 طلبًا يوميًا[2].

يمكن لـ «تور» أيضًا الوصول إلى مواقع الدارك ويب، هذه المواقع المظلمة هي منتديات ومواقع أخرى لا تُفهرس بواسطة محركات البحث العامة وتُعرف باسم «الخدمات المخفية» Hidden Services[3].

في حين يُشاد بالدارك ويب لدوره في تعزيز الحركات الاجتماعية، فإن إخفاء الهوية الذي يوفره «تور» يوفر أيضًا ملاذًا لمجموعة واسعة من الأسواق الإجرامية. حيث يمكن للمستخدمين بيع وشراء منتجات وخدمات غير قانونية مثل الأسلحة والمخدرات وبطاقات الائتمان المسروقة. من بين هذه الأسواق، هناك منصات سيئة السمعة مثل «سيلك رود» و«ألفا باي»، التي تخدم مئات الآلاف من العملاء عبر الإنترنت. تشبه هذه الأسواق الأسواق القانونية مثل «إيباي»، حيث تسهل على البائعين الإعلان عن منتجاتهم وتقدم خدمات «الإيداع المؤقت» للعملاء الذين يدفعون بالعملات الرقمية مثل «البيتكوين.

فقد قللت الدارك ويب من مخاوف التعرض للكشف من خلال استضافة مواقع ومنتديات لا يمكن الوصول إليها إلا عبر مستخدمي متصفح «تور»، حيث وفرت منصة مثالية لإنشاء فضاءات إلكترونية يستطيع فيها ذوو الميول الجنسية تجاه الأطفال الاجتماع بحرية لمناقشة أفكارهم ومشاعرهم دون خوف من التعرض للتعرف، كما أن إخفاء الهوية الذي توفره الدارك ويب أتاح فرصة جديدة

(1) Owen G, Savage O (2015) The Tor Darknet. Global Commission on Internet Governance, London

(2) Owen G, Savage O (2015) The Tor Darknet. Global Commission on Internet Governance, London

(3) Van der Bruggen M, van Balen I, van Bunningen A, Talens P, Owens JN, Clapp K (2022) Even "lurkers" download: the behavior and illegal activities of members on a child sexual exploitation TOR hidden service. Aggress Violent Behav 101793. *https://doi.org/10. 1016/j.avb.2022.101793*

للوصول إلى تبادل مواد استغلال الأطفال جنسيًا، مما يربط بين العرض والطلب على نطاق عالمي غير مسبوق. ومع توفر الهواتف الذكية المزودة بكاميرات ذات جودة عالية، تلاشت الحدود بين المستهلكين والمنتجين لهذه المواد، مما أدى إلى زيادة كمية مواد استغلال الأطفال المتداولة. وفي الوقت الحالي، تقع منتديات الدارك ويب الخاصة بـ CSAM في قلب مجتمع إلكتروني عالمي يخدم اهتمامات مئات الآلاف من الأفراد الذين لديهم ميول جنسية نحو الأطفال.

لاحظت الأجهزة الرقابية زيادة في الجرائم الجنسية ضد الأطفال عبر الدارك ويب منذ عام 2009، عندما تم استهداف خدمة «فريدوم هوستينج» Freedom Hosting في أيرلندا، مما أدى إلى معركة قانونية استمرت 11 عامًا لتسليم مدير الموقع إلى الولايات المتحدة. وفي عام 2011، تعاونت اليوروبول مع 13 دولة في إطار «عملية الإنقاذ» Operation Rescue التي استهدفت المواقع المتعلقة باستغلال الأطفال جنسيًا، وقد أسفرت العملية عن تحديد هوية 670 مشتبهًا بهم، واعتقال 184 شخصًا، وحماية 230 طفلًا من الأذى الجنسي[1].

وفي الآونة الأخيرة، لا تزال اليوروبول تعتبر الدارك ويب تهديدًا إجراميًا رئيسيًا، وتشير منصة مكافحة التهديدات الإجرامية EMPACT إلى أن الشبكات المظلمة مثل «تور» تبقى المنصة الرئيسية للوصول إلى مواد استغلال الأطفال وتوزيعها بطرق غير تجارية[2].

تعتبرهذه الشبكات جذابة للمجرمين وسهلة الاستخدام، حيث يشعر الجناة بمزيد من الأمان والانخراط في مناقشات حول اهتماماتهم الجنسية داخل هذه المجتمعات المخفية على الإنترنت.

(1) Pierluigi P FBI admitted attack against Freedom Hosting. Security Affairs. *https://securityaffairs.co/wordpress/17767/hacking/fbi- admitted-attack-freedom-hosting.html*

(2) Council of the European Union (2023) Council conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022. https://data. c o n s i l i u m . e u r o p a . e u / d o c / d o c u m e n t / S T - 7 1 0 0 - 2 0 2 3 - I N I T / e n / p d f .

المبحث الثاني

عمليات الإتجار بالبشر عبر الدارك ويب

تنتشر عبر شبكة الدارك ويب مواقع تستغل النساء والأطفال جنسيًا[1] في ما يعرف بالغرف الحمراء، حيث تقوم عصابات الاتجار بالبشر بالاستفادة من هذه المنصات. كما تنتشر أيضًا عمليات بيع الأعضاء البشرية، وتشير بعض التقارير إلى وجود مواقع على الشبكة المظلمة مخصصة لإجراء تجارب على البشر، حيث يقوم مستخدمو هذه المواقع بخطف المشردين من الشوارع لاستخدامهم في التجارب العلمية، ويتم إدراج معلومات هؤلاء الأشخاص ضمن قوائم مخصصة للمهتمين بهذه التجارب. هناك أيضًا مواقع تختص في الإتجار بالنساء، حيث تعرض قوائم بكل المواصفات المطلوبة التي يمكن للمشتري الاختيار من بينها. الأكثر فزعًا هو سوق الأطفال على الدارك ويب، والذي يعد من أكثر الأسواق انتشارًا[2]، بحسب دراسة أجرتها جامعة بورتموث البريطانية في ديسمبر 2004، حيث تم الكشف عن أن أكثر المحتوى المتداول عبر شبكة Tor هو المواد الإباحية المتعلقة بالأطفال، تليها الأسواق السوداء التي تتاجر في المخدرات والأسلحة من جميع الأنواع، بالإضافة إلى الاتجار بالبشر وبالأعضاء البشرية. ولضمان جودة الخدمة في هذه الأسواق، يتم تقييم كل بائع من قبل المشترين لزيادة الثقة بين البائعين والمشترين الجدد، وذلك بجانب بيع أوراق الهوية المزورة مثل جوازات السفر. أكدت دراسة حديثة أجرتها جامعة كينجز كوليج البريطانية أن معظم الاستخدامات التي تتم عبر شبكة Tor وما يطلق عليه onion تتضمن تبادل محتوى غير قانوني. في بعض الحالات، يصل الأمر إلى مواقع مخصصة لمشاركة تجارب تناول لحوم البشر، حيث يشارك الأفراد في الكتابة عن تجربتهم في أكل لحم البشر لأول مرة.

---

(1) على الرغم من أن جرائم الاعتداء على الأطفال واستغلالهم جنسيا موجودة من قبل ظهور الإنترنت، فإن البعد الإلكتروني لهذه الجرائم قد مكَّن الجناة من التفاعل فيما بينهم والحصول على مواد الاستغلال الجنسي للأطفال عبر الإنترنت، وعلاوة على ذلك، فإن العدد المتزايد من الأطفال الصغار الذين يمكنهم الوصول إلى الإنترنت قد منح الجناة فرصة للوصول إلى الأطفال بسهولة أكبر – مقارنةً بالبيئة غير المتصلة بالإنترنت – وكان لذلك بدوره آثار كبيرة على طريقة عمل مرتكبي الجرائم ذات الصلة، وأصبح التقدم في التكنولوجيا محوريًا في الاستغلال الجنسي التجارى للأطفال، ويمكن للسياح الذين يمارسون الجنس مع الأطفال الاستفادة من تطبيقات الحوسبة الحسابية لتخزين الصور أو مقاطع الفيديو، ومن ثم تجنب المخاطرة بالنقل الفعلى لمواد تصور اعتداءات جنسية على الأطفال، وعلاوة على ذلك، تربط تكنولوجيا الهاتف المحمول بين منظمى عمليات استغلال الأطفال والاعتداء عليهم جنسيا والضحايا والمستهلكين، ومن ثم، تقل حاجة المنتجين والموزعين إلى الحضور شخصيا أثناء المعاملات، مما يؤدى بدوره إلى تحسين فرصهم فى تحاشي كشف أمرهم.

(2) محمد أحمد الضبع، «الإنترنت المظلم وجرائم الاتجار بالبشر: التحديات الأمنية والقانونية"، مجلة العلوم القانونية والاجتماعية، جامعة المنصورة، المجلد 9، العدد 2، 2022، ص. 125–154.

وقد كشفت الأبحاث والأدلة المباشرة أن المتجرين بالبشر يستخدمون التكنولوجيا في جميع مراحل الجريمة، بدءًا من استدراج الضحايا إلى مراقبتهم واستغلالهم. واحدة من أهم مزايا استخدام التكنولوجيا من قبل هؤلاء المتجرين هو أنها تتيح لهم العمل دون الكشف عن هويتهم. كما تسمح لهم العملات المشفرة بتنفيذ المعاملات المالية ونقل العائدات الإجرامية دون الكشف عن هويتهم. كما تسهل هذه التكنولوجيا عملية استدراج الضحايا واستغلالهم، من خلال استخدام مواقع الإعلانات المبوبة على الإنترنت وشبكات التواصل الاجتماعي كوسائل للإتجار بالبشر.[1] علاوة على ذلك، فإن إساءة استخدام هذه التقنيات تساعد المتجرين على إجراء صفقات مع زبائنهم ودخول أسواق جديدة لتوسيع نطاق عملياتهم الإجرامية. بإمكانهم أيضًا استخدام تطبيقات البث المباشر للوصول إلى أسواق أوسع لزبائن قد لا يكون لهم أي اتصال فعلي مسبق بالضحية[2].

إضافة إلى ذلك، تساعد تقنيات إساءة الاستخدام على مراقبة الضحايا وإجبارهم، حيث يمكن للمتجرين الاستفادة من تطبيقات تتبع الحركة وتحديد المواقع لتسهيل استغلال الضحايا. وإذا ما تمكن الضحايا من الإفلات من قبضة المتجرين، تظل إمكانية تعقبهم متاحة باستخدام هذه التطبيقات التي تتيح للجناة تحديد مكان وجود ضحاياهم، حيث تعتمد هذه التطبيقات على بيانات من الهواتف المحمولة الخاصة بالضحايا[3]. في نفس الوقت، تستخدم أجهزة إنفاذ القانون تطبيقات تتبع مماثلة للكشف عن أماكن وجود المجرمين المشتبه فيهم أو أي فرد آخر متورط في شبكة الإتجار بالبشر، إذ يتم استغلال بيانات تحديد المواقع الخاصة بالضحايا كشكل من أشكال جمع الأدلة وفقًا لليوروبول، أصبحت عمليات بث الاعتداءات الجنسية على الأطفال عبر الغرف الحمراء خطرًا حقيقيًا، حيث يتم نقل هذه اللقطات من خلال تطبيقات وسائل التواصل الاجتماعي وتطبيقات الدردشة المرئية ومنصات الألعاب وغرف الدردشة عبر الإنترنت. ومن أبرز المخاطر المتعلقة بتوزيع مواد الاستغلال الجنسي للأطفال على الإنترنت هو الزيادة المستمرة في استخدام الشبكة الخفية، حيث أشارت مؤسسة رصد الإنترنت Watch Internet Foundation إلى أن المواقع التي تستخدم تقنيات المسار الرقمي لإخفاء صور الاعتداء الجنسي على الأطفال لا تزال تمثل مشكلة كبيرة. وقد لاحظت المؤسسة أيضًا زيادة ملحوظة في عدد عناوين المواقع المرتبطة بالاعتداء الجنسي على الأطفال، حيث ارتفع عدد العناوين من 68,092 في عام 2015 إلى 105,047 في عام 2018 [4].

علاوة على ذلك، يواصل الأشخاص الذين يسعون للاعتداء الجنسي على الأطفال باستخدام

(1) Mark Latonero, Technology and Human Trafficking: The Rise of the Digital Pimp, USC Annenberg Center on Communication Leadership & Policy, 2011.

(2) Inter-Agency Coordination Group against Trafficking in Persons, "Human trafficking and technology: trends, challenges and opportunities", Issue brief, No.7(2019), pp.1-2

(3) Europol, Internet Organised Crime Threat Assessment (IOCTA) 2018, p. 35.

(4) Internet Watch Foundation, Once Upon a Year (Cambridge, United Kingdom, 2018), pp. 19 and 43.

الإنترنت البحث عن طرق جديدة للتهرب من الكشف، وذلك من خلال اكتسابهم مهارات تقنية متقدمة. في الآونة الأخيرة، تحول الاستخدام من المنتديات الكبيرة إلى تشكيل مجموعات صغيرة من المستخدمين، وهي الطريقة التي تسهلها تطبيقات التراسل المشفرة من البداية للنهاية عبر الأجهزة المحمولة. لمواجهة هذه الجرائم على شبكة الإنترنت، تم إنشاء قواعد بيانات خاصة لتحميل مواد الاعتداء الجنسي على الأطفال لاستخدامها كأدلة في التحقيقات، مثل قاعدة البيانات الدولية للاستغلال الجنسي للأطفال التابعة للمنظمة الدولية للشرطة الجنائية، كما يستخدم المركز الوطني للأطفال المفقودين والمستغلين في الولايات المتحدة قاعدة بيانات مركزية لتخزين المواد المرتبطة بهذه الأنواع من الاعتداءات.

وفي سياق آخر، تشير بعض التقارير الصحفية إلى أن الدارك ويب ساهم في إنقاذ طفل روسي يبلغ من العمر سبع سنوات، كان قد اختطفه أحد المعتدين واحتجزه في مخبأ تحت الأرض لمدة 52 يومًا في روسيا. تم تحرير الطفل بواسطة القوات الخاصة الروسية بالتعاون مع الإنتربول، حيث وردت المعلومات عن مكانه من منشورات عبر الدارك ويب التي ساعدت في تحديد موقعه[1].

كما هناك علاقة وثيقة بين الدارك ويب وعمليات تهريب المهاجرين، حيث تنتشر على هذه الشبكة العديد من المواقع التي تعرض جوازات السفر السليمة والمزورة للبيع، والتي تُستخدم في تهريب المهاجرين. كما أن تكنولوجيا المعلومات والاتصالات أصبحت أداة رئيسية يستخدمها المهاجرون والمتهربون على حد سواء لنقل المعلومات المتعلقة بالمسارات والخدمات والأسعار. من جانب آخر، ساعدت وسائل التواصل الاجتماعي المهربين على تغيير المسارات وتفادي التدابير التي تتخذها أجهزة إنفاذ القانون في دول العبور، مما ساهم في زيادة فعالية عمليات التهريب وتعطيل التحقيقات المتعلقة بهذه الجرائم[2].

يمكن أن تؤدي التطورات في تكنولوجيا الأجهزة المحمولة إلى تغيير العلاقة بين المهاجرين والمهربين، حيث أصبح بإمكان المهاجرين من خلال منصات مثل فيسبوك التحقق من موثوقية المهربين وتبادل المعلومات حولهم. وقد وصفت هذه العمليات بأنها "سلم الجدارة بالثقة"[3].

---

(1) انظر مقال بعنوان اختفى 52 يوما .. الدارك ويب ينقذ طفلا مخطوفا في مخبأ، منشور على موقع جريدة أخبار اليوم بتاريخ 2020/11/25، على الرابط
https://akhbarelyom.com/news/newdetails/3174288/1

(2) عبد الله محمود السيد، «الإتجار بالبشر عبر الإنترنت: دراسة تحليلية للجوانب الجنائية"، مجلة الدراسات الأمنية والقانونية، جامعة نايف العربية للعلوم الأمنية، العدد 44، 2021، ص. 85–112.، سناء بوخريص، «الإنترنت المظلم كوسيلة لارتكاب الجريمة المنظمة: دراسة حالة جرائم الإتجار بالبشر"، المجلة الجزائرية للقانون والاقتصاد، جامعة الجزائر 1، العدد 17، 2023.

(3) Judith Zijlstra and Ilse van Liempt, "Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys", International Journal of Migration and Border Studies, vol. 3, Nos. 2 and 3 (March 2017), pp. 176-177.

تمت عمليات الدفع للمهربين عبر نظم الدفع الإلكترونية، في حين قد تزيد العملات المشفرة من قدرة المهربين على تلقي الأموال وإخفائها، مما يعزز إمكانية غسل الأموال ويجنبهم التعرض للتحقيق أو التوقيف. تساهم التكنولوجيا أيضًا في توفير وثائق سفر مزورة باستخدام معدات متقدمة لتزييف الجوازات أو نسخها بطرق احتيالية[1]، مما يُسهل تهريب المهاجرين.

من زاوية أخرى، تسهم الرقمنة في تقليص الفجوات المعلوماتية التي قد يستفيد منها المهربون، حيث تُستخدم الإنترنت كوسيلة مفيدة لدعم التواصل بين المهاجرين والشبكات الاجتماعية للمعلومات، كما شهدنا زيادة في استقلالية المهاجرين في بعض الحالات، حيث أصبحوا أقل اعتمادًا على المهربين.

تتفاوت كيفية استخدام المهاجرين لوسائل التواصل الاجتماعي بناءً على جنسياتهم، خلفياتهم التعليمية، والوصول إلى الإنترنت، مما يُظهر وجود فجوة رقمية بين مجموعات المهاجرين من حيث القدرة على استخدام التكنولوجيا الفعالة ودفع تكاليف الخدمات الرقمية[2].

من جهة إنفاذ القانون، هناك اهتمام متزايد في استخدام التكنولوجيا لتعطيل شبكات تهريب المهاجرين، وقد تُسهم الأدلة المتاحة من وسائل التواصل الاجتماعي والتكنولوجيا في دعم تحقيقات السلطات الجنائية. وعليه، من الضروري تعزيز فعالية التدابير الجنائية وتشجيع تعاون مقدمي خدمات الإنترنت في رصد وحل الجرائم المرتبطة بالتهريب، مع تعزيز الشراكات بين الحكومات والقطاع الخاص والمنظمات غير الحكومية لهذا الغرض.

(1) UNODC Regional Office for South-East Asia and the Pacific, Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption. (Bangkok, 2019), p. 26.

(2) Alam Khorshed and Sophia Imran, "The digital divide and social inclusion among refugee migrants: a case in regional Australia", Information Technology and People, vol. 28, No. 2

الخاتمة

لقد بيّنت هذه الدراسة أن الثورة الرقمية، وعلى رأسها تقنية البلوك تشين، ليست مجرد ظاهرة تقنية، بل تحوّل بنيوي عميق في أنماط التفاعل الإنساني، بما في ذلك ارتكاب الجريمة. وقد أثبت التحليل أن البلوك تشين – رغم خصائصها المفيدة في تعزيز الشفافية والأمن السيبراني – يمكن أن تتحول إلى بيئة خصبة للأفعال الإجرامية، لا سيما تلك التي تمسّ الأشخاص وكرامتهم، كالابتزاز الجنسي، واستغلال الأطفال، والإتجار بالبشر، خصوصًا من خلال منصات «الدارك نت» والعقود الذكية.

وفي السياق الإماراتي، وعلى الرغم من الخطوات الريادية التي اتُخذت في مجال التحول الرقمي وتبني تقنيات البلوك تشين، لا تزال البنية التشريعية القائمة غير مكتملة أو غير كافية لمواجهة التحديات المستجدة، خاصة من حيث التجريم والملاحقة القضائية للانتهاكات التي تتم باستخدام هذه التقنيات. فقد أظهرت اللامركزية وإخفاء الهوية وغياب سلطة مركزية محددة، أنها تمثل عقبات حقيقية أمام تطبيق القواعد الجنائية التقليدية.

النتائج

• أظهرت الدراسة أن قانون العقوبات الإماراتي، رغم شموله العام، لا يتضمن تجريمًا دقيقًا أو توصيفًا قانونيًا خاصًا بالأفعال الجرمية المرتكبة بواسطة تقنيات مثل البلوك تشين، لا سيما في البيئات غير المركزية والمشفّرة. فالمفاهيم التقليدية للجريمة الجنائية (مثل الفاعل والشريك والمكان) تواجه تحديًا جوهريًا في سياق الشبكات اللامركزية

• أفضت البلوك تشين إلى ظاهرة «المجهولية التقنية» التي يصعب معها تحديد الفاعل، ما يطرح إشكالية أمام نص المادة (38) من قانون العقوبات الإماراتي التي تربط المسؤولية الجنائية بالفعل الإرادي الواعي. وبالتالي، فإن الملاحقة القضائية تعترضها عقبات في التكييف القانوني وإثبات القصد الجرمي.

• تعذر تطبيق بعض المبادئ الإجرائية الجنائية التقليدية وعدم مواءمة قواعد الإثبات الجنائي للتقنيات الحديثة. فنظام الإثبات القائم على الكتابة، الاعتراف، والشهادة، يصعب تطبيقه على جرائم البلوك تشين التي تعتمد على «أكواد مشفّرة» ومعاملات غير قابلة للتعديل، دون أن يكون هناك إطار قانوني يُعترف فيه بالمخرجات التقنية كأدلة جنائية مكتملة الشروط.

التوصيات

• تجريم خاص للأفعال الماسة بالأشخاص المرتكبة عبر شبكات مشفّرة أو منصات لا مركزية، حيث ينبغي تعديل قانون العقوبات الإماراتي أو قانون مكافحة الجرائم الإلكترونية، لإدراج نصوص صريحة تُجرّم الاعتداءات الواقعة على الأشخاص (كالابتزاز الجنسي، استغلال الأطفال، والإتجار بالبشر) إذا تم ارتكابها عبر الدارك ويب أو من خلال منصات بلوك تشين مجهولة المصدر، مع

اعتبار استخدام أدوات إخفاء الهوية ظرفًا مشددًا في العقوبة.

• إنشاء وحدة وطنية مختصة برصد وتتبع الانتهاكات الجسيمة للأشخاص في الفضاء الرقمي المشفّر وتوصية بإنشاء وحدة تحقيق جنائي رقمية متخصصة ضمن النيابة العامة أو هيئة الأمن السيبراني، مزوّدة بأدوات تحليل سلاسل الكتل (blockchain forensics)، وتعقب المستخدمين في بيئات الدارك نت، مع صلاحيات للوصول إلى بيانات الجهات الوسيطة والتعاون مع المنصات العالمية لتحديد الفاعلين في الجرائم المجهولة.

• وضع إطار قانوني للتعاون القضائي الدولي في ملاحقة الجرائم الجسيمة ضد الأشخاص عبر الإنترنت المظلم.

• وضرورة تفعيل آليات الإنابة القضائية الدولية والتسليم، بما يشمل الجرائم المرتكبة ضد الأشخاص باستخدام تقنيات التشفير العالية، وتجاوز عقبة "ازدواجية التجريم" بالتنصيص على مبدأ "النتيجة الضارة" كمعيار للاختصاص، خصوصًا في الجرائم ضد القاصرين أو تلك المرتكبة من الخارج وامتدت آثارها إلى داخل الدولة.

المراجع

أولًا: المراجع العربية

1. المراجع العامة

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

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

• د. سارة النجار، البلوك تشين وتطبيقاتها في العالم العربي. الرياض: دار الفكر السعودي، 2023.

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

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

• النيابة العامة لدولة الإمارات العربية المتحدة، التقرير السنوي حول مكافحة الجرائم الإلكترونية والرقمية 2023. أبوظبي: إدارة مكافحة الجرائم التقنية، 2024.

2. المراجع المتخصصة

• مصطفى البنا، «البلوك تشين وتحديات القانون الجزائي العربي"، المجلة القانونية الخليجية، العدد 9، 2023.

• عبد الله محمود السيد، «الاتجار بالبشر عبر الإنترنت: دراسة تحليلية للجوانب الجنائية"، مجلة الدراسات الأمنية والقانونية، جامعة نايف العربية للعلوم الأمنية، العدد 44، 2021.

• محمد أحمد الضبع، «الإنترنت المظلم وجرائم الاتجار بالبشر: التحديات الأمنية والقانونية"، مجلة العلوم القانونية والاجتماعية، جامعة المنصورة، المجلد 9، العدد 2، 2022.

• سناء بوخريص، «الإنترنت المظلم كوسيلة لارتكاب الجريمة المنظمة: دراسة حالة جرائم الاتجار بالبشر"، المجلة الجزائرية للقانون والاقتصاد، جامعة الجزائر 1، العدد 17، 2023.

3. الدراسات والتقارير الصحفية

• "اختفى 52 يوما .. الدارك ويب ينقذ طفلا مخطوفا في مخبأ"، جريدة أخبار اليوم، 25 نوفمبر 2020.
رابط: https://akhbarelyom.com/news/newdetails/3174288/1

ثانيًا: المراجع الأجنبية

1. المراجع العامة

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

• Owen, G., & Savage, O. The Tor Darknet. Global Commission on Internet Governance, London, 2015.

•Datareportal. Digital Around the World, 2022.

https://datareportal.com/global-digitaloverview

• Goldman, J., & Ronken, C. (2000). The Concept of Childhood. https://www.ccc.qld.gov.au/sites/default/files/2020-02/Project-AXIS-Volume-4-Selected-research-papers-Report-2000.pdf

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

• Latonero, Mark. Technology and Human Trafficking: The Rise of the Digital Pimp. USC Annenberg Center on Communication Leadership & Policy, 2011.

• Inter-Agency Coordination Group Against Trafficking in Persons. Human Trafficking and Technology: Trends, Challenges and Opportunities, Issue Brief No. 7, 2019.

• Europol. Internet Organised Crime Threat Assessment (IOCTA), 2018.

• Internet Watch Foundation. Once Upon a Year. Cambridge, United Kingdom, 2018.

• Van der Bruggen, M., et al. "Even 'Lurkers' Download: The Behavior and Illegal Activities of Members on a Child Sexual Exploitation TOR Hidden Service." Aggression and Violent Behavior, 2022.

• Insoll, T., et al. "Risk Factors for Child Sexual Abuse Material Users Contacting Children Online." Journal of Online Trust and Safety, Vol. 1, No. 2, 2022. https://doi.org/10.54501/jots.v1i2.29

• Pierluigi, P. "FBI Admitted Attack Against Freedom Hosting." Security Affairs. https://securityaffairs.co/wordpress/17767/hacking/fbi-admitted-attack-freedom-hosting.html

• Council of the European Union. Council Conclusions on the Permanent Continuation of the EU Policy Cycle for Organised and Serious International Crime: EMPACT 2022. 2023. https://data.consilium.europa.eu/doc/document/ST-7100-2023-INIT/en/pdf

• Zijlstra, Judith & van Liempt, Ilse. "Smart(phone) Travelling: Understanding the Use and Impact of Mobile Technology on Irregular Migration Journeys." International Journal of Migration and Border Studies, Vol. 3, Nos. 2–3, 2017.

• UNODC Regional Office for South-East Asia and the Pacific. Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption. Bangkok, 2019.

• Khorshed, Alam & Imran, Sophia. "The Digital Divide and Social Inclusion Among Refugee Migrants: A Case in Regional Australia." Information Technology and People, Vol. 28, No. 2.