جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة قطاع الشريعة والقانون

مجلة علمية نصف سنوية محكمة

تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها

كلية الشريعة والقانون بالقاهرة

جامعة الأزهر

العدد الثامن عشر

أغسطس ٢٠٢٥م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة قطاع الشريعة والقانون

جمهورية مصر العربية – كلية الشريعة والقانون – القاهرة – الدراسة – شارع جوهر القائد

للتواصل مع المجلة : 201028127441+ ، 201221067852+

البريد الالكتروني

Journal.sha.law@azhar.edu.eg

جميع الآراء الواردة في هذه المجلة تعبر عن وجهة نظر أصحابها، ولا تعبر بالضرورة عن وجهة نظر المجلة وليست مسئولة عنها

رقم الإيـــداع

٢٠٢٥ / ١٨٠٥٣

الترقيم الدولي للنشر

ISSN: 2636-2570

الترقيم الدولي الإلكتروني

ISSN: 2805-329X

الموقع الإلكتروني

https://jssl.journals.ekb.eg

دور تقنية البلوك تشين في مكافحة غش الأدوية:
نحو إطار قانوني جنائي متكامل

The Role of Blockchain Technology in Combating Drug Counterfeiting:
Towards a Comprehensive Criminal Legal Framework

إعداد

د. محمد فتحي شحتة ابراهيم دياب

أستاذ القانون الجنائي المشارك

قسم القانون -كلية الشريعة والقانون- جامعة حائل

دور تقنية البلوك تشين في مكافحة غش الأدوية: نحو إطار قانوني جنائي متكامل

محمد فتحي شحتة ابراهيم دياب
قسم القانون، كلية الشريعة والقانون، جامعة حائل، المملكة العربية السعودية.
البريد الإلكتروني: m.fathi@uoh.edu.sa

ملخص البحث:

في سياق مكافحة جريمة تزييف الأدوية، يعالج هذا البحث فجوة معرفية وتشريعية مهمة، تتمثل في غياب إطار قانوني جنائي متكامل قادر على استيعاب الفرص والتحديات التي تفرضها تقنية البلوك تشين. تتمحور مشكلة البحث حول قصور المفاهيم التقليدية للإثبات والمسؤولية والولاية القضائية عن التعامل مع الطبيعة اللامركزية والعابرة للحدود لهذه التقنية، مما يخلق حالة من عدم اليقين القانوني التي تهدد فعالية العدالة الجنائية وحماية الصحة العامة.

يهدف البحث بشكل أساس إلى اقتراح نموذج لإطار قانوني جنائي شامل، ويجيب عن التساؤل المحوري: كيف يمكن تكييف القانون الجنائي ليوازن بين الاستفادة من قدرات البلوك تشين وضمانات المحاكمة العادلة؟ ولتحقيق ذلك، تم اعتماد منهج بحثي نوعي، يعتمد على التحليل القانوني المقارن للنصوص التشريعية والاتفاقيات الدولية والأدبيات الأكاديمية.

كشفت النتائج الرئيسة عن مفارقة جوهرية؛ فبينما توفر البلوك تشين سلامة داخلية فائقة للدليل، فإن حجيتها تقوضها "مشكلة الأوراكل" (صحة البيانات المدخلة). كما أظهرت النتائج أن اللامركزية تفكك مفاهيم الفاعل المادي والسيادة الإقليمية. وبناءً عليه، يوصي البحث بسن تشريعات خاصة تجرم إساءة استخدام التقنية، وتضع قواعد واضحة لمسؤولية الأطراف الوسيطة، وتتبنى معايير حديثة للاختصاص القضائي كـ"معيار الأثر". كما يقترح البحث تكثيف التعاون الدولي وتدريب الكوادر القضائية كاتجاهات بحثية وعملية مستقبلية.

الكلمات المفتاحية: تزييف الأدوية باستخدام البلوك تشين، الإطار القانوني للبلوك تشين، كيفية منع تزييف الأدوية، البلوك تشين في سلسلة الإمداد الدوائية، المسؤولية الجنائية لمطوري البلوك تشين.

The Role of Blockchain Technology in Combating Drug Counterfeiting: Towards a Comprehensive Criminal Legal Framework

Mohamed Fathi Shehta Ibrahim Diab
Department of Law, College of Shari'a and Law, University of Hail, Saudi Arabia.
E-mail: m.fathi@uoh.edu.sa

Abstract:

In the context of combating the crime of drug counterfeiting, this research addresses a significant doctrinal and legislative lacuna: the absence of a comprehensive criminal legal framework capable of encompassing the opportunities and challenges posed by blockchain technology. The research problem centers on the inadequacy of conventional doctrines of evidence, liability, and jurisdiction to contend with the decentralized and transnational nature of this technology, thereby creating a state of legal uncertainty that threatens the efficacy of criminal justice and the protection of public health.

The principal objective of this study is to propose a model for a comprehensive criminal legal framework, answering the central research question: How can criminal law be adapted to balance leveraging the capabilities of blockchain with the fundamental safeguards of a fair trial? To this end, a qualitative research methodology is employed, based on the comparative legal analysis of statutory provisions, international conventions, and scholarly doctrine.

The principal findings reveal a fundamental paradox: while blockchain affords superior internal integrity to evidence, its probative value is critically undermined by the 'Oracle Problem'—the validity of input data. Furthermore, the findings demonstrate that decentralization deconstructs the legal concepts of *actus reus* and territorial sovereignty. Accordingly, the research recommends the enactment of *sui generis* legislation that criminalizes the misuse of the technology, establishes clear rules for intermediary liability, and adopts modern jurisdictional standards such as the 'Effects Doctrine'. The research further proposes the intensification of

international cooperation and the specialized training of judicial personnel as crucial avenues for future research and practice.

Keywords: Blockchain Drug Counterfeiting, Legal Framework For Blockchain, How To Prevent Counterfeit Drugs, Blockchain In Pharmaceutical Supply Chain, Criminal Liability Blockchain Developers.

١. مقدمة

يمثل غش وتزييف الأدوية تهديداً وجودياً للصحة العامة العالمية، وأمناً قومياً للدول، إذ تشير تقديرات منظمة الصحة العالمية إلى أن ما يقارب ١٠٪ من الأدوية المتداولة في الدول النامية هي أدوية مغشوشة أو دون المعايير المطلوبة، مما يؤدي إلى مئات الآلاف من الوفيات سنوياً، فضلاً عن الخسائر الاقتصادية الفادحة التي تتكبدها شركات الأدوية المشروعة والأنظمة الصحية. من منظور القانون الجنائي، لا تقتصر هذه الظاهرة على كونها جريمة غش تجاري يسيرة، بل هي جريمة مركبة ومعقدة، غالباً ما ترتبط بشبكات الجريمة المنظمة العابرة للحدود، وتمثل اعتداءً مباشراً على الحق في الحياة والسلامة الجسدية.

إن الآليات التقليدية لمكافحة هذه الجريمة، التي تعتمد على الرقابة المادية، والتتبع الورقي والسلاسل التوريد المركزية، أثبتت قصورها الشديد في مواجهة التطور الهائل لأساليب المزورين وقدرتهم على اختراق سلاسل الإمداد الدوائية. وفي خضم هذا التحدي، تبرز تقنية "البلوك تشين" (Blockchain) بوصفه بارقة أمل وحل تكنولوجي ثوري؛ فبفضل خصائصها الفريدة المتمثلة في اللامركزية، والثبات، وعدم القابلية للتغيير، والشفافية، تقدم البلوك تشين إمكانية إنشاء سجل رقمي موثوق وآمن لتتبع الدواء منذ لحظة تصنيعه وحتى وصوله إلى يد المريض، وهو ما يعرف بمفهوم "من المصنع إلى المريض".

لكن هذا الحل التكنولوجي الواعد يثير في المقابل تحديات قانونية جنائية غير مسبوقة. فكيف يمكن للقانون الجنائي بأدواته ومفاهيمه التي تطورت عبر قرون أن يستوعب هذه التقنية ويتفاعل معها؟ كيف يمكن تكييف مفاهيم الإثبات الجنائي، والمسؤولية الجنائية، والولاية القضائية لتنسجم مع طبيعة البلوك تشين اللامركزية والعابرة للحدود؟ إن الفجوة بين سرعة التطور التكنولوجي وبطء التطور التشريعي تخلق فراغاً قانونياً قد يستغله المجرمون، أو قد يعوق تبني هذه التقنية المنقذة للحياة.

من هنا ينطلق هذا البحث ليس فقط لاستعراض الإمكانيات التقنية للبلوك تشين في مكافحة غش الأدوية، بل ليغوص في عمق الإشكاليات القانونية الجنائية التي تثيرها، ويهدف في نهاية المطاف إلى وضع لبنات أساسية لإطار قانوني جنائي متكامل، يوازن بين ضرورة الاستفادة من هذه التقنية لتعزيز العدالة الجنائية، وحماية المجتمع، وبين احترام الضمانات، والحقوق الأساسية للمتهمين.

١,١. أهمية البحث:

تكمن أهمية هذا البحث في أبعاد متعددة:

١,١,١. الأهمية النظرية:

– سد الفجوة المعرفية: – يسد هذا البحث فجوة كبيرة في الأدبيات القانونية الجنائية العربية والعالمية، التي نادراً ما تناولت تقنية البلوك تشين من منظور جنائي موضوعي وإجرائي متعمق، خاصة في سياق جريمة محددة كغش الأدوية.

– تطوير النظرية العامة للجريمة: -يسهم البحث في إعادة التفكير في أركان الجريمة التقليدية (الركن المادي والمعنوي) في البيئة الرقمية اللامركزية. على سبيل المثال، كيف يتجسد "الفعل المادي" في إدخال بيانات كاذبة على سلسلة كتل؟ وكيف يمكن إثبات "القصد الجنائي" لأطراف متعددين في شبكة لا مركزية؟

– إثراء فقه الإثبات الجنائي: – يقدم البحث تحليلاً معمقاً لطبيعة "الدليل الرقمي" المستمد من البلوك تشين، ويناقش حجيته وقيمته الثبوتية في مواجهة مبادئ الإثبات التقليدية، مثل مبدأ "شفوية المرافعة" ومبدأ "الاقتناع القضائي الحر".

١,١,٢. الأهمية العملية والتطبيقية:

ـ دليل للمشرّع الوطني والدولي: يقدم البحث توصيات تشريعية واضحة ومحددة لصناع القرار والبرلمانات، لتعديل القوانين الجنائية وقوانين الإجراءات الجنائية الحالية، أو سن تشريعات جديدة تتواءم مع هذه التقنية.

– أداة للقضاة وأعضاء النيابة العامة: يزود البحث القضاة والمحققين بفهم قانوني وتقني عميق لكيفية التعامل مع الأدلة المستمدة من البلوك تشين، وكيفية تقديرها وتأسيس الأحكام عليها.

– مرجع للمحامين والمدافعين: يساعد المحامين على فهم نقاط القوة والضعف في الأدلة المستمدة من هذه التقنية، مما يمكنهم من بناء دفوعهم واستراتيجياتهم الدفاعية بفعالية.

– تعزيز التعاون القضائي الدولي: نظراً للطبيعة العابرة للحدود لجريمة غش الأدوية وتقنية البلوك تشين، يقدم البحث مقترحات لتطوير آليات التعاون الدولي في المسائل الجنائية، مثل طلبات المساعدة القانونية المتبادلة وتسليم المجرمين في هذا السياق الجديد.

١,٢. أهداف البحث:

يسعى هذا البحث إلى تحقيق الأهداف التالية:

– تحليل الطبيعة الإجرامية لظاهرة غش الأدوية في ضوء التشريعات الجنائية الوطنية والمقارنة والاتفاقيات الدولية، وتحديد خصائصها بوصفها جريمة منظمة عابرة للحدود.

– تقييم مدى كفاية الأطر القانونية الجنائية الحالية (الموضوعية والإجرائية) في التصدي لهذه الجريمة، وإبراز أوجه القصور التي تستدعي التدخل التشريعي.

– استكشاف الآلية التقنية لعمل البلوك تشين في تتبع سلاسل الإمداد الدوائية، مع التركيز على الخصائص ذات الأثر القانوني المباشر (مثل التوقيعات الرقمية، والعقود الذكية، وسجلات المعاملات).

– تحديد وتحليل الإشكاليات الجنائية الرئيسة التي يثيرها استخدام البلوك تشين بوصفه أداة للمكافحة، وتحديداً في مجالات الإثبات، والمسؤولية الجنائية، والولاية القضائية.

– اقتراح نموذج لإطار قانوني جنائي متكامل يتضمن تعديلات على مستوى القانون الموضوعي (تجريم أفعال محددة)، والقانون الإجرائي (قبول الأدلة وإجراءات التحقيق)، والتعاون الدولي.

١,٣. أسباب اختيار البحث:

ـ حداثة الموضوع وأصالته: يعد تقاطع البلوك تشين مع القانون الجنائي حقلاً بحثياً بكراً، مما يمنح البحث قيمة علمية مضافة وفرصاً كبيرة للمساهمة الأصيلة.

– الطابع الملح لهذه الإشكالية: إن خطورة جريمة غش الأدوية، وتأثيرها المباشر على حياة الإنسان يستدعيان البحث عن حلول فعّالة، تشمل الحلول التقنية والقانونية.

– الفراغ التشريعي العالمي: لا يوجد حاليًا تشريع جنائي مُخصص يُنظّم تطبيق تقنية البلوك تشين في مجال مكافحة الجريمة؛ لذا فإن هذا البحث استشرافي وله أهمية بالغة في توجيه السياسات التشريعية المستقبلية

– الاهتمامات الشخصية والأكاديمية: بصفتي باحثًا في القانون الجنائي، يُمثّل هذا الموضوع تحديًا فكريًا مثيرًا للاهتمام، إذ يتطلب التوفيق بين مبادئ القانون الجنائي الراسخة والطبيعة المتغيرة للتكنولوجيا، التي تُشكّل جوهر تطور الفلسفة والممارسة القانونية.

١,٤. إشكاليات البحث:

تتمحور الإشكالية الرئيسة للبحث حول "القصور المفاهيمي والتشريعي في القانون الجنائي التقليدي عن مواكبة واستيعاب الفرص والتحديات التي تفرضها تقنية البلوك تشين بوصفها أداة لمكافحة جريمة غش الأدوية، مما يولد حالة من عدم اليقين القانوني وقد يعوق تطبيق العدالة الجنائية الفعالة.

وتتفرع عن هذه الإشكالية الرئيسة عدة إشكاليات فرعية:

– إشكالية الإثبات: هل يمكن اعتبار البيانات المسجلة على سلسلة الكتل "دليلاً كتابياً" أم "قرينة"؟ ما هي شروط قبول هذا الدليل أمام القضاء الجنائي؟ وكيف يمكن التحقق من صحة وحجية البيانات المدخلة أصلاً إلى السلسلة مشكلة The Oracle Problem؟ وكيف نوفق بين ثبات السجل وحق المتهم في مناقشة الدليل؟

– إشكالية المسؤولية الجنائية: في بيئة لا مركزية، من هو المسؤول جنائياً عن جريمة ترتكب عبر الشبكة أو يتم كشفها بواسطتها؟ هل هو المزور الذي استخدم الشبكة؟ أم مطور البروتوكول؟ أم مشغلو العقد (Nodes) الذين يتحققون من صحة المعاملات؟ وكيف يمكن تطبيق نظريات المساهمة الجنائية (الفاعل الأصلي والشريك) في هذا السياق؟

– إشكالية الولاية القضائية: بما أن البلوك تشين شبكة عالمية موزعة، فأي دولة تمتلك الاختصاص القضائي لمحاكمة الجريمة؟ هل هي دولة الضحية؟ أم دولة المزور؟ أم دولة توجد فيها إحدى "عقد" الشبكة؟ هذا يمثل تحدياً كبيراً لمبادئ الاختصاص الإقليمي والشخصي التقليدية.

- إشكالية التوازن بين المكافحة والحقوق: كيف يمكن الموازنة بين استخدام شفافية البلوك تشين لأغراض التحقيق الجنائي، وبين الحق في الخصوصية وحماية البيانات الشخصية للمستخدمين الشرعيين للسلسلة (المرضى، الصيادلة)؟

١,٥. تساؤلات البحث:

للإجابة على إشكاليات البحث، سيجيب البحث عن التساؤلات التالية:

التساؤل الرئيس: إلى أي مدى يمكن تطوير إطار قانوني جنائي شامل وفعال يدمج تقنية البلوك تشين بوصفها أداة لمكافحة جريمة غش الأدوية مع ضمان احترام المبادئ الأساسية للعدالة الجنائية؟

- التساؤلات الفرعية:

- ما هي أوجه القصور في التشريعات الجنائية الوطنية والدولية الحالية التي تعوق المكافحة الفعالة لجريمة غش الأدوية؟

- من الناحية القانونية، ما هي الطبيعة القانونية للبيانات المسجلة على البلوك تشين، وما هي حجيتها في الإثبات الجنائي وفقاً للنظريات القائمة؟

- كيف يمكن تحديد وتوزيع المسؤولية الجنائية على مختلف الأطراف الفاعلة في منظومة البلوك تشين (المستخدمين، المطورين، مشغلي العقد)؟

- ما هو النموذج الأنسب للولاية القضائية الجنائية للتعامل مع الجرائم المرتبطة بالبلوك تشين العابرة للحدود؟

- ما هي الضوابط التشريعية والإجرائية اللازمة لتحقيق التوازن بين متطلبات التحقيق الجنائي باستخدام البلوك تشين، والحق في الخصوصية وحماية البيانات؟

١,٦. الدراسات السابقة:

سيقوم البحث بمراجعة نقدية وتحليلية للدراسات السابقة ضمن ثلاثة محاور رئيسة، مع التركيز على إبراز الفجوة التي يسعى هذا البحث لملئها:

- المحور الأول: الدراسات القانونية حول جريمة غش الأدوية: وتشمل الأبحاث التي تناولت التكييف القانوني للجريمة، وعقوباتها، والتحديات التي تواجه إنفاذ القانون. (مثال: دراسات حول اتفاقية "ميديكرايم" للمجلس الأوروبي). سيُظهر البحث أن هذه الدراسات غالباً ما تركز على الجوانب التقليدية للجريمة دون التطرق بعمق للحلول التكنولوجية المتقدمة.

- المحور الثاني: الدراسات التقنية والقانونية العامة حول البلوك تشين: وتشمل الأبحاث التي تشرح آلية عمل البلوك تشين وتطبيقاتها في سلاسل الإمداد، وبعض الكتابات القانونية الأولية التي تناولت آثارها على قانون العقود، والملكية الفكرية، والخصوصية. سيُظهر البحث أن هذه الدراسات تفتقر إلى التركيز الجنائي المتخصص، وتتعامل مع القانون بوصفه عنصرا ثانويا.

- المحور الثالث: الدراسات التي تربط بين البلوك تشين ومكافحة التزييف (بشكل عام): هناك عدد قليل من الدراسات التي بدأت في استكشاف هذا الرابط، لكنها في الغالب دراسات حالة تركز على الجدوى الاقتصادية أو التقنية، أو تتناول الجانب التنظيمي والمدني. الفجوة البحثية التي سيغطيها هذا البحث تكمن هنا تحديداً: لا توجد دراسة شاملة ومتعمقة تتناول الموضوع من منظور القانون الجنائي الموضوعي والإجرائي بشكل متكامل.

١,٧. منهج البحث:

لتحقيق أهداف البحث والإجابة على تساؤلاته، سيتم الاعتماد على منهج متكامل يجمع بين:

- المنهج التحليلي: سيتم استخدامه لتحليل النصوص القانونية ذات الصلة (قوانين العقوبات، قوانين الإجراءات الجنائية، الاتفاقيات الدولية)، وتفكيك المفاهيم القانونية التقليدية (مثل الدليل، المسؤولية، الاختصاص) لتقييم مدى قابليتها للتطبيق في سياق البلوك تشين.

٢ - المنهج المقارن: سيتم عقد مقارنات بين الأنظمة القانونية المختلفة (مثل النظام الأنجلو-أمريكي والنظام اللاتيني-جرماني) في تعاملها مع الدليل الرقمي والجرائم السيبرانية، للاستفادة من التجارب الرائدة واستلهام الحلول التي يمكن تكييفها. سيتم التركيز على تشريعات دول مثل الولايات المتحدة (فيما يخص الأدلة الرقمية) والاتحاد الأوروبي (فيما يخص حماية البيانات.

١. المنهج الاستشرافي/البنائي: لن يكتفي البحث بالوصف والتحليل، بل سيسعى إلى بناء واقتراح حلول مستقبلية. سيتم استخدام هذا المنهج في الجزء الأخير من البحث لصياغة "الإطار القانوني الجنائي المتكامل" المقترح، وتقديم توصيات تشريعية عملية.

١,٨. خطة البحث:

مقدمة عامة:

- تمهيد: خطورة جريمة غش الأدوية بوصفها تهديدا عالميا.
- عرض موجز لقصور آليات المكافحة التقليدية.
- تقديم تقنية البلوك تشين بوصفها حلا تكنولوجيا واعدا.
- طرح الإشكالية الرئيسة: الفجوة بين التكنولوجيا والقانون الجنائي.
- بيان أهمية البحث وأهدافه ومنهجيته وهيكله العام.

٢. الإطار المفاهيمي لجريمة غش الأدوية وتقنية البلوك تشين

٢.١. الطبيعة القانونية لجريمة غش الأدوية

٢.٢. ماهية تقنية البلوك تشين وآلية عملها في سلاسل الإمداد الدوائية

٣. إشكالية الإثبات الجنائي بالبيانات المستمدة من البلوك تشين

٣.١. الطبيعة القانونية لسجل البلوك تشين بوصفها دليل إثبات (دليل كتابي، سجل إلكتروني، قرينة).

٣.٢. حجية الدليل المستمد من البلوك تشين بين الحصانة التقنية والهشاشة الإجرامية.

٤. إشكالية إسناد المسؤولية الجنائية في الشبكات اللامركزية

٤.١. تحديد مرتكب الفعل المادي في بيئة البلوك تشين: من هو الفاعل في "مسرح الجريمة الخوارزمي"؟

٤.٢. إثبات القصد الجنائي لدى الأطراف المتعددة.

٤.٣. مدى مسؤولية الأطراف الوسيطة من حيادية الكود إلى التواطؤ الجنائي (مطور البروتوكول، مشغل العقدة، منصة التبادل).

٥. إشكالية الولاية القضائية الجنائية على الجرائم المرتبطة بالبلوك تشين.

٥.١. قصور معايير الاختصاص التقليدية في مواجهة الجريمة اللامركزية.

٥.٢. نحو تبني معايير حديثة للاختصاص (معيار الأثر نموذجاً).

٦. خاتمة عامة

٦.١. النتائج الرئيسة للبحث: تلخيص لأهم ما توصلت إليه الدراسة من نتائج بخصوص الإشكاليات المطروحة.

٦.٢. التوصيات:

٦.٣. نحو بناء إطار قانوني جنائي متكامل

٢. الإطار المفاهيمي لجريمة غش الأدوية وتقنية البلوك تشين

تمهيد:

إن أي تحليل قانوني جنائي معمّق يتطلب، كشرط منهجي أولي، بناء أساس مفاهيمي صلب وواضح للمصطلحات والموضوعات التي يتناولها. وفي سياق هذا البحث، الذي يقع عند نقطة التقاطع الدقيقة بين القانون الجنائي التقليدي والتكنولوجيا الرقمية الثورية، تكتسب هذه الضرورة المنهجية أهمية مضاعفة فلا يمكن تقييم جدوى حل تكنولوجي لمشكلة إجرامية دون فهم دقيق لكل من طبيعة المشكلة وآلية عمل الحل المقترح.

من هذا المنطلق، يهدف هذا القسم إلى إرساء الإطار المفاهيمي المزدوج الذي سيقوم عليه صرح البحث بأكمله. فهو سيتناول بالتحليل طرفي المعادلة: الجريمة من جهة، والتكنولوجيا من جهة أخرى.

في القسم الفرعي الأول سيتم تفكيك البنية القانونية لجريمة غش الأدوية. لن يقتصر التحليل على مجرد تعريف الظاهرة، بل سيغوص في أعماق توصيفها الجنائي، متتبعاً تطوره في التشريعات الوطنية والمقارنة، ومبيناً التحول الحاسم من اعتباره مجرد اعتداء على الملكية الفكرية إلى كونه جريمة مستقلة تهدد الصحة العامة والحق في الحياة. كما سيسلط الضوء على الأبعاد الدولية للجريمة، متخذاً من اتفاقية "ميديكرايم" نموذجاً للدراسة، ومحللاً خصائصها بوصفها نشاطا إجراميا منظما وعابرا للحدود، وهو ما يبرر الحاجة إلى حلول تتجاوز الأطر الوطنية التقليدية.

"أما في القسم الفرعي الثاني، فسينتقل من عالم القانون إلى عالم التكنولوجيا، ليقدم تحليلاً قانونياً-تقنياً لتقنية البلوك تشين. سيتجاوز هذا التحليل الشرح السطحي، ليركز على تفكيك بنيتها المعمارية القائمة على اللامركزية والثبات، التي تمنحها قيمتها الاستثنائية في سياق إنفاذ القانون الجنائي". سيتم بعد ذلك استعراض التطبيق العملي لهذه المبادئ في تأمين سلاسل الإمداد الدوائية عبر أنظمة التتبع (Track and Trace)، مع إيلاء اهتمام خاص لدور "العقود الذكية" بوصفها أداة لأتمتة عمليات التحقق والرقابة، وهو مفهوم سيكون له آثار قانونية عميقة سيتم استكشافها لاحقاً في صلب البحث.

إن الهدف النهائي لهذا القسم هو تزويد القارئ بالعدسة المفاهيمية اللازمة لفهم التحديات والفرص التي ستُطرح في الفصول اللاحقة. فمن خلال بناء جسر معرفي بين عالم القانون الجنائي وعالم البلوك تشين، نمهد الطريق لإجراء حوار مثمر بين المجالين، وهو الحوار الذي يمثل جوهر الإشكالية البحثية لهذا العمل.

٢,١. الطبيعة القانونية لجريمة غش الأدوية

إن تحديد الطبيعة القانونية لجريمة غش الأدوية **يتجاوز** كونه مسألة تصنيف فقهي مجرد، بل هو عملية تأسيسية تحدد مسار الاستجابة الجنائية بأكملها. فالوصف الذي يتبناه المشرّع هو الذي يحدد المصلحة المحمية جنائياً، ويرسم حدود الركن المادي، والركن المعنوي للجريمة، ويوجه السياسة العقابية، ويؤطر

صلاحيات أجهزة إنفاذ القانون. إن الفشل في إدراك الجوهر الحقيقي لهذه الجريمة، واعتبارها مجرد مخالفة تجارية أو اعتداء على أصل غير مادي، قد أدى تاريخياً إلى استجابات تشريعية وقضائية فاترة، لا تتناسب إطلاقاً مع جسامة الخطر الذي تمثله على الحق في الحياة والسلامة الجسدية، وهما من أسمى الحقوق التي ينهض القانون الجنائي لحمايتها.

يهدف هذا القسم الفرعي إلى تفسير هذه القضية المعقدة من خلال تحليل ثلاثي الأبعاد. سنبدأ بدراسة التشريعات الوطنية والمقارنة لكشف الاختلافات في التوصيفات الجنائية والآثار المترتبة على هذا الاختلاف. ثم سنحلل من منظور دولي، كيف تعيد الاتفاقية الدولية بشأن الجرائم الطبية تعريف الجريمة على نطاق عالمي، محولةً إياها من قضية تتعلق بالملكية الفكرية إلى قضية تتعلق بالصحة العامة والقانون الجنائي. وأخيرًا، سنضع الجريمة في إطار الجريمة المنظمة العابرة للحدود الوطنية، كاشفين عن بنيتها التحتية الإجرامية ودوافعها الاقتصادية، ومُبينين الحاجة إلى استراتيجية شاملة لمكافحة الجريمة تتجاوز الأساليب التقليدية.

٢,١,١. التوصيف الجنائي للجريمة في التشريعات الوطنية والمقارنة

إن استقراء الخارطة التشريعية العالمية يكشف عن حالة من التفتت والتنافر في التعامل مع جريمة غش الأدوية. هذا التباين لا يعكس مجرد اختلافات في الصياغة القانونية، بل يكشف عن تباين أعمق في الفلسفة الجنائية التي تحكم نظرة كل نظام قانوني إلى هذه الجريمة. يمكن من منظور تحليلي، تصنيف هذه المقاربات المتباينة إلى ثلاثة نماذج رئيسة؛ لكل منها انعكاساته المباشرة على فعالية النظام الجنائي في مواجهة هذا التهديد.

النموذج الأول: الاختزال في إطار جرائم الملكية الفكرية

تاريخياً، وفي العديد من الأنظمة القانونية، خاصة تلك التي تأثرت بالتقاليد التجارية، كان المدخل الأول للتعامل مع الأدوية المغشوشة هو من خلال قوانين حماية الملكية الفكرية، وتحديداً جرائم التعدي على العلامات التجارية وبراءات الاختراع. وفقاً لهذا النموذج، فإن جوهر الفعل الإجرامي ليس هو الخطر الصحي، بل هو الاستغلال غير المشروع لسمعة وشهرة علامة تجارية مملوكة للغير، أو تقليد منتج محمي ببراءة اختراع. (Glass, 2018)

من منظور القانون الجنائي، يعاني هذا النموذج من قصور بنيوي قاتل لعدة أسباب:

خطأ في تحديد المصلحة المحمية: إن حصر المصلحة المحمية في الحقوق التجارية لشركات الأدوية هو اختزال مخلّ، فهو يتجاهل المصلحة الأسمى والأولى بالحماية، وهي "الصحة العامة" و"الحق في الحياة والسلامة الجسدية" للمرضى. القانون الجنائي، في جوهره، هو قانون اجتماعي يهدف إلى حماية القيم الأساسية للمجتمع، وليس مجرد أداة لحماية المصالح الاقتصادية الخاصة (Attaran,

2012, as cited in Mackey & Liang, 2018). إن وضع الضرر الاقتصادي الذي يلحق بالشركة على قدم المساواة مع خطر الموت أو العجز الذي يهدد المريض هو تشويه لميزان العدالة الجنائية.

قصور في نطاق التجريم: هذا النموذج يترك فجوات تشريعية واسعة، فهو لا يوفر أي حماية للأدوية الجنيسية (generic drugs) التي لا تحمل علامة تجارية مشهورة أو التي انتهت مدة حماية براءة اختراعها. هذه الأدوية تشكل جزءاً كبيراً من السوق الدوائية، خاصة في الدول النامية، وهي هدف رئيس للمزورين. وبالتالي، فإن تصنيع دواء جنيس بمواد سامة قد لا يقع تحت طائلة التجريم وفقاً لهذا النموذج الضيق، لأنه لا يوجد "تعدٍ على علامة تجارية" بالمعنى الدقيق (Pisani, 2019).

صعوبات في الإثبات الجنائي: يتطلب إثبات جريمة التعدي على العلامة التجارية إثبات أن العلامة التجارية التي يستخدمها المتهم "متطابقة أو متشابهة جدًا بحيث لا تُسبب لبسًا". لا تُشدد جميع قضايا الأدوية المقلدة على "التشابه"، خاصةً في الحالات التي تُباع فيها المنتجات عبر الإنترنت بأسماء مختلفة أو "بدائل". والأهم من ذلك، يقع عبء الإثبات غالبًا على عاتق صاحب الحق، الذي قد يتردد في المشاركة في إجراءات جنائية معقدة ومكلفة. (Chaudhry & Stumpf, 2021)

عدم تناسب العقوبة مع الجرم: العقوبات المقررة لجرائم الملكية الفكرية، في معظم التشريعات، هي عقوبات يسيرة نسبياً (غرامات مالية أو حبس قصير المدة). هذه العقوبات تفتقر إلى الردع الكافي لشبكات إجرامية تحقق أرباحاً تقدر بمليارات الدولارات. إن اعتبار غش الأدوية مجرد "جنحة" ملكية فكرية يرسل إشارة خاطئة للمجرمين بأن هذا النشاط هو "جريمة منخفضة المخاطر، عالية الربح" (low-risk, high-reward crime) (Kazem-Goudarzi, 2022).

النموذج الثاني: الإدراج ضمن جرائم الغش التجاري والصحة العامة

يمثل هذا النموذج تطوراً عن سابقه، إذ ينقل التركيز من حماية المنتج إلى حماية المستهلك والمجتمع. في هذه الحالة، يتم تكييف الجريمة بوصفه شكلا من أشكال الغش في السلع بموجب قوانين حماية المستهلك، أو بوصفه جريمة ضد الصحة العامة بموجب قوانين تنظيم الأغذية والأدوية. هذا النموذج أفضل لأنه يعترف صراحة بالضرر الذي يلحق بالمستهلك والصحة العامة.

ومع ذلك، لا يزال هذا النموذج يواجه تحديات جوهرية من منظور جنائي:

التعميم وعدم التخصيص: إن إدراج جريمة غش الأدوية ضمن الإطار العام لجرائم "الغش التجاري" أو "جرائم حماية المستهلك" يؤدي إلى إشكالية "التعميم المخلّ". فهذا النهج يضع الدواء، وهو منتج ذو طبيعة فريدة وحساسة يرتبط ارتباطاً وجودياً بالحياة والصحة، في نفس المرتبة القانونية مع السلع الاستهلاكية العادية كالأجهزة الإلكترونية أو الملابس. هذا التعميم يفشل في إدراك أن الضرر المحتمل من الدواء المغشوش ليس مجرد خسارة مالية للمستهلك، بل هو تهديد مباشر وغير قابل للإصلاح للسلامة الجسدية والحق في الحياة. إن غياب توصيف جنائي متخصص لا يقلل فقط من الجسامة

الرمزية للجريمة في الوعي القانوني والاجتماعي، بل يضعف أيضاً الرسالة الردعية التي يهدف القانون الجنائي إلى إرسالها، مما يوحي بأن المجتمع لا يميز في الخطورة بين خداع المستهلك في سلعة كمالية وبين تعريضه لخطر الموت (Elliott, 2019).

تحديات الركن المعنوي: تتطلب العديد من جرائم الغش التجاري إثبات "قصد الخداع" لدى الجاني. بينما في جرائم غش الأدوية، قد يكون من الصعب إثبات أن نية المزور كانت خداع المريض تحديداً. فالدافع الأساس هو الربح المادي، وقد يكون المزور غير مبالٍ بالنتائج الصحية. من ناحية أخرى، في جرائم الصحة العامة، قد يتطلب القانون إثبات "القصد الجنائي المباشر" لإلحاق الضرر بالصحة، وهو أمر شبه مستحيل إثباته. إن الحاجة إلى تكييف مفاهيم القصد الجنائي التقليدية لتشمل "اللامبالاة" أو "الإهمال الجسيم" بوصفه شكلا من أشكال الركن المعنوي الكافي للإدانة تصبح ضرورية، وهو ما قد لا توفره النصوص العامة (Kharb, 2020).

إشكاليات السببية: إشكاليات السببية: في الحالات التي تؤدي فيها الأدوية المغشوشة إلى وفاة أو أذى جسيم، يواجه الادعاء العام تحدياً إثباتياً هائلاً في إقامة رابطة السببية بشكل يقيني لا يدع مجالاً للشك المعقول، وهو المعيار المطلوب في الإثبات الجنائي ،فالدفاع غالباً ما يثير دفوعاً قوية تتمحور حول انقطاع رابطة السببية، مجادلاً بأن النتيجة الضارة (الوفاة أو تدهور الحالة الصحية) لم تكن ناجمة مباشرة عن الدواء المغشوش، بل عن المرض الأساس الذي كان يعاني منه الضحية، أو عن تفاعل دوائي غير متوقع، أو عن عوامل أخرى متداخلة. هذا العبء الثقيل في إثبات أن الدواء المغشوش كان "السبب الجوهري والفعال" للضرر، وليس مجرد جزء من الخلفية الظرفية، قد يؤدي إلى إفلات الجناة من العقاب على الجرائم الأشد خطورة كالقتل أو الإيذاء الجسيم، والاكتفاء بإدانتهم بجريمة الغش أو التزييف اليسيرة، التي تحمل عقوبات أقل بكثير (Glass, 2018). إن هذه الصعوبة في ترجمة الضرر الصحي الفادح إلى إدانة جنائية متناسبة تمثل أحد أخطر أوجه القصور في الأنظمة التي لا تملك نصوصاً تجريمية خاصة ومستقلة لهذه الأفعال.

النموذج الثالث: التجريم المستقل والخاص

إدراكاً لأوجه القصور في النموذجين السابقين، اتجهت التشريعات الأكثر تقدماً والاتفاقيات الدولية الحديثة إلى تبني نموذج ثالث، وهو إنشاء جريمة مستقلة وخاصة لغش وتزييف المنتجات الطبية. هذا النموذج هو الأكثر فعالية من منظور السياسة الجنائية، لأنه يسمح للمشرّع بتصميم جريمة "مفصلة حسب المقاس" لتناسب أبعادها الفريدة.

تتمثل المزايا الجوهرية لهذا النموذج في:

الوضوح والدقة في التجريم: يسمح هذا النموذج بتجريم طيف واسع من الأفعال المرتبطة بالظاهرة الإجرامية، بدءاً من التصنيع المتعمد، والتوريد، والعرض، والاتجار، وصولاً إلى الأفعال المساعدة مثل

تزييف العبوات، وتزوير الوثائق، والإعلان والترويج عبر الإنترنت. هذا التحديد الدقيق للركن المادي يغلق الثغرات التي تتركها القوانين العامة (Riccardi, 2021).

التركيز على الخطر وليس الضرر: يمكن تعريف الجريمة بأنها كـ "جريمة خطر" بدلا من "جريمة ضرر". هذا يعني أن الفعل الإجرامي يقع بمجرد فور إنتاج الدواء المزيف أو تداوله ولا حاجة لإثبات الضرر الفعلي الذي لحق بمريض معين. هذا التحول في عبء الإثبات يخفف كثيرا من الصعوبات التي يواجهها الادعاء العام، ويُجسّد المفهوم الجنائي الحديث المتمثل في منع المخاطر قبل وقوعها.

فرض عقوبات رادعة: إن إنشاء جريمة مستقلة يسمح للمشرّع بفرض عقوبات صارمة تتناسب مع جسامة الفعل. يمكن أن تشمل هذه العقوبات السجن لمدد طويلة، وغرامات مالية ضخمة، ومصادرة العائدات الإجرامية. إن تصنيف الجريمة كـ "جناية" بدلاً من "جنحة" يمنح أجهزة إنفاذ القانون صلاحيات تحقيق أوسع، مثل التنصت والمراقبة، ويسهل التعاون الدولي وتسليم المجرمين (Gattinara et al., 2018).

إن المقارنة بين هذه النماذج الثلاثة تظهر بوضوح أن تبني نموذج التجريم المستقل (Sui Generis) ليس مجرد خيار تشريعي، بل هو ضرورة حتمية لبناء نظام عدالة جنائية قادر على حماية الحق في الحياة والصحة العامة من هذا التهديد القاتل.

٢,١,٢. الجريمة في ضوء الاتفاقيات الدولية (اتفاقية ميديكرايم نموذجاً) (The MEDICRIME Convention as a Model)

قبل ظهور اتفاقية ميديكرايم، كان المشهد القانوني الدولي يعاني من فراغ معاهداتي صارخ فيما يتعلق بتجريم غش الأدوية. الأدوات القانونية الدولية القائمة لم تكن مصممة للتعامل مع هذه الظاهرة بشكل مباشر وفعال. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (UNTOC) لعام ٢٠٠٠، على الرغم من أهميتها، لم تدرج غش الأدوية ضمن قائمة الجرائم التي تغطيها بشكل صريح. أما اتفاقية منظمة التجارة العالمية بشأن الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (TRIPS)، فقد حصرت نفسها، كما يوحي اسمها، في إطار الملكية الفكرية، مع التركيز على الإنفاذ المدني والإداري، ولم تفرض التزامات جنائية واضحة تتجاوز القرصنة التجارية المتعمدة (Delepierre, 2019).

في هذا السياق، جاءت اتفاقية مجلس أوروبا بشأن تزييف المنتجات الطبية والجرائم المماثلة التي تنطوي على تهديدات للصحة العامة (CETS No. 211)، المعروفة باتفاقية ميديكرايم، التي اعتمدت في عام ٢٠١١، لتحدث ثورة مفاهيمية وقانونية. هذه الاتفاقية، المفتوحة للتوقيع من قبل الدول غير الأعضاء في مجلس أوروبا، تمثل أول صك قانوني دولي ملزم مكرس بالكامل لمكافحة هذه الجريمة من منظور القانون الجنائي والصحة العامة.

الأهمية الجوهرية لاتفاقية ميديكرايم من منظور جنائي:

إعادة تعريف المصلحة المحمية على المستوى الدولي: الإنجاز الأبرز للاتفاقية هو أنها نقلت النقاش الدولي بشكل حاسم من "حماية الملكية الفكرية" إلى "حماية الصحة العامة". ديباجة الاتفاقية والمادة الأولى منها تؤكدان صراحة أن الهدف هو حماية الصحة العامة من خلال تجريم هذه الأفعال. هذا التحول الفلسفي له آثار قانونية عميقة، فهو يبرر فرض عقوبات جنائية صارمة ويضع حقوق الضحايا (المرضى) في صميم الاستجابة القانونية (Gattinara et al., 2018).

تحديد دقيق للأفعال واجبة التجريم: تفرض الاتفاقية على الدول الأطراف التزامات واضحة ومحددة بتجريم مجموعة من الأفعال الجوهرية في قانونها الوطني. هذا الالتزام بالتجريم الإلزامي لا يمثل مجرد توصية، بل هو أداة قانونية تهدف إلى تحقيق قدر من التنسيق والتوحيد التشريعي بين الأنظمة القانونية الوطنية المختلفة. فمن خلال فرض تعريفات مشتركة للأفعال الإجرامية، تسعى الاتفاقية إلى تقليص الثغرات والفجوات القانونية التي تستغلها الشبكات الإجرامية للانتقال بين الولايات القضائية ذات الأنظمة العقابية المتساهلة. إن هذا التنسيق التشريعي يُعد شرطاً مسبقاً لا غنى عنه لضمان فعالية التعاون الدولي، إذ يضمن أن الفعل المجرم في دولة ما هو مجرم أيضاً في دولة أخرى، مما يسهل عمليات تسليم المجرمين والمساعدة القانونية المتبادلة (Vian, 2020). تشمل هذه الأفعال:

المادة ٥ (تصنيع المنتجات المزيفة): تجرم "التصنيع العمدي" للمنتجات الطبية المزيفة، والأجهزة الطبية، والمواد الفعالة، والمكونات الأخرى.

المادة ٦ (التوريد والاتجار): تجرم "التوريد العمدي، أو عرض التوريد، أو الاتجار" بالمنتجات المزيفة.

المادة ٧ (تزييف الوثائق): تجرم "تزييف الوثائق" المرتبطة بالمنتجات الطبية، مثل شهادات المنشأ أو وثائق التتبع.

المادة ٨ (الجرائم المماثلة): توسع نطاق التجريم ليشمل التصنيع والتوريد العمدي للمنتجات الطبية دون ترخيص أو بما يخالف معايير السلامة.

هذا التحديد الدقيق للركن المادي لكل جريمة يوفر أساساً قانونياً صلباً للملاحقات القضائية.

تعريف شامل لمفهوم "التزييف: تقدم المادة ٤(f) من الاتفاقية تعريفاً شاملاً للتزييف بأنه "التمثيل الخادع فيما يتعلق بالهوية و/ أو المصدر". هذا التعريف واسع ومدروس بعناية. فهو لا يقتصر على انتهاك حقوق الملكية الفكرية، بل يشمل أي تضليل يتعلق بماهية المنتج أو منشئه. هذا يعني أن الدواء يعد مزيفاً حتى لو لم يكن محمياً ببراءة اختراع، طالما تم تضليل المستهلك بشأن مصدره الموثوق أو مكوناته الحقيقية. هذا التعريف يغطي الأدوية الجنيسة، والأدوية المسروقة، والأدوية منتهية الصلاحية التي يعاد تغليفها، مما يغلق العديد من الثغرات القانونية (Council of Europe, 2011).

تحديد المسؤولية الجنائية للشخص المعنوي: في خطوة مهمة، تُعدّ المادة ١٢ خطوةً مهمةً في إلزام الدول الأطراف بضمان محاسبة الأشخاص الاعتباريين (مثل الشركات) على الجرائم المنصوص عليها في الاتفاقية، التي يرتكبها نيابةً عنهم أشخاص طبيعيون يتصرفون بصفتهم القيادية. كما تُشترط المادة أن تكون العقوبات المفروضة على الأشخاص الاعتباريين "فعالة ومتناسبة ورادعة"، وقد تشمل غرامات جنائية أو غير جنائية، أو حتى تدابير مثل وضعهم تحت الإشراف القضائي أو إغلاقهم. (Fitriana & Adijaya, 2022) يُعدّ هذا البند بالغ الأهمية لمقاضاة الشركات المتورطة في هذه التجارة غير المشروعة.

إطار متكامل للتعاون الدولي: إدراكاً لحقيقة أن الشبكات الإجرامية تستغل ببراعة الثغرات والفجوات في التعاون بين الأنظمة القضائية المختلفة، تخصص اتفاقية ميديكرايم فصلاً كاملاً (الفصل الخامس) لتأسيس بنية قانونية متينة للتعاون الدولي. تتجاوز أحكام هذا الفصل مجرد التشجيع على التعاون، لتؤسس لآليات إجرائية محددة تهدف إلى تسهيل وتسريع المساعدة القانونية المتبادلة، وتسليم المجرمين، وإجراء التحقيقات المشتركة، وتبادل المعلومات بشكل استباقي وفعال. إن الهدف الجوهري هو خلق لغة إجرائية مشتركة بين أجهزة إنفاذ القانون في الدول الأطراف، مما يقلل من العقبات البيروقراطية والقانونية التي تعوق تقليدياً الملاحقات العابرة للحدود. فوجود هذا الإطار التعاهدي المشترك يمنع المجرمين من إيجاد ملاذات آمنة ويضمن عدم انتهاء الملاحقة القضائية بمجرد عبور الجاني أو الأدلة للحدود الوطنية (Mackey & Cuomo, 2021).

على الرغم من هذه المزايا الجوهرية، فإن فعالية اتفاقية ميديكرايم لا تزال تواجه تحديات. فعملية التصديق عليها، خاصة من قبل دول خارج أوروبا تعد من المراكز الرئيسة لتصنيع أو عبور الأدوية المغشوشة، لا تزال بطيئة. كما أن التنفيذ الفعلي لأحكامها يتطلب تعديلات تشريعية كبيرة وبناء قدرات فنية وقانونية لدى أجهزة الشرطة والجمارك والقضاء في الدول الأطراف (Margaron, 2020). ومع ذلك، تظل الاتفاقية المعيار الذهبي والبوصلة التي توجه الجهود الدولية نحو استجابة جنائية متماسكة وفعالة.

٢,١,٣. خصائص الجريمة كجريمة منظمة عابرة للحدود

إن الفهم الكامل للطبيعة القانونية لجريمة غش الأدوية لا يكتمل دون تحليل بنيتها التحتية الإجرامية. فهذه الجريمة، في الغالبية العظمى من الحالات، ليست نتاج أفعال فردية معزولة، بل هي نشاط اقتصادي مربح تديره شبكات إجرامية منظمة ومتطورة. إن تطبيق إطار التحليل الذي توفره المادة ٢(a) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (UNTOC)) يكشف بوضوح عن توافر جميع أركان الجريمة المنظمة في هذه الظاهرة.

أولاً، الهيكل التنظيمي المتطور:

تعرف اتفاقية UNTOC "الجماعة الإجرامية المنظمة" بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، قائمة لفترة من الزمن، وتعمل بهدف ارتكاب جريمة خطيرة. تتجاوز شبكات غش

الأدوية هذا التعريف بكثير، حيث تعمل بوصفها نماذج أعمال إجرامية معقدة تشبه الشركات المشروعة. فهي تتميز بـ:

تقسيم العمل والتخصص: يوجد داخل الشبكة أدوار متخصصة: خبراء كيميائيون لتصنيع المواد الفعالة الزائفة، وعمال لتشغيل آلات الضغط والتغليف، ومصممو جرافيك لتقليد العبوات والشعارات بدقة، ومسؤولون لوجستيون لإدارة عمليات الشحن والتخزين، ومسوقون عبر الإنترنت لإدارة الصيدليات الإلكترونية غير المشروعة، ومختصون في غسيل الأموال لإخفاء العائدات الإجرامية (Brophy et al., 2021).

المرونة والقدرة على التكيف: تتجاوز هذه الشبكات النموذج الهرمي التقليدي للجريمة المنظمة، لتتبنى هياكل قائمة على الشبكات تتميز بالسيولة التنظيمية. فهي تتكون من عُقد لا مركزية أو خلايا شبه مستقلة، تتصل ببعضها البعض لأداء مهام محددة (مثل التصنيع أو التوزيع) ثم قد تنفصل أو يعاد تشكيلها. هذه المرونة ليست عَرَضية، بل هي استراتيجية متعمدة لزيادة الصمود في وجه عمليات إنفاذ القانون؛ فهي تسمح للشبكة بامتصاص الصدمات الناتجة عن القبض على بعض أعضائها دون أن ينهار الهيكل بأكمله، كما تمكنها من التكيف السريع مع التغيرات في بيئة العمل الإجرامي، كتغيير طرق التهريب أو نقل مواقع التصنيع بسهولة عند اكتشافها، مما يجعل استهدافها بأساليب التحقيق التقليدية التي تركز على "رأس" التنظيم أمراً بالغ الصعوبة (Spink et al., 2019).

استخدام التكنولوجيا: تستغل هذه الشبكات التكنولوجيا بشكل مكثف، ليس فقط في التصنيع، بل أيضاً في التواصل المشفر، واستخدام العملات الرقمية لإخفاء المعاملات المالية، وإنشاء واجهات رقمية متطورة على الإنترنت العادي والإنترنت المظلم للوصول إلى قاعدة عملاء عالمية (Felbab-Brown, 2021).

ثانياً، الدافع المالي والربحية الاستثنائية:

الهدف الأساس لهذه الشبكات، كما تنص اتفاقية UNTOC، هو الحصول على منفعة مالية. وتعد تجارة الأدوية المغشوشة واحدة من أكثر الأنشطة الإجرامية ربحية في العالم. هوامش الربح فيها تفوق بكثير تلك الموجودة في تجارة المخدرات. فتكلفة إنتاج قرص دواء مزيف قد لا تتجاوز بضعة سنتات (باستخدام مواد رخيصة مثل الطباشير أو غبار الطوب)، بينما يباع بسعر يقارب سعر الدواء الأصلي. هذه الربحية الفلكية، مقترنة بتصور (صحيح في كثير من الأحيان) بأن العقوبات أقل صرامة ومخاطر الكشف أقل، تجعلها مجالاً استثمارياً جذاباً للغاية للجماعات الإجرامية التي تسعى إلى تنويع مصادر دخلها (Alghasham, 2022).

ثالثاً، الطابع العابر للحدود:

تكتسب الجريمة طابعاً عابراً للحدود وفقاً للمادة ٣(٢) من اتفاقية UNTOC إذا ارتكبت في أكثر من دولة، أو إذا كان جزء كبير من التحضير لها أو تخطيطها أو توجيهها أو الإشراف عليها يتم في دولة أخرى. وهذا هو الوضع النموذجي في جريمة غش الأدوية. فالسلسلة الإجرامية مجزأة جغرافياً بشكل متعمد:

– المصادر: قد يتم استيراد المواد الكيميائية الأولية من دولة (مثل الصين أو الهند).

– التصنيع: قد يتم تصنيع المنتج النهائي في مختبر سري في دولة أخرى.

– التعبئة والتغليف: قد يتم شحن الأقراص السائبة إلى دولة ثالثة حيث توجد آلات متطورة لطباعة العبوات والنشرات المزيفة.

– التوزيع: يتم شحن المنتج النهائي عبر شبكة معقدة من الموانئ والمطارات في دول عبور متعددة لإخفاء بلد المنشأ الحقيقي.

– البيع: يتم بيعها للمستهلكين في أسواق الوجهة النهائية في جميع أنحاء العالم.

هذا التفتيت الجغرافي المتعمد ليس عشوائياً، بل هو استراتيجية إجرامية تهدف إلى استغلال الاختلافات في التشريعات، وضعف الرقابة الحدودية، وصعوبات التعاون القضائي الدولي. إنه يخلق تحديات هائلة تتعلق بالأنظمة القضائية، وجمع الأدلة عبر الحدود، وتحديد هوية الجناة الرئيسيين الذين يديرون العملية عن بعد (Mackey et al., 2020).

ولذا يرى الباحث أن إدراك هذه الخصائص الثلاث – التنظيم المعقد، والربحية الفائقة، والطابع العابر للحدود – يؤكد أن أي استجابة جنائية فعالة يجب أن تكون بنفس القدر من التطور والشمول والتنسيق الدولي. فمواجهة شبكة عالمية لا يمكن أن تتم إلا من خلال شبكة عالمية من التعاون بين أجهزة إنفاذ القانون، وهو ما يمهد الطريق لفهم لماذا يمكن لتقنية عالمية ولامركزية مثل البلوك تشين أن تلعب دوراً محورياً في هذه المواجهة.

٢,٢. ماهية تقنية البلوك تشين وآلية عملها في سلاسل الإمداد الدوائية

بناءً على ما سبق من تفكيك للبنية القانونية لجريمة غش الأدوية، يتجه التركيز في هذا الجزء نحو استكشاف الحل التكنولوجي الذي يقع في صميم هذه الدراسة: تقنية البلوك تشين. إن الانتقال من تحليل "المشكلة" إلى تحليل "الحل" المقترح يقتضي حذراً منهجياً؛ فلا يمكن تبني أي تقنية، مهما بدت واعدة، دون إخضاعها لفحص قانوني دقيق. إن الهدف من هذا القسم الفرعي ليس تقديم شرح تقني ميسر، بل إجراء تشريح قانوني لآلية عمل البلوك تشين، مع التركيز على الخصائص التي تتقاطع مباشرة مع مفاهيم القانون الجنائي الموضوعي والإجرائي.

يتناول هذا القسم الفرعي الثاني بناء جسر معرفي بين عالم التشفير والعدالة الجنائية، وذلك عبر ثلاث خطوات مترابطة: تتمثل الخطوة الأولى في تجريد المبادئ التقنية. أما الخطوة الثانية، فتنقل النقاش من التنظير إلى التطبيق، بينما تعالج الخطوة الثالثة والأخيرة 'العقود الذكية.

٢,٢,١. المبادئ التقنية الأساسية وتداعياتها على القانون الجنائي

إن القيمة الحقيقية لتقنية البلوك تشين في سياق مكافحة الجريمة لا تكمن في كونها مجرد قاعدة بيانات متطورة، بل في مجموعة من المبادئ المعمارية التي تتحدى بشكل مباشر الافتراضات التي بنيت عليها الأنظمة القانونية التقليدية. إن فهم هذه المبادئ ليس ترفاً تقنياً، بل هو شرط أساس لتقييم مدى قدرة القانون الجنائي على استيعاب هذه التقنية والتفاعل معها.

أولاً: اللامركزية من نقطة الضعف الوحيدة إلى تحدي الأنظمة القضائية

في الأنظمة التقليدية، يتم تخزين البيانات في خوادم مركزية تملكها وتديرها جهة واحدة (بنك، شركة، حكومة). من منظور جنائي، يمثل هذا الهيكل "نقطة ضعف وحيدة" ونقطة هجوم رئيسة للمجرمين، ولكنه في الوقت نفسه يمثل "نقطة إنفاذ وحيدة" للسلطات. فيمكن للنيابة العامة أو المحكمة إصدار أمر قضائي لهذه الجهة المركزية لتسليم البيانات أو حجبها.

تقنية البلوك تشين تقلب هذا النموذج رأساً على عقب. فهي تعتمد على "سجل الأستاذ الموزع" (Distributed Ledger Technology - DLT)، إذ يتم نسخ السجل بالكامل وتوزيعه على عدد كبير من المشاركين في الشبكة (يطلق عليهم "العُقد" أو Nodes)، دون وجود خادم مركزي. (Zyskind et al., 2015)

هذا التصميم المعماري له تداعيات قانونية جنائية عميقة:

تقويض مفهوم الحيازة والسيطرة: في القانون الجنائي الإجرائي، ترتبط أوامر التفتيش والضبط بمفهوم "الحيازة" أو "السيطرة" على البيانات. في شبكة البلوك تشين، من هو "الحائز" الفعلي للبيانات؟ هل هي كل عقدة تملك نسخة من السجل؟ أم لا أحد يملكها بشكل حصري؟ إن غياب جهة مركزية مسيطرة يخلق فراغاً مفاهيمياً، فلا يوجد طرف واحد يمكن مخاطبته بأمر قضائي لتسليم "السجل الأصلي"، لأن كل النسخ متطابقة من حيث المبدأ. (Werbach, 2018)

تفاقم إشكالية الولاية القضائية: إذا كانت عُقد الشبكة موزعة عبر عشرات الدول، فأي دولة تملك الاختصاص القضائي للتحقيق في جريمة تم كشفها عبر هذه الشبكة؟ هل هي دولة الضحية؟ أم دولة الجاني؟ أم كل دولة يوجد على أراضيها عقدة من عقد الشبكة؟ هذا التشتت الجغرافي المتعمد يمثل تحدياً خطيراً لمبدأ "الإقليمية" الذي يشكل أساس الاختصاص الجنائي في معظم النظم القانونية. قد يؤدي ذلك إلى نزاعات إيجابية أو سلبية في الاختصاص، أو إلى سباق نحو الملاحقة بين الدول المختلفة (Finck, 2018).

إعادة تعريف المساهمة الإجرامية: في بيئة لامركزية، يصبح تحديد المسؤولية الجنائية معقدًا. هل يُمكن اعتبار مشغلي العُقد (أو المُعدّنين) الذين يُصادقون على المعاملات ويضيفونها إلى سجل الحسابات "شركاء" في الجرائم التي تُسهّلها الشبكة، حتى لو لم يفهموا محتوى المعاملات؟ يُثير هذا تساؤلات حول مدى قابلية تطبيق النظريات التقليدية للمساهمة الإجرامية، ويستلزم مناقشة مدى ضرورة إثبات "النية الإجرامية" لهذه الجهات الفاعلة الموزعة؟ (Hess & Broring, 2021)

ثانياً: التشفير: من ضمان الأصالة والسلامة إلى إشكالية الخصوصية

يعتمد أمن البلوك تشين بشكل أساس على تقنيات التشفير المتقدمة، وتحديداً "التشفير غير المتماثل" (asymmetric cryptography) الذي يستخدم زوجاً من المفاتيح (مفتاح عام ومفتاح خاص) و"دوال التجزئة" (hash functions).

المفاتيح العامة والخاصة: كل مستخدم لديه مفتاح خاص يحتفظ به سراً، ومفتاح عام يشاركه مع الآخرين. المفتاح الخاص يستخدم للتوقيع الرقمي على المعاملات، لإثبات أن المستخدم هو من قام بها. المفتاح العام يستخدم للتحقق من صحة هذا التوقيع.

دوال التجزئة: هي خوارزميات تحول أي حجم من البيانات إلى سلسلة نصية ذات طول ثابت وفريدة من نوعها (تسمى "الهاش" أو "البصمة الرقمية"). أي تغيير طفيف في البيانات الأصلية، ولو حرف واحد، ينتج عنه "هاش" مختلف تماماً.

من منظور القانون الجنائي، لهذه الأدوات التشفيرية آثار مزدوجة:

تعزيز القيمة الثبوتية للدليل الرقمي: التوقيع الرقمي باستخدام المفتاح الخاص يوفر دليلاً قوياً على "أصالة" المعاملة ونسبتها إلى شخص معين (أو بالأحرى، إلى حائز المفتاح الخاص). كما أن ربط الكتل ببعضها البعض باستخدام "الهاش" يضمن "سلامة" السجل بأكمله. هذان العنصران (الأصالة والسلامة) هما من أهم الشروط لقبول الدليل الرقمي في المحاكمات الجنائية. يمكن للادعاء العام أن يجادل بأن السجل المحمي بهذه الطريقة يتمتع بدرجة عالية من الحجية تفوق السجلات الورقية أو الرقمية المركزية القابلة للتلاعب (Savelyev, 2018).

تحدي الخصوصية مقابل حق الدولة في التحقيق: على الرغم من أن معاملات البلوك تشين العامة (مثل بيتكوين) شفافة، فإنها غالباً ما تكون "مجهولة الهوية اسمياً"؛ أي أن المعاملات مرتبطة بعنوان مشفر (المفتاح العام) وليس بهوية حقيقية، هذا يخلق توازناً دقيقاً؛ فبينما يمكن لأجهزة إنفاذ القانون تتبع تدفق المعاملات على السلسلة، فإن ربط العنوان المشفر بهوية شخص حقيقي يتطلب إجراءات تحقيق إضافية، مثل تتبع نقاط الدخول والخروج من النظام (مثل منصات تبادل العملات). هذا يثير تساؤلات حول مدى حق الأفراد في الخصوصية في معاملاتهم المالية الرقمية، مقابل سلطة الدولة في الكشف عن هوية المشتبه بهم في جرائم خطيرة. (Narayanan et al., 2020)

ثالثاً: الثبات- من الدليل القاطع إلى معضلة "البيانات الخاطئة"

خاصية "الثبات" أو "عدم القابلية للتغيير" هي من أكثر خصائص البلوك تشين جاذبية من منظور قانوني. فبمجرد إضافة كتلة (مجموعة من المعاملات) إلى السلسلة والتحقق منها، يصبح من المستحيل عملياً تغييرها أو حذفها دون تغيير جميع الكتل اللاحقة، وهو أمر تكتشفه الشبكة وترفضه فوراً. هذا يخلق سجلاً تاريخياً دائماً ومقاوماً للتلاعب.

التداعيات الجنائية لهذه الخاصية هائلة:

إنشاء "دليل غير قابل للإنكار": خاصية الثبات تعني أن المتهم لا يمكنه إنكار قيامه بمعاملة تم تسجيلها وتوقيعها بمفتاحه الخاص. هذا يقوض الدفوع التقليدية المتعلقة بتزوير السجلات أو تغييرها لاحقاً. يمكن للادعاء أن يقدم سجل البلوك تشين دليلاً يتمتع بقرينة صحة قوية، ناقلاً عبء إثبات العكس إلى الدفاع. (Yeoh, 2021)

معضلة "البيانات الخاطئة" أو "مشكلة الأوراكل": إن البلوك تشين تضمن ثبات البيانات بعد إدخالها، لكنها لا تضمن صحة هذه البيانات قبل إدخالها. إذا أدخل شخص ما ، عن قصد أو غير قصد، معلومات زائفة في السلسلة على سبيل المثال: تسجيل دواء أصلي على أنه مزيف، أو العكس)، فستصبح هذه المعلومات الزائفة جزءًا ثابتًا ودائمًا من السجل. من منظور الطب الشرعي، تُسمى هذه المشكلة "البيانات غير الصحيحة الواردة، البيانات غير الصحيحة الصادرة"، مما يعني أن سجلات سلسلة الكتل ليست صحيحة تمامًا، بل هي انعكاس لما قرر المشاركون تسجيله. لذلك، لا يمكن أن تقتصر التحقيقات الجنائية على مراجعة سلسلة البيانات، بل يجب أن تمتد أيضًا إلى التحقق من ظروف وآليات إدخال البيانات في سلسلة البيانات (أي ما يُسمى "أوراكل" أو "مصدر البيانات الموثوق به"). (Casey et al., 2019)

التعارض مع الحقوق القانونية الأخرى: قد يتعارض مبدأ الثبات المطلق مع الحقوق القانونية الراسخة، مثل "الحق في النسيان" المنصوص عليه في لوائح حماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR)، أو الحق في تصحيح البيانات غير الدقيقة. في سياق جنائي، قد يجادل الدفاع بأن عدم القدرة على تصحيح خطأ في السجل ينتهك حق المتهم في محاكمة عادلة. وهذا يُنشئ تعارضًا بين الحاجة إلى أدلة متسقة وموثوقة، والحاجة إلى المرونة في تصحيح الأخطاء وحماية الحقوق الفردية.

رابعاً: آلية الإجماع – من الثقة الموزعة إلى تحدي "شاهد الإثبات"

في غياب سلطة مركزية، كيف تتفق الشبكة على المعاملات التي يجب إضافتها إلى السجل؟ يتم ذلك من خلال "آلية إجماع"، وهي مجموعة من القواعد التي تتبعها العُقد للتحقق من صحة المعاملات والاتفاق على نسخة واحدة من "الحقيقة". أشهر هذه الآليات هي "إثبات العمل"، إذ تتنافس العُقد لحل لغز حسابي معقد، و"إثبات الحصة" (Proof-of-Stake)، فيتم اختيار المدققين بناءً على كمية العملة التي يملكونها.

من منظور قانوني جنائي، تثير آلية الإجماع تساؤلات حول طبيعة ومصدر " حُجِّيَّة " السجل:

طبيعة السجل بوصفه دليل إثبات: هل يمكن اعتبار السجل الذي تم التحقق منه بواسطة شبكة من المشاركين المجهولين "سجلاً تجارياً" بالمعنى التقليدي، والذي يتمتع عادةً بقبول أوسع في المحاكم؟ أم هو نوع جديد من الأدلة يتطلب قواعد إثبات خاصة؟ في أنظمة القانون العام، قد يواجه السجل تحدياً بموجب "قاعدة منع الإشاعة"؛ لأن كل إدخال في السجل هو "إفادة خارج المحكمة" يتم تقديمها لإثبات حقيقة محتواها. من هو "الشاهد" الذي يمكن استجوابه حول صحة هذه الإفادة؟ هل هم جميع مشغلي العُقد المجهولين؟ (Grigg, 2020).

تأسيس الحجية أمام القضاء: لكي يتم قبول سجل البلوك تشين دليلا، سيتعين على الادعاء العام أن يقدم "شاهداً خبيراً" يشرح للمحكمة كيف تعمل التقنية، وكيف تضمن آلية الإجماع المحددة سلامة وحجية البيانات. سيتعين على القضاة والمحامين تطوير فهم عميق لهذه الآليات لتقييم القيمة الثبوتية للدليل المقدم، والموازنة بينها وبين أي تحيزات أو مخاطر محتملة (Bambara & Schartum, 2021).

إن هذا التحليل للمبادئ الأساسية يوضح أن البلوك تشين ليست مجرد أداة، بل هي بيئة قانونية جديدة تتحدى المفاهيم الجنائية الراسخة وتجبرنا على إعادة التفكير في كيفية تعريفنا للسيطرة، والولاية القضائية، والمسؤولية، والدليل في العصر الرقمي اللامركزي.

٢,١,٢. تطبيق البلوك تشين على سلسلة التوريد الدوائية (Track and Trace)

بعد استعراض المبادئ النظرية، ننتقل الآن إلى التطبيق العملي الأكثر أهمية في سياق هذا البحث: استخدام البلوك تشين لإنشاء نظام تتبع وتعقب (Track and Trace) لسلاسل الإمداد الدوائية. إن الهدف من هذه الأنظمة هو خلق "سيرة ذاتية رقمية" لكل علبة دواء، تكون موثوقة، وشفافة، ومقاومة للتلاعب، منذ لحظة خروجها من المصنع وحتى وصولها إلى يد المريض.

آلية العمل: من "التوأم المادي" إلى "التوأم الرقمي"

تعمل أنظمة التتبع القائمة على البلوك تشين من خلال ربط كل منتج مادي بـ "توأم رقمي" فريد على السلسلة. تتم العملية عبر الخطوات التالية:

الترميز: عند نقطة التصنيع، يتم إعطاء كل علبة دواء أو دفعة إنتاج هوية رقمية فريدة. يمكن أن تكون هذه الهوية على شكل رقم تسلسلي، أو رمز استجابة سريعة (QR code)، أو علامة اتصال قريب المدى (NFC tag). هذه الهوية الفريدة هي التي سيتم تسجيلها على البلوك تشين كـ "أصل رقمي" أو "توكن" (token).. (Mettler, 2016)

تسجيل المعاملات: عند كل نقطة حيوية في سلسلة التوريد (التصنيع، الشحن، التخزين، التوزيع، الجمارك، الصيدلية)، يقوم الطرف المسؤول بمسح الهوية الرقمية للعلبة وتسجيل معاملة جديدة على البلوك تشين. على سبيل المثال: (Kamble et al., 2020)

- المصنع: يسجل معاملة "إنشاء" (للعلبة رقم. ABC
- شركة الشحن: تسجل معاملة "نقل ملكية" للعلبة ABC من المصنع إليها.
- الصيدلية: تسجل معاملة "استلام" للعلبة. ABC

إنشاء سجل غير قابل للتغيير: كل معاملة من هذه المعاملات يتم تجميعها في كتلة، وتشفيرها، وربطها بالكتلة السابقة، وتوزيعها على جميع المشاركين في الشبكة. والنتيجة هي سجل تاريخي كامل ومفصل ومختوم بالوقت لرحلة علبة الدواء، لا يمكن لأي طرف تغييره أو حذفه بأثر رجعي. (Hasan et al., 2019)

الآثار من منظور القانون الجنائي: من الردع اللاحق إلى المنع الاستباقي

إن تطبيق آلية التتبع القائمة على البلوك تشين له آثار تحويلية تتجاوز مجرد تسهيل التحقيق بعد وقوع الجريمة، لتؤسس لنموذج استباقي يهدف إلى منعها قبل وقوعها. هذا التحول من الردع اللاحق إلى المنع المدمج في التصميم يمكن تحليله من خلال منظورين رئيسين في السياسة الجنائية.

أولاً: المنع الجنائي الظرفي

يعمل هذا النظام رادعًا بنيويًا، ليس فقط من خلال التهديد بالعقاب، بل من خلال إعادة هندسة البيئة الظرفية للجريمة، وهو ما يقع في صميم نظرية المنع الجنائي الظرفي. هذه النظرية، التي ترتكز على فرضية "الاختيار العقلاني"، تفترض أن الجريمة هي نتاج فرصة سانحة، ويمكن منعها من خلال التلاعب المنهجي بالبيئة لجعل الخيارات الإجرامية تبدو أقل جاذبية للمجرم المحتمل (Reyns, 2021).

يطبق نظام البلوك تشين هذا المبدأ بشكل فعال من خلال ثلاث آليات رئيسة:

١ ـ زيادة الجهد المطلوب لارتكاب الجريمة:

تخلق البنية التحتية للبلوك تشين عقبات تشغيلية وتقنية هائلة أمام المزورين. فبدلاً من مجرد اختراق قاعدة بيانات مركزية واحدة، يجب على المجرم الآن أن يتغلب على نظام موزع ومحمي بالتشفير. إن إدخال منتج مزيف إلى سلسلة التوريد المشروعة يتطلب إما كسر التشفير القوي للسلسلة، أو التواطؤ مع عدد كبير من المشاركين، أو إنشاء هوية رقمية مزيفة يمكنها خداع النظام. كل هذه الخيارات تتطلب جهداً وموارد وخبرة فنية تفوق بكثير ما تتطلبه الأساليب التقليدية، مما يرفع "تكلفة" ارتكاب الجريمة بشكل كبير.

٢ ـ زيادة مخاطر الكشف:

لعل هذا هو الأثر الأقوى للبلوك تشين. فالشفافية والثبات تخلقان مسار تدقيق رقمي شبه كامل. كل معاملة، وكل عملية نقل حيازة، وكل تغيير في الحالة يتم تسجيله بشكل دائم وربطه بهوية رقمية لطرف

معين. هذا يعني أن أي محاولة لإدخال منتج غير شرعي أو التلاعب ببيانات منتج شرعي ستترك "بصمة رقمية" لا يمكن محوها. هذا يزيد بشكل كبير من "اليقين العقابي"، وهو العامل الأكثر تأثيراً في الردع. فالجاني المحتمل يدرك أن أفعاله ستكون مرئية وقابلة للتتبع، وأن احتمالية كشفه والتعرف عليه تقترب من اليقين، مما يجعل المخاطرة غير مقبولة. (Casino et al., 2019)

٣ ـ تقليل المكافآت المتوقعة.

الدافع الأساس لجريمة غش الأدوية هو الربح المادي الهائل، الذي ينشأ من القدرة على بيع منتج منخفض التكلفة بسعر يقارب سعر المنتج الأصلي. يعمل نظام البلوك تشين على تقويض هذا النموذج الاقتصادي الإجرامي بشكل مباشر. فعندما يصبح من المستحيل عملياً إدخال الأدوية المزيفة إلى سلسلة التوريد المشروعة وبيعها للمستهلكين عبر القنوات الرسمية (مثل الصيدليات والمستشفيات)، فإن قدرة المزورين على تحقيق أسعار مرتفعة تنهار. سيضطرون إلى محاولة بيع منتجاتهم في الأسواق السوداء الهامشية أو عبر الإنترنت المظلم، حيث يكون المشترون أكثر حذراً والأسعار أقل بكثير. هذا يؤدي إلى تآكل هوامش الربح بشكل كبير، مما يجعل النشاط الإجرامي بأكمله أقل جدوى من الناحية الاقتصادية ويقلل من جاذبيته كـ "استثمار" للجريمة المنظمة. (Astill et al., 2019).

إعادة تعريف "سلسلة حيازة الدليل": في التحقيقات الجنائية، تعتبر "سلسلة الحيازة" أي السجل الموثق الذي يوضح من تعامل مع الدليل ومتى وأين – أمراً حيوياً لضمان قبول الدليل في المحكمة. غالباً ما تكون سلاسل الحيازة التقليدية ورقية وعرضة للخطأ البشري والتلاعب.

يقدم البلوك تشين "سلسلة حيازة رقمية" آلية وموثوقة. فالسجل على السلسلة هو في جوهره سجل لحيازة الدواء عبر الزمن. يمكن للمحققين استخدامه لتحديد النقطة الدقيقة في سلسلة التوريد التي حدث فيها الخلل (على سبيل المثال، النقطة التي اختفى فيها الدواء الأصلي وظهر فيها الدواء المزيف). هذا يوفر دليلاً قوياً ومباشراً يمكن تقديمه للمحكمة، مما يسهل بشكل كبير عبء الإثبات على الادعاء العام. (Kshetri, 2018)

تحديد المسؤولية بشكل دقيق: في سلاسل التوريد التقليدية المعقدة، قد يكون من الصعب تحديد الطرف المسؤول عن دخول منتج مزيف. أما في نظام البلوك تشين، فإن كل طرف يسجل معاملاته بتوقيعه الرقمي. هذا يخلق مساراً للمساءلة لا يمكن إنكاره. إذا قبل موزع شحنة دون التحقق من هويتها الرقمية على السلسلة، أو إذا سجل معلومات خاطئة، فإن مسؤوليته عن هذا الإهمال أو الفعل العمدي تكون موثقة بشكل واضح، مما يسهل إثبات "الركن المادي" ويسهم في إثبات "الركن المعنوي" للجريمة (Abou-Nassar et al., 2020).

٢,٢,٣. دور العقود الذكية في أتمتة الرقابة والتحقق

إذا كانت البلوك تشين هي السجل الموثوق الذي يوفر "الذاكرة" غير القابلة للتغيير، فإن "العقود الذكية" هي المحرك الذي يوفر "المنطق" القابل للتنفيذ تلقائياً على هذا السجل. من الضروري التأكيد منذ البداية أن مصطلح "العقد الذكي" هو تسمية مضللة إلى حد ما، فهو في جوهره ليس "عقداً" بالمعنى القانوني التقليدي الذي يتطلب توافق الإرادتين والأهلية والمحل والسبب. بل هو، من الناحية الفنية، برنامج حاسوبي أو بروتوكول معاملات يتم تخزينه على البلوك تشين ومصمم لتنفيذ بنود محددة بشكل آلي وفوري عند استيفاء شروط مبرمجة مسبقاً. يمكن تشبيهه بآلة بيع آلية: إذا تم إدخال المبلغ الصحيح (الشرط)، فإن الكود سينفذ النتيجة (إخراج المنتج) بشكل حتمي ودون الحاجة إلى تدخل أو تقدير بشري (Szabo, 1997; De Filippi & Wright, 2018).

في سياق سلسلة التوريد الدوائية، يمكن استخدام العقود الذكية لأتمتة عدد لا يحصى من عمليات التحقق والرقابة:

المثال الأول: (الدفع عند الاستلام الموثق): يمكن برمجة عقد ذكي ليقوم بتحويل ثمن شحنة الدواء من حساب الموزع إلى حساب المصنع تلقائياً، ولكن فقط بعد أن يقوم الموزع بمسح كود الشحنة وتسجيل استلامها بشكل صحيح على البلوك تشين.

المثال الثاني (التحقق من درجة الحرارة): إذا كان من الضروري تخزين دواء عند درجة حرارة محددة، يمكن ربط عقد ذكي بمستشعر إنترنت الأشياء (IoT) داخل حاوية شحن. إذا اكتشف المستشعر أن درجة الحرارة تتجاوز الحد المسموح به، يمكن للعقد الذكي تلقائيًا تصنيف الشحنة على أنها "تالفة" أو "غير مطابقة للمواصفات"، مما يمنع بيعها أو حتى يفرض غرامة تلقائيًا على شركة الشحن.

التداعيات من منظور القانون الجنائي:

إن إدخال هذه الدرجة من الأتمتة يفتح آفاقاً جديدة للمنع والرقابة، ولكنه يثير أيضاً تساؤلات جنائية غير مسبوقة.

الإنفاذ الاستباقي والتنظيم الخوارزمي:

تعمل العقود الذكية بوصفها شكلا من أشكال "الإنفاذ الاستباقي". فبدلاً من النموذج القانوني التقليدي الذي يعتمد على الرقابة اللاحقة والعقاب بعد وقوع المخالفة، تقدم العقود الذكية نموذجاً يعتمد على المنع المسبق (ex-ante). فهي تمنع المعاملات غير المطابقة للشروط المبرمجة من الحدوث أصلاً.

هذا التحول ينقل جزءاً من عبء الرقابة من المؤسسات القانونية التقليدية (الدولة، القضاء) إلى البنية التحتية التقنية نفسها. يُعرف هذا المفهوم في الأدبيات بعدة مصطلحات مترادفة:

- التنظيم عبر الكود أو "القانون هو الكود" (Code is Law). هذا المصطلح، الذي أشاعه البروفيسور لورانس ليسيغ، هو الأكثر استخداماً لوصف كيف أن الكود المعماري لبيئة رقمية ما يعمل

بوصفها شكلا من أشكال القانون، إذ يحدد ما هو ممكن وما هو مستحيل داخل تلك البيئة (Lessig, 2006).

– التنظيم المدمج في التصميم" أو "المنع التصميمي". يركز هذا المصطلح على فكرة أن القيود التنظيمية يتم دمجها في تصميم النظام نفسه، بدلاً من فرضها من الخارج.

– التنظيم الخوارزمي: يبرز هذا المصطلح دور الخوارزميات في تنفيذ القواعد التنظيمية بشكل آلي.

من منظور السياسة الجنائية، يمثل هذا تحولاً نموذجياً من "الردع" القائم على التهديد بالعقاب، إلى "المنع" القائم على الاستحالة التقنية (Re-Du-Plessis, 2019).

إشكالية القصد الجنائي في الأكواد المستقل: ماذا لو تم تصميم عقد ذكي بشكل خبيث لارتكاب جريمة؟ على سبيل المثال، عقد ذكي مصمم لسرقة الأموال تلقائياً عند تحقق شرط معين، أو لتسهيل بيع أدوية مسروقة. من هو المسؤول جنائياً عن فعل ارتكبه برنامج مستقل؟

المبرمج: هل هو الشخص الذي كتب الكود؟ هنا، يمكن تطبيق نظريات "الفاعل المعنوي" أو "الارتكاب بالواسطة"، فيكون الكود هو "الأداة" التي استخدمها المبرمج لارتكاب الجريمة. يجب إثبات أن المبرمج كان لديه القصد الجنائي وقت كتابة الكود (Mik, 2019).

الناشر: هل هو الشخص الذي قام بنشر العقد على البلوك تشين وتفعيله؟ قد يكون هذا الشخص مختلفاً عن المبرمج.

المستخدم: ماذا لو كان الكود نفسه محايداً، ولكن تم استخدامه لأغراض إجرامية؟

إن تحديد "الفعل المادي" و"القصد الجنائي" في سياق الأفعال التي ترتكبها برامج شبه مستقلة يمثل أحد أكبر التحديات التي تواجه النظرية العامة للجريمة في القرن الحادي والعشرين.

العقود الذكية بوصفها دليل إثبات: إن سجل تنفيذ العقد الذكي هو في حد ذاته دليل جنائي بالغ الأهمية. فهو يقدم سجلاً ثابتاً ومختوماً بالوقت للشروط التي تم التحقق منها والإجراءات التي تم اتخاذها. يمكن استخدامه لإثبات أو نفي وقوع أحداث معينة بشكل قاطع. على سبيل المثال، لإثبات أن شركة شحن أخلت بالتزاماتها المتعلقة بدرجة الحرارة، يمكن تقديم سجل العقد الذكي الذي يوضح قراءة المستشعر والإجراء التلقائي الذي اتخذه العقد. هذا الدليل الخوارزمي ش يتطلب من القضاة والمحامين تطوير مهارات جديدة لفهمه وتقييمه (De-Filippi & Wright, 2018).

في الختام، يظهر هذا القسم الفرعي أن تقنية البلوك تشين، بخصائصها الفريدة وتطبيقاتها المتقدمة، ليست مجرد حل تقني لمشكلة لوجستية. إنها بنية تحتية جديدة للثقة والمساءلة، تحمل في طياتها القدرة على إعادة تشكيل أدوات القانون الجنائي في منع الجريمة والتحقيق فيها وإثباتها. ولكنها في الوقت نفسه، تفرض على الفكر القانوني الجنائي تحديات مفاهيمية عميقة تتطلب إجابات تشريعية وقضائية مبتكرة، وهو ما سيتناوله القسم التالي من هذا البحث.

٣. إشكالية الإثبات الجنائي بالبيانات المستمدة من البلوك تشين

تمهيد:ـ

بعد أن استعرض البحث في القسم السابق الإمكانيات التقنية الهائلة التي تقدمها البلوك تشين لمكافحة غش الأدوية، ينتقل التحليل الآن من عالم "الإمكانية التقنية" إلى عالم "المقبولية القانونية". فهذه الإمكانيات تظل مجرد حبر على ورق ما لم يتمكن النظام القانوني الجنائي، بأدواته ومبادئه الراسخة، من استيعابها والتعامل معها. وفي قلب هذا التحدي تقع "إشكالية الإثبات"، التي تمثل الجسر الذي يجب أن تعبره أي معلومة لتكتسب وصف "الدليل" وتؤثر في قناعة القاضي الجنائي.

إن الإثبات الجنائي ليس مجرد عملية فنية، بل هو نشاط إجرائي تحكمه فلسفة عميقة تهدف إلى الموازنة بين هدفين متعارضين: "مصلحة المجتمع في العقاب" و"مصلحة الفرد في الحرية". هذه الموازنة تتجلى في مجموعة من المبادئ الضابطة، كمبدأ "الأصل في الإنسان البراءة"، ومبدأ "تفسير الشك لصالح المتهم"، ومبدأ "حرية القاضي في تكوين اقتناعه". وفي هذا السياق، يطرح ظهور دليل جديد، بخصائص غير مسبوقة كالثبات واللامركزية، تساؤلات جوهرية تهدد بزعزعة هذه المبادئ المستقرة.

يهدف هذا القسم إلى تشريح هذه الإشكالية المعقدة. سنبدأ في القسم الفرع الأول بمحاولة تكييف الطبيعة القانونية لسجل البلوك تشين، متسائلين عما إذا كان يمكن إدراجه ضمن فئات الأدلة التقليدية كـ الدليل الكتابي" أو "السجل الإلكتروني"، أم أنه يمثل "قرينة" يسيرة، أم ربما نوعاً جديداً من الأدلة يتطلب تنظيماً خاصاً. وفي القسم الفرعي الثاني، سنغوص أعمق في مسألة "حجية" هذا الدليل، إذ إننا سوف نحلل شروط قبوله أمام القضاء الجنائي، ونواجه التحديات العملية التي تعترض موثوقيته، وعلى رأسها "مشكلة الأوراكل" وكيفية التوفيق بين ثبات السجل وحق المتهم في مناقشة الدليل. وأخيراً، في القسم الفرعي الثالث، ستتناول الجانب الإجرائي، مستكشفين كيفية وصول أجهزة إنفاذ القانون إلى هذا الدليل في بيئة لا مركزية، وما يثيره ذلك من تحديات تتعلق بإجراءات التحقيق والضبط والتفتيش.

٣,١. الطبيعة القانونية لسجل البلوك تشين بوصفها دليل إثبات (دليل كتابي، سجل إلكتروني، قرينة).

إن إدخال أي تقنية جديدة إلى قاعة المحكمة الجنائية يفرض على النظام القانوني الإجابة على سؤال جوهري: ما هو التكييف القانوني للمعلومات التي تنتجها هذه التقنية؟ هذا السؤال ليس مجرد مسألة تصنيف أكاديمي، بل هو بوابة إجرائية تحدد القواعد التي تحكم قبول الدليل، وعبء الإثبات، والسلطة التقديرية للقاضي في تقييمه. وفي حالة البلوك تشين، بسجلها الموزع والمشفر والثابت، يصبح هذا السؤال أكثر إلحاحاً وتعقيداً.

إن دخول سجلات البلوك تشين إلى ساحة الإثبات الجنائي يفرض على النظام القانوني التصدي لمسألة تأسيسية، وهي: كيفية التكييف القانوني لهذا النوع الجديد من الأدلة. هذا التكييف ليس مجرد تصنيف نظري، بل هو عملية إجرائية تحدد مسار الدليل داخل الدعوى، وعليه فإن التحليل يبدأ باستكشاف مدى ملاءمة الفئات التقليدية للأدلة، انطلاقاً من فئة "الدليل الكتابي" العريقة، ثم الانتقال إلى إطار "السجل الإلكتروني" الأكثر حداثة، وصولاً إلى إمكانية التعامل معه كـ"قرينة قضائية" تخضع لتقدير المحكمة.

وكما سيتضح، فإن كل مسار من هذه المسارات يكشف عن حلول جزئية، لكنه يصطدم في الوقت ذاته بعقبات مفاهيمية بنيوية، مما يبرز الحاجة إلى تبني نهج قانوني جديد ومخصص لهذه التقنية (Finck, 2019).

٣,١,١. إشكالية القياس على فئة الأدلة الكتابية

إن المقاربة الأولى التي قد يلجأ إليها الفكر القانوني هي محاولة قياس سجل البلوك تشين على فئة "الأدلة الكتابية" أو "المحررات"، نظراً لاحتوائه على بيانات مدونة ومنسوبة إلى أطراف محددة عبر التوقيع. وعلى الرغم من وجود تشابهات وظيفية ظاهرية، فإن هذا القياس سرعان ما ينهار عند مواجهته بالخصائص البنيوية للبلوك تشين التي تتناقض مع الافتراضات الأساسية لقانون الإثبات التقليدي.

١ـ أوجه التشابه الوظيفي:

يمكن القول إن سجل البلوك تشين يؤدي وظائف مشابهة للمحرر التقليدي:

التدوين والإثبات: كلاهما يسجل واقعة أو تصرفاً قانونياً بشكل مكتوب ودائم.

تحديد المصدر: كما ينسب المحرر الورقي لموقعه، تنسب المعاملة في البلوك تشين لصاحبها عبر "التوقيع الرقمي"، الذي يتم باستخدام المفتاح الخاص للمستخدم.

٢ ـ عقبات القياس الجوهرية:

على الرغم من هذا التشابه الوظيفي، فإن القياس يصطدم بعقبات جوهرية تجعله قياساً مع الفارق:

انهيار مفهوم "الأصل المادي": تقوم حجية المحررات في العديد من النظم القانونية على وجود "أصل مادي" يمكن فحصه والتحقق منه. في المقابل، تقوم البلوك تشين على مبدأ "غياب الأصل" الوحيد؛ فكل نسخة من السجل الموزع هي أصل بحد ذاتها. هذا يقوض بشكل كامل القواعد الإجرائية المصممة للتعامل مع النسخ والأصول، مثل إجراءات المضاهاة والتحقيق في التزوير المادي (Bambara & Schartum, 2021).

تشتت مفهوم "الكاتب" أو "المحرر": إن القواعد التقليدية لحجية المحررات تقوم على فرضية وجود "كاتب" أو "محرر" يمكن تحديد هويته وإسناد المحرر إليه. لكن في بيئة البلوك تشين، يتلاشى هذا المفهوم. فمن هو "الكاتب" القانوني للسجل؟ هل هو المستخدم الذي أنشأ المعاملة الأولية؟ أم المبرمج الذي صمم بروتوكول البلوك تشين؟ أم شبكة "العُقد" المجهولة التي قامت بعملية التحقق

والمصادقة وأضافت الكتلة إلى السلسلة؟ إن عملية إنشاء السجل هي عملية خوارزمية جماعية وليست فعلاً إرادياً فردياً. هذا الغموض في تحديد الفاعل القانوني يمثل عقبة كَأْدَاء أمام تطبيق القواعد التي تربط حجية الدليل بشخص كاتبه، ويجعل من الصعب تحديد من هو المسؤول جنائياً عن محتواه (Hess & Broring, 2021).

مشكلة الإسناد في التوقيع الرقمي: إن القواعد التقليدية لحجية المحررات تقوم على فرضية وجود "كاتب" أو "محرر" يمكن تحديد هويته وإسناد المحرر إليه. لكن في بيئة البلوك تشين، يتلاشى هذا المفهوم ليحل محله "إسناد خوارزمي"، فمن هو "الكاتب" القانوني للسجل؟ هل هو المستخدم الذي أنشأ المعاملة الأولية؟ أم المبرمج الذي صمم بروتوكول البلوك تشين؟ أم شبكة "العُقد" المجهولة التي قامت بعملية التحقق والمصادقة وأضافت الكتلة إلى السلسلة؟ إن عملية إنشاء السجل هي عملية خوارزمية جماعية وليست فعلاً إرادياً فردياً. هذا الغموض في تحديد الفاعل القانوني يمثل عقبة كَأْداء أمام تطبيق القواعد التي تربط حجية الدليل بشخص كاتبه، ويجعل من الصعب تحديد من هو المسؤول عن محتواه (Werbach, 2018).

إن هذه العقبات تجعل من الواضح أن القواعد المصممة لعالم الورق والحبر لا يمكن نقلها بيسر لتنطبق على عالم السجلات الموزعة والمشفرة.

٣,١,٢. مدى كفاية إطار الأدلة الرقمية القائم

نظراً لقصور فئة الأدلة الكتابية، يبدو من المنطقي الانتقال إلى الإطار الأوسع والأكثر حداثة، وهو "الأدلة الرقمية" أو "السجلات الإلكترونية. هذا الإطار مصمم للتعامل مع البيانات غير المادية، ويركز على مفاهيم "الحجية" و"السلامة" بدلاً من "الأصل المادي".

١ـ مزايا التكييف بوصفه سجلا إلكترونيا:

الملاءمة المفاهيمية: تتوافق خصائص البلوك تشين (الثبات، السلامة، الأصالة عبر التشفير) بشكل كبير مع المتطلبات التي تضعها معظم التشريعات لقبول الأدلة الرقمية، مما يجعل هذا التكييف نقطة انطلاق منطقية (Casey et al., 2019).

الاستفادة من القواعد القائمة: يتيح هذا التكييف الاستفادة من التشريعات والسوابق القضائية الموجودة بالفعل بشأن قبول الأدلة الرقمية، بدلاً من الحاجة إلى إنشاء إطار قانوني جديد بالكامل من الصفر.

٢ ـ أوجه القصور والتحديات الجديدة:

مع ذلك، فإن سجل البلوك تشين ليس مجرد سجل إلكتروني عادي، وخصائصه الفريدة تثير تحديات جديدة حتى داخل إطار الأدلة الرقمية:

غياب "حارس السجل" المركزي: تفترض معظم قواعد الأدلة الرقمية وجود "حارس للسجل" – بوصفه مسؤول تقنية المعلومات في شركة ما – يمكن استدعاؤه للشهادة حول كيفية إنشاء النظام وصيانته. في شبكة بلوك تشين لامركزية، لا يوجد مثل هذا الحارس، هذا يطرح سؤالاً إجرائياً صعباً: من هو الشاهد المؤهل لتقديم "الأساس" لقبول الدليل أمام المحكمة؟ (Grigg, 2020).

التعقيد التقني وعبء الخبرة: إن مستوى التعقيد التقني للبلوك تشين يفوق بكثير مستوى تعقيد الأدلة الرقمية التقليدية (كبريد إلكتروني). هذا يعني أن قبول الدليل وتقييمه سيعتمد بشكل شبه كامل على شهادة الخبراء الفنيين، مما قد يحد من قدرة القاضي على ممارسة "اقتناعه القضائي الحر" ويفتح الباب أمام "معركة الخبراء" التي قد تحجب الحقيقة بدلاً من كشفها (De-Filippi & Wright, 2018).

إذن، وعلى الرغم من أن إطار الأدلة الرقمية هو الأقرب لاستيعاب سجل البلوك تشين، فإنه إطار غير كافٍ بمفرده، ويتطلب إما تفسيراً قضائياً مرناً أو تطويراً تشريعياً يأخذ في الاعتبار الطبيعة اللامركزية والمعقدة لهذه التقنية.

٣,١,٣. التعامل مع السجل بوصفه قرينة قضائية: بين المرونة والغموض

في مواجهة الصعوبات السابقة، قد يميل القضاء، خاصة في النظم التي تتبنى مبدأ حرية الإثبات الجنائي، إلى تجنب التصنيف الصارم والتعامل مع سجل البلوك تشين بوصفه "قرينة قضائية" يسيرة، تخضع لتقدير قاضي الموضوع.

١ـ مزايا نهج القرينة:

المرونة القضائية: يمنح هذا النهج القاضي سلطة تقديرية واسعة لتقييم "القوة الإقناعية" للبيانات في كل حالة على حدة، ووزنها مع باقي الأدلة في الدعوى، دون التقيد بقواعد شكلية صارمة.

تجاوز العقبات الإجرائية: يسمح هذا النهج بتجاوز العقبات الإجرائية المتعلقة بتحديد "الأصل" أو "حارس السجل"، والتركيز مباشرة على جوهر الدليل ومضمونه.

٢ ـ مخاطر وعيوب هذا النهج:

إهدار القيمة الثبوتية: إن إنزال سجل البلوك تشين، بكل ضماناته التقنية، إلى مرتبة قرينة يسيرة يعامله كأي دليل ظرفي آخر، ويهدر قيمته الثبوتية المتفوقة. هذا قد يقلل من أهميته في نظر أجهزة إنفاذ القانون ويضعف دوره بوصفه أداة للمكافحة (Casino et al., 2019).

غياب اليقين القانوني: إن ترك الأمر بالكامل لتقدير القضاة دون معايير واضحة سيؤدي حتماً إلى تباين في الأحكام وإلى غياب اليقين القانوني. فما يعتبره قاضٍ قرينة قوية، قد يعتبره آخر مجرد إشارة لا قيمة لها، مما يضر باستقرار المعاملات ومصالح المتقاضين (Yeoh, 2021).

خلاصة القسم الفرعي: نحو تكييف قانوني مستقل

يُظهر هذا التحليل أن كل فئة من فئات الإثبات التقليدية (الكتابي، الإلكتروني، القرينة) تفشل في استيعاب الطبيعة الهجينة والمركبة لسجل البلوك تشين بشكل كامل. فمحاولة إدخاله في قوالب قانونية قديمة هي أشبه بمحاولة تخزين بيانات رقمية على مخطوطة ورقية.

لذا، فإن الاستجابة القانونية الأكثر نضجاً وفعالية تكمن في الاعتراف بأننا أمام "دليل من نوع جديد". هذا الاعتراف يجب أن يقود إلى أحد مسارين: إما تطوير القضاء لتفسير مرن لقواعد الأدلة الرقمية ينشئ "قرينة قانونية" قوية لصحة بيانات البلوك تشين (مع إمكانية دحضها)، أو تدخل تشريعي مباشر لإنشاء فئة مستقلة من "أدلة السجلات الموزعة" مع قواعد إثبات خاصة بها (Finck, 2019). إن وضوح التكييف القانوني هو الخطوة الأولى والضرورية لدمج هذه التقنية الثورية في منظومة العدالة الجنائية بشكل آمن وفعال.

٣,٢. حجية الدليل المستمد من البلوك تشين بين الحصانة التقنية والهشاشة الإجرامية

إن اجتياز الدليل لعتبة "التكييف القانوني" لا يمنحه حصانة أو حجية مطلقة، بل يؤهله فقط للدخول إلى المرحلة التالية والأكثر صرامة: اختبار "الحجية". في فقه الإثبات الجنائي، الحجية ليست مفهوماً أحادياً، بل هي نتاج تفاعل معقد بين "الصلاحية" و"الوزن". الحجية تتعلق بالسلامة الداخلية للدليل وقدرته على عكس الحقيقة، بينما الوزن يتعلق بمدى تأثير هذا الدليل على قناعة القاضي اليقينية عند الموازنة بينه وبين كافة أدلة الدعوى.

يطرح سجل البلوك تشين مفارقة إثباتية فريدة: فهو يقدم درجة من السلامة التشفيرية التقنية الداخلية قد تفوق أي دليل رقمي آخر بفضل خصائص الثبات والتشفير، ولكنه في الوقت نفسه، يعاني من هشاشة بنيوية في تفاعله مع العالم الخارجي، مما قد يقوض وزنه الثبوتي بالكامل. إن هذه المفارقة هي التي تجعل تقييم حجيته مهمة قضائية دقيقة وحساسة.

سيتناول هذا القسم الفرعي هذه المسألة من خلال ثلاثة فروع متكاملة. أولا سنتناول نقطة ضعف هذه التقنية وهي "كعب أخيل". وهي التحدي المتعلق بصحة بيانات الإدخال. ثم سنحلل التعارض الدستوري بين الثبات وحقوق الدفاع الأساسية. وأخيرًا، سنستكشف التحديات الإجرائية التي تواجهها جهات إنفاذ القانون في الحصول على هذه الأدلة ومعالجتها في بيئة لامركزية.

٣,٢,١. تحدي صحة البيانات المدخلة: كعب أخيل الإثبات بالبلوك تشين

إن الوهم الأكبر الذي قد يقع فيه غير المتخصص هو الاعتقاد بأن البلوك تشين هي "آلة حقيقة" قادرة على التحقق من صحة البيانات بشكل مطلق. والحقيقة القانونية الدقيقة هي أنها، في جوهرها، "آلة ذاكرة" أو "آلة سلامة بيانات"؛ فهي تتذكر ما قيل لها ببراعة وأمانة مطلقة، وتضمن عدم تغيير هذه الذاكرة، لكنها لا تملك أي قدرة ذاتية على التمييز بين الحقيقة والكذب في محتوى ما قيل لها. هذه الفجوة بين الذاكرة المثلى

والوعي المنعدم هي جوهر ما يعرف بـ "مشكلة الأوراكل". "الأوراكل" هو أي قناة – سواء كانت بشرية أو آلية – يتم من خلالها إدخال بيانات من العالم المادي إلى العالم الرقمي للبلوك تشين. من منظور القانون الجنائي، هذه المشكلة ليست مجرد ثغرة تقنية، بل هي بوابة للاحتيال والتضليل، وهي تقوض بشكل مباشر المبدأ الأساس الذي يقوم عليه الإثبات: البحث عن الحقيقة الموضوعية (Casey & Lundy, 2021).

أولاً: الطبيعة المزدوجة للأوراكل في سلسلة الإمداد الدوائية

في سياق مكافحة غش الأدوية، يمكن أن يتخذ الأوراكل شكلين رئيسين، لكل منهما نقاط ضعفه الجنائية:

الأوراكل البشري:

وهو الموظف أو العامل الذي يقوم بالفعل المادي لإدخال البيانات، كمسح رمز الاستجابة السريعة (QR code) على علبة الدواء. هنا، تكون حجية السجل بأكمله رهينة لأمانة وكفاءة هذا الشخص. يمكن أن يفشل الأوراكل البشري جنائياً بطرق متعددة:

الفعل العمدي: يمكن لموظف فاسد متواطئ مع شبكة إجرامية أن يقوم عمداً بتزييف المدخلات. السيناريو الكلاسيكي: يستلم الموظف شحنة أدوية أصلية وأخرى مزيفة. يقوم بمسح الرموز الخاصة بالشحنة الأصلية لتسجيلها على البلوك تشين، ولكنه يقوم فعلياً بشحن الأدوية المزيفة، بينما يسرق الأصلية لبيعها في السوق السوداء. النتيجة: سجل بلوك تشين "أمثل" من الناحية التقنية، يثبت واقعة كاذبة تماماً. هنا، تتحول البلوك تشين من أداة لكشف الجريمة إلى أداة لإخفائها وتوفير غطاء شرعي لها (Butler & Giuliano, 2018).

الإهمال الجسيم: قد لا يكون الأوراكل البشري فاسداً، ولكنه مهمل. فقد يقوم الموظف بمسح الرمز الخطأ، أو إدخال بيانات غير دقيقة عن طريق السهو، أو عدم اتباع البروتوكولات الأمنية الواجبة. في القانون المدني، قد يؤدي هذا إلى مسؤولية تعاقدية أو تقصيرية. أما في القانون الجنائي، فإن العواقب قد تكون وخيمة؛ فهذا الخطأ، الذي سيتم تخليده بشكل "ثابت" على السلسلة، قد يؤدي إلى بناء قضية جنائية ضد شخص بريء أو تبرئة مجرم. هذا يثير تساؤلات معقدة حول مدى إمكانية مساءلة الموظف المهمل جنائياً عن هذه النتائج. فهل يمكن اعتبار إهماله في إدخال البيانات "سبباً" مباشراً في "شهادة الزور" أو "تضليل العدالة"؟ يتوقف ذلك على مدى جسامة الإهمال وما إذا كان التشريع الجنائي يعاقب على هذه الجرائم في صورتها غير العمدية، وهو أمر نادر في معظم النظم القانونية، مما قد يخلق فراغاً في المساءلة (Bambara & Schartum, 2021).

الإكراه: قد يتم إجبار الأوراكل البشري، تحت التهديد المادي أو المعنوي، على إدخال بيانات خاطئة. في هذه الحالة، ووفقاً للمبادئ العامة للقانون الجنائي، ينتفي الركن المعنوي لديه؛ لأن إرادته كانت معيبة، مما يمنع مساءلته جنائياً بوصفه فاعلا أصليا أو شريكا في الجريمة. ومع ذلك، من منظور قانون الإثبات، فإن

النتيجة تظل واحدة: سجل بلوك تشين موثوق من الناحية التقنية، ولكنه كاذب من الناحية الموضوعية. هذا يوضح مرة أخرى أن سلامة السجل التشفيرية لا يمكن أن تكون بديلاً عن التحقيق في الظروف الواقعية المحيطة بعملية إدخال البيانات؛ لأن الدليل الرقمي "الأمثل" قد يكون نتاجاً لإرادة إجرامية لم تترك أي أثر على الكود نفسه (Zamfir, 2018).

الأوراكل الآلي:

وهو جهاز أو مستشعر يقوم بإدخال البيانات تلقائياً، مثل مستشعرات إنترنت الأشياء (IoT) التي تقيس درجة حرارة حاوية الشحن. وعلى الرغم من أن هذا يقلل من خطر الخطأ البشري، فإنه يفتح الباب أمام أنواع أخرى من الهجمات:

الاختراق السيبراني: إن ربط البلوك تشين بأجهزة إنترنت الأشياء (IoT) مثل المستشعرات يخلق سطح هجوم جديد – هو كل نقاط الضعف المحتملة التي تنشأ من إضافة مكونات جديدة (المستشعرات) إلى نظام آمن أصلاً، مما يزيد من فرص المهاجمين في إيجاد ثغرة لاختراقه-. فبينما قد تكون البلوك تشين نفسها آمنة، فإن المستشعرات وقنوات الاتصال التي تربطها بالسلسلة غالباً ما تكون أقل أمناً. يمكن للمجرمين استغلال هذه الثغرات لاختراق المستشعر نفسه، أو اعتراض قناة الاتصال بينه وبين البلوك تشين (فيما يعرف بهجوم "الرجل في المنتصف" – هو هجوم تنصت وتلاعب، إذ يضع المهاجم نفسه سراً في مسار الاتصال بين طرفين، ويعترض رسائلهما، ويقرؤها، ويعدلها، ثم يعيد إرسالها دون أن يكتشفه أي منهما. إنه يحول قناة اتصال موثوقة ظاهرياً إلى أداة للتضليل- وإجباره على إرسال بيانات مزيفة. على سبيل المثال، يمكنهم إرسال قراءة "٥ درجات مئوية" بينما درجة الحرارة الفعلية للدواء هي ٣٠ درجة، مما يجعل الدواء التالف يبدو سليماً على السجل الثابت. هذا يعني أن حجية النظام كله لا تقاس بقوة أمن البلوك تشين فقط، بل بقوة أمن أضعف حلقة في السلسلة، وهي غالباً ما تكون هي أجهزة الأوراكل الآلي (Dorri et al., 2019).

التلاعب المادي: إن التهديدات لا تقتصر على الهجمات السيبرانية، بل تمتد إلى التلاعب المادي المباشر بالأوراكل الآلي. فالمستشعرات هي أجهزة مادية موجودة في العالم الحقيقي، وبالتالي فهي عرضة للهجوم المادي. يمكن للمجرمين، على سبيل المثال، التلاعب ببيئة المستشعر لخداعه؛ كأن يتم وضع مستشعر درجة الحرارة في حاوية صغيرة مبردة بشكل مصطنع داخل شاحنة الشحن الساخنة، أو تغطية مستشعر الضوء لمنعه من تسجيل تعرض الدواء للشمس. في هذه الحالة، يكون المستشعر نفسه يعمل بشكل صحيح من الناحية التقنية، ويرسل بيانات دقيقة عن البيئة المصطنعة التي وضع فيها، ولكن هذه البيانات لا تعكس على الإطلاق الظروف الحقيقية التي يتعرض لها المنتج الدوائي. هذا يوضح أن أمن سلسلة التوريد القائمة على البلوك تشين لا يعتمد فقط على الأمن السيبراني، بل أيضاً على الأمن المادي ووجود ضوابط لمنع الوصول غير المصرح به إلى الأجهزة الطرفية (Weber et al., 2019).

العطل والخطأ في المعايرة: بعيداً عن أي تدخل إجرامي، فإن المستشعرات، كأي جهاز مادي، تخضع للتلف والاهتراء. فقد تتعطل بشكل مفاجئ، أو تفقد دقتها تدريجياً مع مرور الوقت فيما يعرف بـ "الانحراف في الاستشعار"، مما يؤدي إلى تسجيل بيانات خاطئة بشكل غير مقصود. من منظور الإثبات الجنائي، يفتح هذا الاحتمال الباب أمام دفوع قوية من جانب الدفاع، فيمكن المجادلة بأن البيانات التي تدين المتهم (مثل ارتفاع درجة الحرارة) لم تكن نتيجة إهماله، بل نتيجة عطل فني في جهاز القياس. لمواجهة هذا الدفع، يقع على عاتق الادعاء عبء إثبات ليس فقط سلامة سجل البلوك تشين، بل أيضاً وجود "نظام صيانة ومعايرة" موثوق للأجهزة الطرفية. إن غياب دليل على الصيانة الدورية والمعايرة الموثقة للمستشعرات قد يكون كافياً لزرع "شك معقول" في قناعة المحكمة حول حجية الدليل الرقمي المقدم (Salah et al., 2019).

ثانياً: الأثر على عبء الإثبات ومبدأ افتراض البراءة

إن وجود مشكلة الأوراكل يعيد تشكيل عبء الإثبات في الدعوى الجنائية بشكل جذري. في النظام التقليدي، إذا قدم الادعاء دليلاً، فإن على الدفاع أن يثير شكاً معقولاً حوله. أما في حالة البلوك تشين، فإن الادعاء العام لا يكفيه أن يثبت سلامة السجل الرقمي، بل يقع عليه عبء إضافي وحاسم: إثبات سلامة وحجية الأوراكل الذي قام بتغذية هذا السجل بالبيانات.

هذا يعني أن على المدعين العامين تقديم أدلة للإجابة على أسئلة مثل:

- من هو الموظف الذي مسح الرمز؟ هل لديه سجل جنائي؟ هل هناك أي دليل على التآمر؟
- هل توجد كاميرات مراقبة في منطقة المسح؟ ماذا التقطت الكاميرات؟
- بالنسبة لجهاز الاستشعار الآلي، متى فُحص آخر مرة؟ من صنعه؟ هل توجد سجلات صيانة ومعايرة؟

إن الفشل في تقديم أدلة مقنعة حول حجية "نقطة الإدخال" يفتح الباب واسعاً أمام الدفاع للتمسك بـ "مبدأ افتراض البراءة". يمكن للمحامي أن يجادل بأنه طالما أن مصدر البيانات مشكوك فيه، فإن السجل الناتج، مهما كان آمناً تقنياً، لا يمكن أن يصل إلى درجة اليقين المطلوبة للإدانة. إنه يخلق "فرضية بديلة معقولة" لا يمكن استبعادها، وهو كل ما يحتاجه الدفاع لزرع الشك في قناعة المحكمة (Chohan, 2019).

ثالثاً: اصطناع "الدليل الزائف الأمثل" بوصفه سلاحا إجراميا

الأخطر من ذلك هو أن المجرمين يمكن أن يستخدموا مشكلة الأوراكل بشكل استباقي بوصفه سلاحا. يمكن لشبكة إجرامية متطورة أن تصمم عملياتها بحيث تستغل الثقة العمياء للنظام في مدخلاته لاصطناع "دليل زائف أمثل". يمكنهم بناء سجل يبدو نظيفاً وأمثل يوثق سلسلة توريد وهمية لمنتجاتهم المزيفة، مما يمنحها غطاءً من الشرعية الرقمية يصعب اختراقه. هذا يقلب دور البلوك تشين رأساً على عقب، فتحولها من

أداة للشفافية إلى أداة للتعتيم، ومن دليل ضد المجرم إلى دليل لصالحه. إن هذا الاحتمال وحده يجب أن يجبر أي قاضٍ جنائي يتعامل مع أدلة البلوك تشين على تبني "مبدأ الشك المنهجي في المصدر" بوصفه قاعدة أساسية عند تقييم هذه الأدلة، مدركاً أن سلامة الكود لا تضمن صدق النوايا (Kshetri, 2021).

٣,٢,٢. التوفيق بين ثبات السجل وحقوق الدفاع الدستورية

إذا كانت "مشكلة الأوراكل" تمثل التحدي الذي يواجه حجية البلوك تشين من الخارج (أي من العالم المادي)، فإن خاصية "الثبات" تولّد تحدياً لا يقل خطورة من الداخل (أي من صميم تصميمها التقني). هذه الخاصية التي تعتبر حجر الزاوية في أمن البلوك تشين، تضعها في مسار تصادمي مباشر مع المبادئ الدستورية والإجرائية التي تشكل أساس المحاكمة الجنائية العادلة.

ففكرة وجود سجل أبدي لا يقبل التغيير أو المحو على الرغم من جاذبيتها الظاهرية من منظور سلامة البيانات تتعارض بشكل صارخ مع فلسفة العدالة الجنائية نفسها؛ فالعدالة ليست نظاماً جامداً، بل هي عملية ديناميكية تسعى لكشف الحقيقة، وتتطلب بطبيعتها المرونة والقدرة على مراجعة الأدلة وتصحيح الأخطاء. إن هذا التوتر بين "جمود الكود" و"مرونة العدالة" يثير إشكاليات دستورية عميقة، أبرزها:

- الصدام مع الحق في المواجهة ومناقشة الأدلة.
- التعارض مع الحق في التصحيح ومبدأ "إصلاح الخطأ القضائي".

سيتناول هذا الفرع تحليل هذين الصدامين، ويقترح إطاراً قانونياً لإعادة توجيه حقوق الدفاع بما يتناسب مع طبيعة هذا الدليل الجديد.

أولاً: الصدام مع الحق في المواجهة ومناقشة الأدلة

"الحق في المواجهة" ، المنصوص عليه في العديد من الدساتير والمواثيق الدولية (مثل المادة ٦ من الاتفاقية الأوروبية لحقوق الإنسان) ، هو أكثر من مجرد حق شكلي. إنه آلية أساسية لكشف الحقيقة، تتيح للدفاع فرصة استجواب شهود الإثبات، وتحدي ذاكرتهم، وكشف دوافعهم، وملاحظة سلوكهم أمام المحكمة.

إن سجل البلوك تشين، عند تقديمه بوصفه دليلا، يصبح "شاهداً إلكترونياً". لكنه شاهد من نوع خاص:

ـ شاهد أصم وأبكم: لا يمكن استجواب سجل البلوك تشين أو مناقشته. فهو يقدم "شهادته" (البيانات المسجلة) حقيقة رياضية نهائية ومطلقة. لا يمكن سؤال السجل: "هل أنت متأكد من هذه المعلومة؟"، "ماذا كانت الظروف المحيطة بتسجيلها؟"، "هل هناك أي احتمال للخطأ؟". إن هذا "الصمت الخوارزمي" يجعله شاهداً غير قابل للاستجواب، مما يتناقض بشكل مباشر مع جوهر الحق في المواجهة الذي يفترض وجود شاهد بشري يمكن اختبار مصداقيته وذاكرته تحت ضغط الاستجواب المتقاطع. إن الاعتماد على مثل هذا الدليل "الأصم" قد يحول عملية الإثبات من حوار نقدي إلى مجرد قبول سلبي

لنتائج عملية حسابية معقدة، وهو ما يثير قلقاً بالغاً بشأن الحفاظ على الطابع الإنساني للعدالة (Cupa, 2021).

غياب لغة الجسد (غياب السلوك الظاهري): يعتمد القضاة والمحلفون، خاصة في أنظمة القانون العام، بشكل كبير على ملاحظة السلوك الظاهري للشاهد– كنبرة صوته، وتواصله البصري، وتردده، وثقته – بوصفها أداة حيوية لتقييم مصداقيته. أما سجل البلوك تشين، فهو دليل بارد ومجرد، لا يملك أي سمات إنسانية يمكن تقييمها. إنه يقدم البيانات بنقاء رياضي مجرد من أي سياق إنساني. هذا الغياب التام لـ "أدلة السلوك" يحرم المحكمة من أحد أقدم وأهم الأدوات التي تستخدمها لتمييز الصدق من الكذب، ويجعل تقييم الدليل يعتمد بشكل حصري على التحليل التقني، مما قد يفقر العملية القضائية ويبعدها عن بعدها الإنساني (Raskin, 2017).

هذا يفرغ الحق في المواجهة من مضمونه الفعلي. فكيف يمكن للمتهم أن يدافع عن نفسه في مواجهة دليل لا يقبل النقاش أو التحدي؟ إن القبول الأعمى لسجل البلوك تشين بوصفه حقيقة نهائية يحول المحاكمة من عملية تحقيق وموازنة إلى مجرد عملية تصديق على ما يقوله الكود، وهو ما يتعارض مع جوهر الوظيفة القضائية (Fairfield, 2018)).

ثانياً: التعارض مع الحق في التصحيح ومبدأ "إصلاح الخطأ القضائي"

إن أحد أهم مبادئ العدالة هو القدرة على إصلاح الخطأ. إذا اكتشف لاحقاً أن دليلاً ما كان مزوراً أو أن شاهداً كان كاذباً، يمكن إعادة فتح القضية وتصحيح الحكم. لكن ماذا لو كان الدليل الخاطئ مسجلاً على بلوك تشين "ثابتة"؟

ترسيخ الخطأ بشكل ثابت: إذا تم إدخال معلومة خاطئة إلى السجل (بسبب مشكلة الأوراكل)، فإن هذه المعلومة يتم ترسيخها لتصبح جزءاً لا يُمحى من الحقيقة الخوارزمية المسجلة. حتى لو ثبت لاحقاً بأدلة قاطعة أن هذه المعلومة خاطئة، فلا توجد آلية تقنية متأصلة في معظم تصميمات البلوك تشين العامة لمسحها أو تعديلها. هذا "التثبيت النهائي للخطأ" لا يتعارض فقط مع حقوق حماية البيانات كالحق في التصحيح، بل يقوض أيضاً قدرة نظام العدالة الجنائية على إصلاح أخطائه، وهو مبدأ جوهري للمحاكمة العادلة (Fairfield, 2018).

انتهاك الحق في السمعة والخصوصية: هذا الأمر له آثار تتجاوز قاعة المحكمة. فالشخص الذي تم تسجيل معلومة خاطئة عنه (مثلاً، اتهامه زوراً بالتعامل مع أدوية مزيفة) سيظل هذا " وصمة العار الرقمية الدائمة" يلاحقه إلى الأبد، مما قد يدمر سمعته وفرصه المستقبلية. هذا يتعارض بشكل مباشر مع "الحق في النسيان" الذي أصبح حقاً معترفاً به في العديد من النظم القانونية المتقدمة (مثل لائحة GDPR الأوروبية) (De Caria, 2019).

ثالثاً: نحو إعادة توجيه حقوق الدفاع

إن الحل لهذا الصدام الدستوري لا يكمن في رفض تقنية البلوك تشين بالكامل، بل في "إعادة توجيه" ممارسة حقوق الدفاع من "محتوى" الدليل إلى "عملية إنتاج" الدليل. يجب أن يتمكن الدفاع من ممارسة حقوقه بشكل كامل من خلال:

الحق في استجواب الأوراكل: إن الحل لهذا التحدي الدستوري لا يكمن في محاولة "استجواب" الكود، بل في إعادة توجيه حق المواجهة من "السجل" إلى "مصدر" البيانات. فبدلاً من استجواب الشاهد الأصم، يجب أن يكون للدفاع الحق الكامل في استجواب الشخص أو فحص الآلية التي قامت بإدخال البيانات. هذا يجعل من "الأوراكل" الشاهد الحقيقي أو "المُصَرِّح" بالمعنى القانوني، بينما لا يعدو السجل كونه مجرد أداة تسجيل فائقة الدقة. إن هذا التحول في بؤرة التدقيق القضائي هو استجابة منطقية لطبيعة التقنية؛ لأن حُجِّيَّة النظام بأكمله لا تتجاوز حُجِّيَّة مدخلاته، وبالتالي يجب أن تتركز الضمانات الإجرائية عند نقطة الإدخال هذه (Mik, 2017).

الحق في تدقيق الكود: يجب أن يكون للدفاع- من خلال خبير فني- الحق في الوصول إلى الكود المصدري للبلوك تشين والعقود الذكية المستخدمة وفحصه. هذا الحق لا يقتصر على مجرد الاطلاع، بل يشمل القدرة على اختبار الكود للبحث عن أي ثغرات أمنية، أو تحيزات مدمجة في الخوارزميات، أو أي نقاط ضعف تصميمية قد تؤثر على حُجِّيَّة النظام. إن هذا يمثل شكلاً جديداً وضرورياً من أشكال "الاكتشاف" في العصر الرقمي، إذ يصبح الكود نفسه ساحة للتحقيق والتدقيق. فبدون القدرة على فحص "الصندوق الأسود" الذي أنتج الدليل، يُحرم الدفاع من فرصة حقيقية لتحدي أساس الأدلة المقدمة ضده (Wexler, 2018).

الحق في مواجهة الخبير: بما أن فهم وقبول الدليل المستمد من البلوك تشين سيعتمد بشكل حاسم على شهادة الخبير الفني الذي يقدمه الادعاء، فإن الحق في المواجهة يتجسد هنا في صورة "الحق في استجواب الخبير". يجب أن يكون للدفاع الحق الكامل، وغير المنقوص في إجراء استجواب متقاطع، دقيق للخبير حول منهجيته، والأدوات التي استخدمها، والافتراضات التي بنى عليها تحليله، ومدى حُجِّيَّة استنتاجاته. علاوة على ذلك، يجب ضمان حق الدفاع في تقديم "خبير مضاد" لتقديم رأي فني مخالف وتحدي شهادة خبير الادعاء. إن "معركة الخبراء" هذه، على الرغم من تعقيدها، هي الآلية الإجرائية الأساسية التي تتيح للمحكمة تقييم الأدلة التقنية المعقدة بشكل نقدي وتمنعها من القبول السلبي لسردية فنية أحادية الجانب (Imwinkelried, 2019).

من خلال هذا التحول، نحافظ على جوهر حقوق الدفاع مع تكييفها لتناسب الطبيعة الفريدة لهذا الدليل الجديد.

٣,٢,٣. الإجراءات الجنائية للوصول إلى الدليل والتحقيق فيه

إن التحديات التي تفرضها البلوك تشين لا تقتصر على قاعة المحكمة، بل تبدأ في مرحلة مبكرة جداً: مرحلة التحقيق، وجمع الاستدلالات. فالطبيعة اللامركزية والعابرة للحدود والمشفرة لهذه التقنية تجعل الأدوات الإجرائية التقليدية، التي صممت لعالم مادي ومركزي، تبدو قديمة وغير فعالة.

أولاً: إشكالية التفتيش والضبط في بيئة لا مركزية

إن الإجراءات الجنائية التقليدية للتفتيش والضبط، كما هي مقننة في معظم الدساتير والقوانين الإجرائية، متجذرة بعمق في مفهوم "المكان" المادي و"الحيازة" المادية؛ فالإذن القضائي بالتفتيش يصدر عادةً لتفتيش "مكان معين" يُحتمل وجود أدلة فيه. لكن شبكة البلوك تشين، بطبيعتها الموزعة والعابرة للحدود، تفكك هذا الارتباط الجغرافي وتجعل مفهوم "المكان" بلا معنى.

فأين هو "المكان" الذي سيصدر الإذن القضائي بتفتيشه؟ هل هو كل عقدة (node) من آلاف العُقد الموزعة في عشرات الدول؟ إن محاولة الحصول على إذن قضائي لكل عقدة على حدة هو أمر مستحيل عملياً وقانونياً، وينتهك سيادة الدول الأخرى. هذا التشتت يخلق ما يمكن تسميته بـ "أزمة مكانية" (للقانون الإجرائي، إذ إن الأدوات القانونية المصممة لعالم من الذرات تجد نفسها عاجزة في عالم من البنات الموزعة (Ferguson, 2017).

ما هو الشيء المراد "ضبطه"؟ لا يمكن "ضبط" أو "حجز" سجل البلوك تشين الموزع. ما يمكن ضبطه هو أحد أمرين:

العقدة (The Node): يمكن للمحققين من خلال إذن قضائي، ضبط جهاز الكمبيوتر الذي يعمل عقدة في الشبكة، لكن هذا الإجراء، الذي يبدو منطقياً للوهلة الأولى، يثير إشكاليات دستورية وإجرائية خطيرة:

– **أولاً، مشكلة الضبط المفرط وانتهاك الخصوصية**: هذا الجهاز يحتوي على نسخة من السجل بأكمله، بما في ذلك معاملات آلاف، بل ملايين، المستخدمين الآخرين الذين لا علاقة لهم بالجريمة قيد التحقيق. إن ضبط هذا الكم الهائل من البيانات غير ذات الصلة يمثل "ضبطاً مفرطاً" وتعدياً جانبياً هائلاً على خصوصية أطراف ثالثة بريئة، مما قد يتعارض بشكل مباشر مع "مبدأ التحديد" الذي تشترطه معظم الأوامر القضائية.

– **ثانياً، عدم جدوى الإجراء**: من منظور السيطرة على الأدلة، فإن ضبط عقدة واحدة هو إجراء شبه عديم الجدوى. فالشبكة اللامركزية مصممة بطبيعتها لتكون صامدة؛ ضبط عقدة واحدة لا يوقف الشبكة، ولا يمنع بقية العقد من الاستمرار في العمل، ولا يحول دون وصول أي شخص آخر إلى نسخة مطابقة من السجل. إنه أشبه بمحاولة تجفيف المحيط عن طريق إزالة كوب واحد من الماء (Sheyn, 2018).

المفتاح الخاص: هذا هو الهدف الأكثر منطقية من الناحية الإجرائية. فالمفتاح الخاص هو أداة السيطرة على الأصول الرقمية والمعاملات. لذلك، يجب أن تركز الأوامر القضائية على "تفتيش" الأجهزة

الإلكترونية للمشتبه به (كمبيوتر، هاتف، محافظ أجهزة) بحثاً عن المفاتيح الخاصة، و"ضبطها" أو الأمر بتسليمها. لقد أصبح المفتاح الخاص هو المعادل الرقمي لخزنة البنك أو مفتاح المنزل في العالم المادي (Epstein, 2018).

ثانياً: تحليل البلوك تشين بوصفه فرعا جديدا من الطب الشرعي الرقمي

إن الحصول على بيانات البلوك تشين ليس سوى البداية. فالبيانات الخام، على الرغم من شفافيتها، غالباً ما تكون ضخمة ومجهولة الهوية اسمياً، مما يجعلها عديمة الفائدة دون تحليل معمق. لمواجهة هذا التحدي، نشأ فرع متخصص من الطب الشرعي الرقمي يُعرف بـ "تحليل البلوك تشين" ، الذي يعتمد على أدوات برمجية متطورة لتطبيق تقنيات تحليل البيانات الضخمة على سجلات البلوك تشين، بهدف:

- **تتبع تدفق الأموال/الأصول**: من خلال تحليل الرسم البياني للمعاملات، يتم ربط المعاملات المختلفة لتتبع مسار أصل معين عبر الشبكة من عنوان إلى آخر.

- **تجميع العناوين**: استخدام تقنيات الاستدلال – مثل افتراض أن جميع المدخلات في معاملة واحدة تنتمي إلى نفس المالك – لتحديد المجموعات المحتملة من العناوين التي من المرجح أن تكون تحت سيطرة شخص أو كيان واحد. (Paquet-Clouston et al., 2019)

إزالة إخفاء الهوية: ربط العناوين المشفرة على السلسلة بهويات حقيقية في العالم المادي، وذلك من خلال تحليل نقاط التفاعل مع الأنظمة المالية التقليدية (مثل منصات تبادل العملات التي تتطلب التحقق من هوية العميل.

إن استخدام هذه الأدوات من قبل أجهزة إنفاذ القانون يثير تساؤلات قانونية مهمة:

هل يعتبر تحليل البلوك تشين "تفتيشاً"؟ هل يحق للدولة تحليل البيانات المتاحة على بلوك تشين عامة بحرية، أم أن هذا النشاط يتطلب إذناً قضائياً لأنه يكشف عن معلومات خاصة بالأفراد؟ الجدل القانوني لا يزال قائماً حول هذه النقطة. (Loideain, 2020)

حجية أدوات التحليل: هذه الأدوات التجارية مثل Chainalysis أو Elliptic تستخدم خوارزميات معقدة ومملوكة للقطاع الخاص. يجب على المحاكم أن تضع معايير واضحة لقبول النتائج الصادرة عن هذه الأدوات، وأن تسمح للدفاع بفحص منهجيتها والتحقق من دقتها.

ثالثاً: حتمية التعاون الدولي في مواجهة اللامركزية

بما أن شبكات البلوك تشين عابرة للحدود بطبيعتها، فإن أي تحقيق فعال يتطلب درجة غير مسبوقة من التعاون القضائي الدولي.

قصور آليات المساعدة القانونية المتبادلة: إن اتفاقيات المساعدة القانونية المتبادلة التقليدية مصممة وفق نموذج "الدولة-مقابل-الدولة" المركزي، وتتطلب مخاطبة سلطة مركزية مختصة في الدولة الأخرى عبر قنوات دبلوماسية غالباً ما تكون بطيئة. لكن في عالم البلوك تشين، تتفتت الأدلة عبر ولايات

قضائية متعددة: فقد تكون العقدة (node) في دولة، والمفتاح الخاص للمشتبه به في دولة ثانية، وبيانات منصة التبادل التي استخدمها في دولة ثالثة. هذا "التفتيت الإثباتي" يجعل عملية المساعدة القانونية المتبادلة، بمساراتها البيروقراطية الطويلة، بطيئة بشكل منهجي وغير متناسبة مع سرعة الجريمة الرقمية، مما يمنح المجرمين وقتاً كافياً لإخفاء آثارهم أو نقل أصولهم.

الحاجة إلى أطر جديدة: هناك حاجة ملحة لتطوير بروتوكولات دولية جديدة وأكثر مرونة لتبادل المعلومات المتعلقة بالبلوك تشين. قد يشمل ذلك إنشاء قنوات اتصال مباشرة بين وحدات الجرائم السيبرانية في الدول المختلفة، أو تطوير اتفاقيات تسمح بالوصول المباشر إلى بيانات العُقد الموجودة في ولايات قضائية أخرى في حالات الجرائم الخطيرة، مع وضع ضوابط صارمة لحماية حقوق الإنسان والسيادة الوطنية (Tziakouris, 2021).

في المحصلة، إن حجية الدليل المستمد من البلوك تشين ليست معطى تقنياً، بل هي بناء قانوني معقد يجب تشييده بحذر. يتطلب الأمر من القضاة أن يكونوا حراس بوابة يقظين، ومن المحققين أن يطوروا مهارات جديدة، ومن المشرعين أن يبتكروا حلولاً إجرائية تتناسب مع تحديات هذا العصر الرقمي اللامركزي.

٤. إشكالية إسناد المسؤولية الجنائية في الشبكات اللامركزية

تمهيد:

بعد أن تجاوز البحث عتبة الإثبات، وفحص كيفية تحويل البيانات المشفرة إلى دليل مقبول أمام القضاء، يواجه الآن التحدي الأكثر جوهرية وعمقاً في القانون الجنائي: إشكالية "الإسناد". فالدليل، مهما بلغت قوته، يظل عديم القيمة ما لم يتم ربطه بشكل يقيني بـ "شخص" مسؤول. إن السؤال "من الفاعل؟" هو حجر الزاوية الذي تقوم عليه فلسفة العقاب بأكملها، التي ترتكز على مبدأ "شخصية المسؤولية الجنائية.

وهنا، تصطدم المبادئ الراسخة للقانون الجنائي، التي تطورت عبر قرون في عالم مادي محكوم بالسببية المباشرة والفاعلين البشريين، بالواقع الجديد الذي تفرضه الشبكات اللامركزية. فهذه البيئة التقنية، بخصائصها الفريدة المتمثلة في اللامركزية التي تفكك السلطة، والتشفير وإخفاء الهوية اسمياً التي تحجب هوية الفاعلين، والأتمتة عبر العقود الذكية التي تفصل بين لحظة القصد ولحظة تنفيذ الفعل، تخلق "ضباباً إسنادياً" غير مسبوق.

تتجلى الإشكالية المركزية لهذا القسم في التعارض الصارخ بين الطبيعة "المشتتة" للفعل في بيئة البلوك تشين، والمتطلبات "المركزة" للإسناد في القانون الجنائي.

فالقانون يبحث عن فاعل مادي محدد، بينما تقدم له التقنية شبكة من المساهمين الموزعين. القانون يتطلب إثبات القصد الجنائي لدى شخص بعينه، والتقنية تقدم له أكواداً تعمل بشكل مستقل. هذا الصدام لا يمثل مجرد تحدٍ تقني، بل هو أزمة مفاهيمية تهدد بترك فراغ قانوني هائل، قد يؤدي إما إلى إفلات المجرمين الحقيقيين من العقاب، أو، على النقيض، إلى تجريم أطراف حسنة النية (كمطوري البرامج أو مشغلي العُقد) لمجرد أنهم جزء من البنية التحتية التقنية.

من هنا تتجلى الأهمية العلمية والعملية لهذا القسم في محاولته سد هذه الفجوة الخطيرة بين سرعة التطور التقني وبطء التطور التشريعي، فهو لا يهدف فقط إلى وصف المشكلة، بل إلى تفكيكها وتحليلها من منظور القانون الجنائي المقارن، في محاولة لتكييف النظريات الجنائية التقليدية (كالفاعل الأصلي، والشريك، والفاعل المعنوي) لتصبح قادرة على التعامل مع هذه الأنماط الجديدة من الفاعلين والأفعال.

ولتحقيق هذه الغاية، سيعتمد هذا القسم على منهج تحليلي مقارن، يستعرض النظريات الجنائية الراسخة في النظم القانونية المختلفة، ويختبر مدى صمودها وقابليتها للتطبيق في البيئة اللامركزية، مستعيناً بسيناريوهات عملية ودراسات حالات واقعية من عالم العملات المشفرة والعقود الذكية.

ينقسم هيكل هذا القسم ثلاثة أقسام فرعية متكاملة، تعالج مستويات الإسناد الثلاثة:

القسم الفرعي الأول: يتناول التحدي الأولي، وهو تحديد الفاعل المادي، ويبحث في كيفية ربط "التوقيع الرقمي" بهوية شخص طبيعي، والتغلب على حواجز إخفاء الهوية.

القسم الفرعي الثاني: يغوص في أعماق الركن المعنوي، محللاً صعوبات إثبات القصد الجنائي في سياق الأفعال التي تنفذها "العقود الذكية" بشكل آلي.

القسم الفرعي الثالث: يعالج الإشكالية الأكثر تعقيداً، وهي مدى مسؤولية الأطراف الوسيطة، مثل المطورين ومشغلي العُقد والمدققين في أنظمة "إثبات الحصة" ، متسائلاً عما إذا كانوا مجرد مقدمي خدمة محايدين أم شركاء في الجريمة.

إن الهدف النهائي لهذا القسم هو وضع لبنات نظرية أولى تسهم في بناء إطار للمسؤولية الجنائية في العصر اللامركزي، إطار يوازن بين ضرورة إنفاذ القانون ومكافحة الجريمة، وحماية حقوق الأفراد وضمان عدم معاقبة شخص على فعل لم يرتكبه أو لم يقصده.

٤,١. تحديد مرتكب الفعل المادي في بيئة البلوك تشين: من هو الفاعل في "مسرح الجريمة الخوارزمي"؟

تمهيد:

إن أول سؤال يطرحه المحقق الجنائي عند مواجهة أي جريمة هو: "من الفاعل؟". هذا السؤال يترجم قانونياً إلى البحث عن الشخص الذي أتى "الفعل المادي" المكون للجريمة. في القانون الجنائي التقليدي، الذي تطور في عالم مادي، غالباً ما يكون الفعل المادي سلوكاً إيجابياً وملموساً، ويكون إسناده إلى فاعل معين ممكناً. لكن في "مسرح الجريمة الخوارزمي" الذي توفره البلوك تشين، يصبح هذا السؤال أكثر تعقيداً. فالفعل المادي هنا هو مجرد "معاملة رقمية" مشفرة، والفاعل هو "عنوان" مجهول الهوية اسمياً. يهدف هذا القسم الفرعي إلى تفكيك هذه الإشكالية، من خلال تحليل التحديات التي تفرضها بنية البلوك تشين على مفهوم "الفاعل المادي"، ثم استعراض الأدوات القانونية والتقنية المتاحة للتغلب على هذه التحديات.

١ـ الإطار المفاهيمي: إعادة تعريف الفعل والفاعل

لفهم التحدي، يجب أولاً إعادة تعريف المفاهيم الأساسية في ضوء الواقع التقني الجديد.

الفعل المادي في البيئة اللامركزية: لم يعد الفعل المادي مجرد سلوك إنساني مباشر، بل أصبح "إيعازاً خوارزميًّا". في سياق البلوك تشين، يتمثل الفعل المادي في "إنشاء معاملة رقمية وتوقيعها بالمفتاح الخاص وبثها إلى الشبكة". هذا الفعل هو الذي يؤدي إلى النتيجة الإجرامية، سواء كانت نقل أصل مسروق أو تنفيذ عقد ذكي احتيالي. إن هذا التحول من الفعل المادي الملموس إلى الفعل الرقمي المجرد يمثل التحدي المفاهيمي الأول. (Hess & Broring, 2021)

طبيعة المعاملات المشفرة والموزعة: كل معاملة على البلوك تشين محمية بطبقتين من الإبهام: التشفير، الذي يضمن سلامة المعاملة، وإخفاء الهوية اسمياً، فلا ترتبط المعاملة بهوية حقيقية بل بـ "عنوان"

عام. يضاف إلى ذلك التوزيع، إذ يتم بث المعاملة إلى شبكة عالمية من العُقد، مما يفصل بين مكان صدور الفعل ومكان تسجيله (Finck, 2019).

الفرق بين الفاعل المادي والمعنوي: في الجرائم التقليدية، غالباً ما يتحد الفاعل المادي (من نفذ الفعل) والفاعل المعنوي (من خطط ودبر). أما في الجرائم الرقمية، وخاصة في البلوك تشين، فقد ينفصلان تماماً. قد يكون الفاعل المادي هو مجرد شخص تم استئجاره لتنفيذ المعاملة، بينما الفاعل المعنوي (العقل المدبر) يختبئ في مكان آخر. هذا الانفصال يجعل من استهداف الفاعل المادي وحده استراتيجية قاصرة.

٢ ـ التحديات القانونية: ضباب الإسناد

إن بنية البلوك تشين تخلق "ضباباً إسنادياً" يجعل من تطبيق المفاهيم التقليدية للفاعل المادي أمراً بالغ الصعوبة.

إشكالية إسناد الفعل إلى شخص طبيعي: التحدي الأكبر هو الانتقال من "العنوان" المشفر إلى "شخص" طبيعي أو اعتباري. فالتوقيع الرقمي يثبت فقط أن المعاملة صدرت عن "حائز المفتاح الخاص". لكنه لا يجيب على الأسئلة الحاسمة: من هو هذا الحائز؟ هل هو شخص واحد أم مجموعة؟ هل سرق المفتاح الخاص؟ إن القانون الجنائي يعاقب الأشخاص لا المفاتيح المشفرة، وهذه الفجوة بين الهوية الرقمية والهوية الحقيقية هي "مشكلة الإسناد الجوهرية. (Werbach, 2018)

قصور مفهوم "الفاعل الأصلي": الفاعل الرئيس أو الجاني الرئيس هو "شخص يتحكم وظيفياً في ارتكاب الجريمة". في بيئة البلوك تشين، قد تكون هذه السيطرة لا مركزية. إذ يتحكم المبرمج الذي كتب العقد الذكي ويسيطر على "منطق" الجريمة، والمستخدم الذي استدعى العقد يسيطر على "توقيت" الجريمة. هذا التشتت للسيطرة يجعل المفهوم التقليدي للجاني " الفاعل الأصلي" صعب التطبيق، وقد يتطلب اللجوء إلى نظريات المساهمة الجنائية التي يصعب إثباتها. ((Hess & Broring, 2021

تأثير تقنيات التخفي: يزداد "ضباب الإسناد" كثافة مع الاستخدام المتعمد لتقنيات مصممة خصيصاً لإخفاء أثر المعاملات، مما يحول "إخفاء الهوية اسمياً" إلى "إخفاء هوية كامل". من أبرز هذه التقنيات:

العملات الرقمية الموجهة للخصوصية: على عكس البلوك تشين الشفافة مثل بيتكوين، تستخدم عملات مثلا باستخدام تقنيات التواقيع الحلقية والعناوين الخفية أو Zcash باستخدام براهين المعرفة الصفرية بروتوكولات تشفير متقدمة لإخفاء المرسل، والمستقبل، وقيمة المعاملة. هذا يجعل تحليل السلسلة لتتبع تدفق الأموال أمراً شبه مستحيل من الناحية التقنية، مما يخلق "صندوقاً أسود" كاملاً أمام المحققين (Möser et al., 2018).

خلاطات العملات: وهي خدمات تقوم بخلط معاملات العديد من المستخدمين لقطع الصلة بين المصدر والوجهة. إن استخدام هذه الأدوات هو فعل متعمد يهدف إلى "تدمير الأدلة" الرقمية، ويثير تساؤلات حول إمكانية اعتباره بحد ذاته قرينة على القصد الجنائي (Fan et al., 2020).

٣ـ الحلول التشريعية المقترحة: تكييف القانون مع الكود

لمواجهة هذه التحديات، يجب على المشرع والقضاء تبني حلول مبتكرة.

التجارب التشريعية المقارنة: بدأت بعض الدول في التحرك. على سبيل المثال، التوجيه الخامس لمكافحة غسيل الأموال في الاتحاد الأوروبي (5AMLD) فرض على منصات تبادل العملات الرقمية ومقدمي خدمات المحافظ تطبيق إجراءات "اعرف عميلك"، مما يجبرهم على ربط العناوين الرقمية بهويات حقيقية. هذا يخلق "نقاط ربط" حيوية يمكن للمحققين استخدامها. (Tziakouris, 2021)

تطبيق نظريات المسؤولية الموسعة: بدلاً من التركيز الحصري على "الفاعل المادي"، يجب على القضاء أن يكون مستعداً لتطبيق نظريات المسؤولية الجنائية بشكل أوسع:

نظرية الفاعل المعنوي: يمكن اعتبار المبرمج الذي يصمم عقداً ذكياً خبيثاً "فاعلاً معنوياً"، والعقد الذكي هو "الأداة" غير المسؤولة التي استخدمها لارتكاب الجريمة (Mik, 2017).

المساهمة الجنائية: يمكن مساءلة الأطراف التي تقدم "مساعدة جوهرية" للجريمة، مثل مشغلي خلاطات العملات، كشركاء في الجريمة الأصلية.

دور العقود الذكية في الإسناد: يمكن تصميم العقود الذكية بحيث تتطلب من المستخدمين ربط هوياتهم الرقمية (عبر أنظمة الهوية اللامركزية قبل التفاعل معها، مما يسهل عملية التحقيق لاحقاً.

٤ـ الإثبات الجنائي: من الكود إلى الإدانة

إن إثبات هوية الفاعل المادي في بيئة البلوك تشين هو عملية تحقيقية معقدة تعتمد على تجميع الأدلة من مصادر متعددة.

تكامل الأدلة بوصفها منهجية إثبات: إن إثبات هوية الفاعل المادي في هذه البيئة المعقدة لا يمكن أن يرتكز على نوع واحد من الأدلة، بل يتطلب بالضرورة اتباع منهجية تكاملية تجمع بين مصادر الأدلة المختلفة. فلا يمكن الاعتماد على تحليل البلوك تشين وحده، بل يجب على المحققين بناء جسر إثباتي يربط بين العالمين الرقمي والمادي، من خلال دمج:

– الأدلة على السلسلة: هي بيانات خام مُستخرجة من سلسلة الكتل نفسها. يتمثل دورها الرئيس في رسم خرائط الجرائم الرقمية، أي تتبع تدفق الأصول، وتحديد العناوين المشبوهة، وكشف أنماط سلوك المعاملات. يُمكن لهذه الأدلة إثبات "ما حدث" و"كيف حدث" بفعالية على المستوى الخوارزمي.

٢ – الأدلة خارج السلسلة: (Off-Chain Evidence) وهي الأدلة التقليدية التي يتم جمعها من العالم الحقيقي. دورها الأساس هو إعطاء هوية لهذه الخريطة الرقمية؛ أي ربط العناوين المشفرة بأشخاص

حقيقيين. وتشمل هذه الأدلة سجلات منصات التبادل التي تخضع لالتزامات "اعرف عميلك" (KYC)، والبيانات المستخرجة من الأجهزة المصادرة للمشتبه بهم (مثل ملفات المحافظ والمفاتيح الخاصة)، وعناوين IP، وشهادات الشهود.

إن القضية الجنائية الناجحة في هذا المجال هي تلك التي تنجح في نسج قصة متماسكة من هذين النوعين من الأدلة، إذ يدعم كل منهما الآخر. فالدليل "على السلسلة" يقود المحققين إلى الدليل "خارج السلسلة" (مثلاً، تتبع الأموال إلى منصة تبادل)، والدليل "خارج السلسلة" يفسر ويعطي معنى للدليل "على السلسلة" (مثلاً، سجلات المنصة تثبت أن المتهم هو صاحب العنوان الذي تلقى الأموال).

الأدلة على السلسلة: تحليل تدفق المعاملات وتجميع العناوين حتى تصل إلى منصة تبادل معروفة.

الأدلة خارج السلسلة: استخدام وسائل التحقيق التقليدية، مثل الحصول على سجلات منصات التبادل، تحليل الأجهزة المصادرة للمشتبه به للعثور على المفاتيح الخاصة، وتتبع عناوين IP (Casey & Lundy, 2021).

الدور الحاسم للخبراء التقنيين: يصبح الخبير في تحليل البلوك تشين "شاهد الإثبات" الرئيس. وتتجه المحاكم، كما في قضية U.S. v. Gratkowski، إلى قبول شهادة الخبراء الذين يستخدمون أدوات تحليل متخصصة (مثل Chainalysis) بوصفه دليلا مقبولا، بشرط أن يتمكن الخبير من شرح منهجيته بوضوح (Sheyn, 2018).

معيار الإثبات: على الرغم من الطبيعة الرقمية للجريمة، يبقى معيار الإثبات "بما لا يدع مجالاً للشك المعقول". لا يكفي أن يُثبت المدعي العام أن المدعى عليه "قد" يتحكم في العنوان؛ بل يجب عليه تقديم سلسلة من الأدلة المترابطة التي تستبعد أي فرضية بديلة معقولة.

الخلاصة:

يُمثل تحديد هوية المجرمين الفعليين في بيئة سلسلة الكتل تحديًا كبيرًا، ولكنه ليس مستحيلًا. يتطلب هذا تحولًا في التفكير القانوني من البحث عن "بصمات" مادية إلى تتبع "آثار" رقمية. يُعدّ إنجاز هذه المهمة بنجاح أمرًا بالغ الأهمية لضمان عدم تحول عالم سلسلة الكتل اللامركزي إلى ملاذ للجريمة.

٤,٢. إثبات القصد الجنائي لدى الأطراف المتعددة.

تمهيد

إذا كان القسم الفرعي السابق قد نجح في تحديد "من" ضغط على الزناد الرقمي، فإن هذا القسم الفرعي يواجه السؤال الأكثر عمقاً وإشكالية: "لماذا؟" وماذا كان يدور في ذهنه؟ إن القانون الجنائي لا يعاقب على مجرد الأفعال المادية، بل على الأفعال التي تصدر عن "إرادة آثمة" (سرور، ٢٠١٥، ص ٦٤٦). هذا المكون النفسي، المعروف بالركن المعنوي أو القصد الجنائي، هو الذي يميز بين المجرم البريء، وبين القاتل العمد والمصاب بالخطأ، وبين المحتال والمخطئ في الحساب (عوض، ٢٠٠٠، ص ٢١١). إنه "روح الجريمة" التي بدونها يظل الفعل مجرد جسد مادي لا قيمة جنائية له.

في البيئة التقليدية، يستدل القاضي على القصد الجنائي من خلال الظروف المحيطة بالفعل، وأقوال الشهود، وسلوك الجاني قبل وبعد الجريمة. لكن في بيئة البلوك تشين، تنهار العديد من هذه القرائن التقليدية. فنحن أمام فاعلين مجهولي الهوية اسمياً، وأفعال تتم عبر أتمتة العقود الذكية، ومساهمات موزعة من أطراف متعددة قد لا يعرف بعضهم بعضاً. كيف يمكن إثبات "العلم والإرادة" في عالم من الأكواد الصماء والفاعلين المحجوبين؟

إن هذا القسم الفرعي سيقوم بتشريح هذه الإشكالية المعقدة. سنبدأ بتحليل صعوبة إثبات القصد الجنائي لدى الفاعل المباشر الذي يبدأ المعاملة، ثم ننتقل إلى التحدي الأكبر وهو البحث عن القصد الجنائي لدى الأطراف الوسيطة التي تشكل البنية التحتية للجريمة، كالمطورين ومشغلي العُقد، سواء كانوا أفراداً أم كيانات اعتبارية.

٤,٢,١. إثبات القصد الجنائي لدى الفاعل المباشر: من النية المسبقة إلى التنفيذ الآلي

الفاعل المباشر: هو الشخص الذي يقوم بإنشاء المعاملة الإجرامية وتوقيعها بمفتاحه الخاص، مما يؤدي إلى تفعيل الجريمة، ومن ثم فإن العنصر الجوهري للقصد المباشر هو الإرادة التي اتجهت على نحو أكيد يقيني إلى الاعتداء على الحق الذي يحميه القانون (حسني، ١٩٨٨، ص ١٩٦). على الرغم من أن تحديد هذا الشخص (كما رأينا في القسم الفرعي السابق) هو تحدٍ بحد ذاته، إلا أن إثبات قصده الجنائي يطرح مجموعة مختلفة من الصعوبات، خاصة في ظل وجود العقود الذكية.

أولاً: فجوة "الزمان والمكان" بين القصد والفعل

في الجرائم التقليدية، غالباً ما يكون هناك تزامن بين لحظة تكوين القصد ولحظة تنفيذ الفعل (وزير، ٢٠٠٣، ص ٢٧٣). أما في عالم العقود الذكية، فقد يكون هناك فاصل زمني ومكاني كبير بينهما.

النية المسبقة: قد يقوم المبرمج بتصميم عقد ذكي احتيالي (مثلاً، عقد مصمم لسرقة الأموال عند استيفاء شرط معين) ونشره على البلوك تشين. هنا، يتكون القصد الجنائي (العلم والإرادة) في لحظة كتابة الكود ونشره.

التنفيذ الآلي: قد لا يتم تنفيذ الفعل الإجرامي إلا بعد أشهر أو سنوات، عندما يقوم ضحية ما بالتفاعل مع العقد، مما يؤدي إلى تفعيل النتيجة الإجرامية تلقائياً.

هذه الفجوة الزمنية تثير تساؤلات حول استمرارية القصد الجنائي. هل يمكن للمتهم أن يدفع بأنه قد "عدل" عن قصده بعد نشر الكود؟ في معظم النظم الجنائية، لا يعتد بالعدول الاختياري إلا إذا حال دون وقوع النتيجة. وبما أن العقد الذكي، بمجرد نشره على بلوك تشين ثابتة، لا يمكن إيقافه أو تعديله، فإن نية المبرمج وقت النشر تعتبر "مجمدة" داخل الكود، ويصبح العقد الذكي امتداداً لإرادته الإجرامية عبر الزمن. إن الكود هنا يصبح تجسيداً مادياً للقصد الجنائي المسبق (Mik, 2017).

ثانياً: استخلاص القصد من الأدلة الظرفية

بما أنه من المستحيل الدخول إلى عقل المتهم، فإن إثبات القصد الجنائي يعتمد دائماً على استخلاصه من الأدلة الظرفية (وزير، ١٩٨٩، ص١٣٤). في سياق البلوك تشين، يمكن تقسيم هذه الأدلة إلى نوعين:

طبيعة الكود نفسه بوصفه دليلا على القصد: إن فحص الكود المصدري للعقد الذكي هو أقوى دليل موضوعي على نية مصممه. فإذا كان الكود مصمماً بطريقة لا يمكن أن تؤدي وظيفياً إلا إلى نتيجة إجرامية (مثل عقد ذكي مصمم لتشغيل مخطط بونزي ينهار حتماً، أو عقد يسرق الأموال تلقائياً عند استيفاء شرط معين)، فإن القول بغياب القصد الجنائي يصبح ضرباً من الخيال. في هذه الحالة، يتجاوز الكود كونه مجرد "أداة" محايدة ليصبح هو نفسه تجسيداً وتوثيقاً للإرادة الإجرامية. يمكن القول إن الكود هنا "يعترف" بنية صاحبه، إذ إن القصد الجنائي يكون "مدمجاً في التصميم" (DuPont, 2017).

تاريخ المعاملات: يمكن لتحليل معاملات المتهم السابقة أن يكشف عن نمط سلوكي إجرامي متكرر، مما يدعم وجود القصد في الجريمة الحالية.

الأدلة خارج السلسلة:

الاتصالات الرقمية: الرسائل على تطبيقات الدردشة المشفرة، أو رسائل البريد الإلكتروني، أو المنشورات على المنتديات في الإنترنت المظلم، التي يناقش فيها المتهم خطته الإجرامية، تعد دليلاً مباشراً على قصده.

سلوك ما بعد الجريمة: محاولات المتهم غسل الأموال المتحصلة من الجريمة باستخدام "خلاطات العملات"، أو تحويلها بسرعة عبر عناوين متعددة، تعتبر قرينة قوية على علمه بالطبيعة غير المشروعة لأفعاله.

خبرة المتهم: إذا كان المتهم خبيراً تقنياً معروفاً، فمن الصعب عليه أن يدعي أنه "لم يفهم" ما سيفعله الكود الذي كتبه أو تفاعل معه.

إن تجميع هذه الأدلة الظرفية خارج السلسلة وربطها بالأدلة الفنية على السلسلة هو ما يسمح للادعاء العام ببناء حجة متماسكة حول القصد الجنائي للمتهم (Choo, 2020).

ثالثاً: الدفع بـ "الجهل بالكود" ومواجهته بنظرية "اللامبالاة المتعمدة"

أحد الدفوع المحتملة من قبل المستخدم (وليس المبرمج) هو الدفع بالجهل أو الغلط (محمود، ١٩٦٧)، أي أنه تفاعل مع عقد ذكي دون أن يفهم تماماً طبيعته الإجرامية.

الدفع بالجهل (علام، ١٩٨٤): قد يدعي المستخدم أنه ضغط على زر "تأكيد المعاملة" دون قراءة الكود المعقد أو فهم عواقبه.

مواجهة الدفع: يمكن للادعاء العام مواجهة هذا الدفع من خلال تطبيق نظريات القصد الجنائي غير المباشر، وأهمها "اللامبالاة المتعمدة" أو "العمى المتعمد"، والمعروفة في بعض النظم اللاتينية بـ Dolus Eventualis. تقوم هذه النظرية على أن الشخص يعتبر قاصداً جنائياً ليس فقط إذا أراد النتيجة، بل أيضاً إذا توقع احتمال وقوعها ورضي بها أو قبل المخاطرة بحدوثها.

يمكن تطبيق هذه النظرية إذا أثبت الادعاء أن المتهم:

كان على علم بوجود "مخاطر عالية" مرتبطة بتفاعله (مثلاً، التفاعل مع عقد ذكي موجود على منصة معروفة بالاحتيال).

اتخذ خطوات متعمدة لتجنب التأكد من حقيقة الأمر (مثلاً، عدم طرح أي أسئلة أو عدم قراءة أي تحذيرات).

في هذه الحالة، فإن "جهل" المتهم ليس جهلاً بريئاً، بل هو "جهل اختياري" يمكن معادلته قانونياً بالعلم، مما يسمح بإثبات القصد الجنائي (Kingston, 2021).

٤,٢,٢. إثبات القصد الجنائي لدى الأطراف الوسيطة: من المساهمة إلى المسؤولية الموضوعية

إن التحدي الأكبر لا يكمن في إثبات قصد الفاعل المباشر، بل في تحديد المسؤولية الجنائية للأطراف التي تشكل البنية التحتية التي مكنت من وقوع الجريمة. هؤلاء الوسطاء (المطورون، مشغلو العُقد، منصات التبادل) غالباً ما يدفعون بأنهم مجرد "أدوات محايدة" أو "مقدمي خدمة"، وأنهم لا يملكون القصد الجنائي اللازم للإدانة. هنا، يجب على القانون الجنائي أن يوازن بدقة بين حماية الابتكار التقني ومنع توفير ملاذات آمنة للجريمة.

أولاً: مسؤولية المطور

هل المطور الذي يكتب كوداً يمكن استخدامه في أغراض إجرامية يعتبر شريكاً في الجريمة؟ الإجابة تعتمد على طبيعة الكود ودرجة حياديته.

الكود ذو الاستخدام المزدوج: إذا قام مطور بإنشاء بروتوكول بلوك تشين عام (مثل إيثيريوم) أو عقد ذكي معياري (مثل عقد ERC-20 لإنشاء التوكنات)، فإن هذا الكود يعتبر محايداً ويمكن استخدامه لأغراض مشروعة وغير مشروعة. هنا، من شبه المستحيل إثبات القصد الجنائي لدى المطور. فمسؤوليته تشبه مسؤولية صانع السيارات الذي لا يسأل عن استخدام سيارته في عملية سطو. إن تحميل المطورين

المسؤولية في هذه الحالة سيؤدي إلى "أثر مبرد" – هو تثبيط أو منع الأفراد والشركات عن ممارسة سلوك مشروع (مثل التعبير عن الرأي، أو البحث العلمي، أو الابتكار التقني) خوفاً من الملاحقة القانونية أو العقوبات المحتملة– على الابتكار التقني (Levy, 2017).

الكود المصمم للجريمة: الوضع يختلف تماماً إذا كان الكود مصمماً بشكل أساس أو حصري لارتكاب الجرائم. على سبيل المثال:

– مبرمج يقوم بتصميم وتوزيع عقد ذكي لا وظيفة له سوى إدارة "مخطط بونزي"– مخطط بونزي هو عملية احتيال استثمارية تعد المستثمرين بعوائد ضخمة جداً ومضمونة في فترة قصيرة، وبمخاطر قليلة أو منعدمة.

– مبرمج يقوم بإنشاء "خلاط عملات" ويقوم بتسويقه بشكل علني على أنه أداة لغسيل الأموال وتجنب الرقابة.

في هذه الحالات، يمكن القول إن القصد الجنائي "مدمج" في تصميم الكود نفسه. لم يعد المطور مجرد صانع أداة محايدة، بل أصبح "مساهماً" أو "شريكاً" من خلال توفير "المساعدة الجوهرية" للجريمة، مع علمه الكامل بأن أداته ستستخدم لهذا الغرض. يمكن إثبات قصده من خلال تصميم الكود، وطريقة تسويقه، والمجتمعات التي ينشط فيها. (Hess & Broring, 2021)

ثانياً: مسؤولية مشغل العقدة أو المُعدِّن

مشغلو العُقد هم العمود الفقري للشبكة، فهم الذين يقومون بالتحقق من صحة المعاملات وإضافتها إلى السجل. هل يمكن مساءلتهم عن محتوى المعاملات التي يقومون بمعالجتها؟

الدفع بـ "الناقل المحايد": الحجة الأساسية للدفاع عنهم هي أنهم يعملون بصفتهم "ناقلين محايدين" للبيانات، على غرار مزودي خدمة الإنترنت. فهم يعالجون آلاف المعاملات المشفرة في الثانية، وليس لديهم القدرة العملية أو التقنية على فحص محتوى كل معاملة وتحديد ما إذا كانت إجرامية أم لا. في معظم الحالات، يكون هذا الدفع صحيحاً، ومن الصعب إثبات أي قصد جنائي لديهم.

حدود الدفع: العلم والرقابة: هذا الدفع يبدأ في الانهيار عندما يكتسب مشغل العقدة (خاصة في تجمعات التعدين الكبيرة – علماً فعلياً" بأن شبكته تستخدم بشكل منهجي لتسهيل أنشطة إجرامية محددة، أو عندما تتاح له القدرة على "الرقابة" أو تصفية المعاملات ولكنه يختار عدم القيام بذلك. على سبيل المثال، إذا تم إخطار تجمع تعدين بأن عناوين معينة مرتبطة بمنظمة إرهابية أو ببرنامج فدية، واستمر في معالجة معاملاتها عن عمد، فإن إثبات "اللامبالاة المتعمدة" أو "التواطؤ" يصبح ممكناً. هذا يفتح الباب لمساءلتهم ليس بصفتهم فاعلين أصليين، بل بصفتهم مساهمين في جرائم مثل غسيل الأموال أو تمويل الإرهاب (Walch, 2019).

ثالثاً: مسؤولية الشخص المعنوي

العديد من الأطراف الوسيطة (كمنصات التبادل، والشركات المطورة للبروتوكولات) هي كيانات اعتبارية. كيف يمكن إسناد "قصد جنائي" لشركة؟

نظريات الإسناد التقليدية: يمكن تطبيق النظريات التقليدية لمسؤولية الشخص المعنوي:

يمكن مواجهة مسؤولية الكيانات الاعتبارية في بيئة البلوك تشين من خلال تطبيق النظريات التقليدية للمسؤولية الجنائية للشركات، وأبرزها:

نظرية "العقل المدبر والإرادة الموجهة":

هذه النظرية، المُرسخة في القانون العام، تُنسب القصد الجنائي إلى الشركة إذا ارتُكب الفعل أو القرار الإجرامي من قِبَل شخص يُمثل "العقل المدبر والإرادة المُوجِّهة" للشركة. لا يشمل هذا أي موظفين، بل يقتصر على كبار المسؤولين الذين يُجسِّدون مركز التحكم في الشركة (مثل مجلس الإدارة أو الإدارة العليا). على سبيل المثال، إذا تجاهل مجلس إدارة منصة تداول عملات رقمية عمدًا تطبيق متطلبات مكافحة غسل الأموال بهدف جذب المزيد من العملاء، فإن القصد الجنائي يُنسب مباشرةً إلى الشركة نفسها، مما يجعلها "مرتكبة" الجريمة، وليست مجرد طرف مسؤول مدنيًا . (Wells, 2021).

نظرية المسؤولية التبعية: تُستخدم هذه النظرية على نطاق واسع في الولايات المتحدة، وطريقة تطبيقها أكثر صرامة. وفقًا لهذه النظرية، تكون الشركة مسؤولة جنائيًا عن الأفعال الإجرامية لموظفيها (حتى الموظفين من المستوى الأدنى) طالما أن موظفيها (حتى الموظفين من المستوى الأدنى) يرتكبون جرائم في نطاق عملهم وكان هدفهم هو جلب فوائد للشركة، حتى لو كانت الفائدة محتملة فقط. (Fisse & Braithwaite, 1993).

نظرية "الثقافة المؤسسية": وهي نظرية أكثر حداثة، ترى أن القصد الجنائي يمكن أن يستخلص من "الثقافة المؤسسية" للشركة. إذا كانت سياسات الشركة وإجراءاتها وهياكلها الداخلية تشجع أو تتسامح مع السلوك الإجرامي، فيمكن اعتبار الشركة نفسها "مذنبة". على سبيل المثال، شركة تطور برامج تحليل بلوك تشين وتبيعها لأجهزة إنفاذ القانون، وفي نفس الوقت تدير سراً خدمة "خلاط عملات" للعملاء في الإنترنت المظلم. هذه "الثقافة المزدوجة" يمكن أن تكون دليلاً قوياً على القصد الجنائي المؤسسي (Dine & Koutsias, 2020).

٤,٣. مدى مسؤولية الأطراف الوسيطة من حيادية الكود إلى التواطؤ الجنائي (مطور البروتوكول، مشغل العقدة، منصة التبادل).

تمهيد:

بعد تفكيك إشكاليات تحديد الفاعل المباشر وإثبات قصده الجنائي، يصل البحث إلى المنطقة الأكثر ضبابية وخطورة في القانون الجنائي الرقمي: مسؤولية الأطراف الوسيطة. هؤلاء الفاعلون – مطورو البروتوكولات، ومشغلو العُقد، ومنصات التبادل – لا يرتكبون الجريمة النهائية بأنفسهم، لكنهم يشكلون البنية التحتية التي تجعلها ممكنة. إنهم يقفون في منطقة رمادية بين تقديم خدمة تقنية محايدة، وتسهيل النشاط الإجرامي عن علم أو إهمال.

إن السؤال المركزي الذي يطرحه هذا القسم الفرعي الثالث هو: متى يتجاوز الوسيط التقني خط "الحيادية" ليقع في دائرة "التجريم"؟ إن الإجابة على هذا السؤال لها عواقب وخيمة. فالتوسع المفرط في المسؤولية قد يؤدي إلى "أثر مبرد" يخنق الابتكار، بينما يؤدي التضييق المفرط إلى خلق "ملاذات آمنة" للجريمة المنظمة. يهدف هذا القسم الفرعي إلى تحليل هذا التوازن الدقيق، من خلال فحص المسؤولية الجنائية على مستويين: المسؤولية الفردية للأشخاص الطبيعيين، ومسؤولية الكيانات الاعتبارية التي تقف خلف هذه الخدمات.

١ ـ الإطار المفاهيمي: تحديد طبيعة الوساطة في البيئة اللامركزية

قبل الخوض في تحليل المسؤولية، لا بد من تحديد الأطراف الوسيطة وتصنيفها قانونياً.

مطورو البروتوكولات: هم المعماريون الذين يصممون القواعد الأساسية للشبكة (مثل مطوري بيتكوين أو إيثيريوم) أو يكتبون كود العقود الذكية.

مشغلو العقد:

هم العمود الفقري للشبكة اللامركزية، ويقومون بتشغيل البرامج التي تحافظ على سلامة السجل وتنميته. وظيفتهم الحيوية هي المشاركة في "آلية الإجماع" للتحقق من صحة المعاملات الجديدة وتجميعها في كتل وإضافتها إلى السلسلة. يُعرف هؤلاء الفاعلون بأسماء مختلفة اعتماداً على آلية الإجماع المستخدمة:

في أنظمة "إثبات العمل" مثل بيتكوين، يُطلق عليهم "المُعدِّنون"، حيث يتنافسون باستخدام القوة الحاسوبية لحل لغز رياضي والفوز بالحق في إضافة الكتلة التالية.

في أنظمة "إثبات الحصة" (مثل إيثيريوم ٢.٠، يُطلق عليهم "المدققون" (، إذ يتم اختيارهم لإنشاء الكتلة التالية بناءً على كمية العملة التي قاموا بحجزها كضمان ("حصة").

لذا، عندما نقول "مشغلو العقد (المُعدِّنون أو المدققون)"، فإننا نشير إلى الكيان الذي يقوم بالوظيفة الحيوية لتأمين الشبكة، والفرق الجوهري بين المصطلحين يكمن في الوسيلة التي يتم بها تحقيق هذا الأمن:

إما من خلال استثمار "العمل" (القوة الحاسوبية) أو استثمار "رأس المال" (الحصة) (De Filippi & Wright, 2018).

منصات التبادل: هي البوابات التي تربط عالم البلوك تشين بالنظام المالي التقليدي، سواء كانت مركزية (CEX) أو لا مركزية (DEX).

إن طبيعة العلاقة القانونية بين هذه الأطراف والمستخدمين هي مسألة معقدة. فهي تتجاوز المفهوم التعاقدي اليسير لتشكل نوعاً جديداً من "بنية الثقة"، فيضع المستخدمون ثقتهم ليس في شخص، بل في سلامة الكود الذي يقدمه المطور وفي حيادية الشبكة التي يديرها مشغلو العقد. هذا الفهم الجديد للعلاقة يفتح الباب أمام فرض "واجبات عناية" قد تترتب عليها مسؤولية جنائية في حالة الإخلال الجسيم بها. (Werbach, 2018)

٢ ـ المسؤولية الجنائية الفردية (الفرع الأول): البحث عن الشريك في الشبكة

من الصعب تكييف المطور بوصفه ـ "فاعلا أصليا" إلا في حالة واحدة: عندما يقوم المطور نفسه بتصميم ونشر وتشغيل تطبيق لا مركزي (dApp) مصمم خصيصاً لارتكاب جريمة. أما في حالة مطوري البروتوكولات العامة، فإنهم يشبهون صانع الطرق الذي لا يسأل عن الجرائم التي تقع على الطريق الذي بناه.

تصبح الصورة أكثر تعقيداً عند بحث مسؤولية المطور أو مشغل العقدة كـ "شريك". تتطلب **معظم النظم القانونية لتطبيق مسؤولية الشريك توافر ركنين**: (**إبراهيم**، ٢٠١٢)

الركن المادي (**فعل المساعدة**): هل كتابة كود محايد يمكن استخدامه في الجريمة يعتبر "مساعدة"؟ الاتجاه الحديث، خاصة في جرائم التكنولوجيا، يميل إلى اعتبار توفير "الأداة الأساسية" للجريمة، مع العلم باستخدامها المحتمل، شكلاً من أشكال المساعدة الجوهرية.

الركن المعنوي (**القصد الجنائي**): وهذا هو التحدي الأكبر. يجب إثبات أن المطور أو مشغل العقدة كان لديه "قصد جنائي" مزدوج: (١) العلم بأن فعله سيساعد في ارتكاب جريمة، و(٢) إرادة تحقيق هذه المساعدة.

القصد المباشر: يصعب إثباته إلا في حالات واضحة، مثل مطور "خلاط عملات" الذي يسوق لخدمته على أنها وسيلة لغسيل الأموال.

القصد غير المباشر أو الاحتمالي: هذا هو الميدان الأكثر خصوبة للمساءلة. يمكن مساءلة الوسيط إذا ثبت أنه توقع بدرجة عالية من الاحتمال أن خدمته ستستخدم لارتكاب جرائم، وعلى الرغم من ذلك قبل هذه المخاطرة. يمكن الاستدلال على هذا القصد من خلال:

ـ **تصميم الخدمة**: هل تم تصميمها مع تجاهل متعمد لأي ضوابط أمنية؟

ـ **نموذج العمل**: هل يعتمد نموذج الربح على تشجيع الاستخدام غير القانوني؟

- **المعرفة الفعلية**: هل بُلغ الوسيط مرارا وتكرارا بأن منصته تستخدم من قبل مجرمين، لكنه لم يتخذ أي إجراء؟ (Hess & Broring, 2021)

أرست قضيةU.S. v. Sterlingov ، التي أدت إلى إدانة مشغل خدمة بتكوين، سابقة قضائية مهمة، حيث اعتمدت هيئة المحلفين على أدلة ظرفية قوية (مثل الإعلانات على الويب المظلم ونصائح للمستخدمين حول كيفية تجنب الكشف) لإثبات أن المشغل كان على دراية تامة بالطبيعة الإجرامية لاستخدام منصته وأنه سهل ذلك عمدا.

٣ ـ مسؤولية الشخص المعنوي (الفرع الثاني): مساءلة الشركات في العالم اللامركزي

يمكن تطبيق نظريات مسؤولية الشخص المعنوي التقليدية بسهولة على "منصات التبادل المركزية" (CEXs) والشركات المطورة للبرمجيات. مثل: نظرية "العقل المدبر" إذا قرر مجلس إدارة منصة تبادل التغاضي عمداً عن متطلبات مكافحة غسيل الأموال، فإن هذا القصد ينسب مباشرة للشركة (Wells, 2021) ، ونظرية المسؤولية بالنيابة: إذا قام موظف في منصة تبادل بمساعدة عميل على غسل الأموال، يمكن مساءلة الشركة جنائياً حتى لو كانت سياساتها الرسمية تمنع ذلك.

المنظمات المستقلة اللامركزية (DAOs) تمثل التحدي الأقصى للمسؤولية الجنائية، إذ يرى بعض الفقهاء أن محاولة تطبيق قواعد مسؤولية الشركات عليها أصبح مستحيلا، غير إن الاتجاهات الحديثة تقترح نماذج بديلة:

نظرية الشراكة غير المسجلة: يمكن معاملة أعضاء DAO (حملة التوكنات المصوتين) بصفتهم شركاء في شراكة غير مسجلة، وبالتالي يكونون مسؤولين بالتضامن عن قرارات المنظمة.

نظرية "ثقب الحجاب اللامركزي": يقترح هذا النموذج البحث عن "المسيطرين الفعليين" داخل المنظمة، حتى لو كانت لا مركزية ظاهرياً، ومساءلتهم. قد يكون هؤلاء هم المطورون الأصليون أو حاملو النسبة الأكبر من توكنات الحوكمة. (Kaal, 2020)

هل يمكن مساءلة شركة تطوير برمجيات جنائياً إذا أدت ثغرة أمنية في عقد ذكي صممته إلى سرقة أموال المستخدمين؟ في معظم الحالات، تقع هذه المسألة في نطاق المسؤولية المدنية. لكن يمكن تصور المسؤولية الجنائية في حالة "الإهمال الجسيم"، إذا ثبت أن الشركة تجاهلت بشكل صارخ ومتهور معايير الأمان الأساسية، أو تم تحذيرها من وجود ثغرة خطيرة ولم تقم بإصلاحها، مما أدى إلى كارثة مالية واسعة النطاق (Levy, 2017).

٤ ـ الإشكاليات القانونية: الفوضى التنظيمية

تنازع القوانين: أي قانون وطني ينطبق على عقد ذكي يعمل على شبكة عالمية؟ غياب قواعد واضحة يخلق حالة من الفوضى.

صعوبة تحديد الاختصاص القضائي: تفشل نظريات الاختصاص التقليدية. يقترح بعض الفقهاء تبني "مبدأ الأثر"، فينعقد الاختصاص للدولة التي ظهر فيها الأثر الضار للجريمة. لكن هذا قد يؤدي إلى تعدد الاختصاصات بشكل غير عملي. الحل قد يكمن في تطوير نظريات جديدة للاختصاص ترتكز على "الوجود الرقمي المستهدف" أو "السيطرة على الشبكة". (Tziakouris, 2021)

إشكالات الإثبات: كما تم تحليله سابقاً، فإن إثبات الركن المادي والمعنوي في هذه البيئة يتطلب **أدوات تحقيقية وخبرات فنية متقدمة**.

٥ ـ الحلول المقترحة: نحو تنظيم ذكي

تعديلات تشريعية: يجب على المشرع أن يتدخل بنصوص واضحة تجرم "إنشاء وتوفير أدوات تقنية بهدف أساس هو ارتكاب الجرائم".

إنشاء هيئات رقابية متخصصة: بدلاً من محاولة إخضاع هذه التقنيات للهيئات الرقابية التقليدية، يجب إنشاء هيئات جديدة تتمتع بالخبرة التقنية. يمكن تطبيق "بيئات الاختبار التنظيمية" للسماح بالابتكار تحت الإشراف.

تطوير آليات التعاون الدولي: من الضروري التغلب على بطء تنفيذ اتفاقيات المساعدة القانونية المتبادلة، وتنفيذ توصية فرقة العمل المعنية بالإجراءات المالية (FATF) بشأن التبادل الفوري لمعلومات الأصول الافتراضية بين الدول. (FATF, 2021)

٦ – الخاتمة: الموازنة بين الابتكار والمساءلة

تُعدّ مسؤولية الوسطاء من أكثر القضايا القانونية تعقيدًا. ويخلص هذا التحليل إلى أن الحل لا يكمن في التطبيق العشوائي للقواعد التقليدية، ولا في منح الوسطاء التكنولوجيين حصانة مطلقة.

النتائج الرئيسة:

– تعتمد مسؤولية المطورين بشكل أساس على درجة حياد الكود الذي يكتبونه.

– غالبًا ما يتطلب إثبات النية الإجرامية للوسطاء اللجوء إلى نظرية القصد الاحتمالي.

– تتطلب أنظمة التشغيل اللامركزية (DAOs) إطارًا قانونيًّا جديدًا للمساءلة.

التوصيات التشريعية:

– وضع تشريعات محددة للجرائم المتعلقة بالأنظمة اللامركزية.

– تعديل قانون الإجراءات الجنائية لتوضيح قواعد عمليات البحث والمصادرة الرقمية عبر الحدود.

– تبني نموذج تنظيمي مرن يعتمد على مبدأ "نفس المخاطر، نفس القواعد".

رؤية مستقبلية:

إن المستقبل يكمن في "التنظيم المدمج في التصميم"، إذ يتم تشجيع المطورين على دمج ضوابط الامتثال في بروتوكولاتهم منذ البداية. إن الهدف ليس خنق الابتكار، بل توجيهه نحو مسار يضمن أن تكون ثورة البلوك تشين ثورة آمنة ومسؤولة.

٥. إشكالية الولاية القضائية الجنائية على الجرائم المرتبطة بالبلوك تشين

تمهيد

بعد أن تناول البحث إشكاليتي الإثبات والمسؤولية، يصل الآن إلى الحلقة الأخيرة، الأكثر تعقيداً في سلسلة العدالة الجنائية: إشكالية "الولاية القضائية" ". فبدون تحديد محكمة مختصة للنظر في الدعوى، يظل الحق في العقاب مجرد حبر على ورق، ويظل المجرم بمنأى عن يد العدالة. إن الولاية القضائية هي التي تمنح الدولة "سلطة القول بالقانون" ، وهي تجسيد لسيادتها على إقليمها ورعاياها.

لكن هذه المفاهيم، التي صيغت وتطورت في عالم جيوسياسي مقسم إلى دول ذات حدود واضحة، تجد نفسها اليوم في مواجهة واقع تقني جديد يتحدى هذه التقسيمات بشكل جذري. فجرائم البلوك تشين، بطبيعتها اللامركزية والعابرة للحدود، لا تقع في "مكان" محدد. فالفعل الإجرامي قد يبدأ في دولة، وتنفذه "عقدة" (Node) في دولة ثانية، وتظهر نتيجته في دولة ثالثة، بينما يختبئ الفاعل في دولة رابعة. هذا "التفتت الجغرافي" للجريمة يخلق "أزمة مكانية" للقانون الإجرائي، ويجعل من تحديد المحكمة المختصة مهمة أشبه بالبحث عن نقطة ثابتة في عالم سائل.

تتجلى الإشكالية المركزية لهذا القسم في الصدام الحتمي بين الطبيعة العالمية واللامركزية لتقنية البلوك تشين، والطبيعة الإقليمية والممركزة لمفهوم الولاية القضائية الجنائية. إن غياب قواعد واضحة ومتفق عليها لتحديد الاختصاص في هذا الفضاء الجديد يؤدي إلى عواقب وخيمة، أهمها: "التنازع السلبي للاختصاص"، فتتقاعس كل دولة عن ملاحقة الجريمة بحجة عدم اختصاصها، مما يخلق "ملاذات آمنة" للمجرمين الرقميين، أو "التنازع الإيجابي للاختصاص"، إذ تدعي عدة دول اختصاصها، مما يؤدي إلى فوضى قانونية وانتهاك لمبدأ "عدم جواز المحاكمة عن ذات الفعل مرتين" .

من هنا، تتجلى أهمية هذا القسم في محاولته استكشاف حلول لهذه الأزمة. ولتحقيق هذه الغاية، سيعتمد هذا القسم على منهج تحليلي مقارن، يدرس النماذج القانونية المختلفة للولاية القضائية ويختبر مدى قدرتها على التكيف مع الواقع اللامركزي.

ينقسم هيكل هذا القسم إلى ثلاثة أقسام فرعية متكاملة، تتبع مساراً منطقياً من تشخيص المشكلة إلى اقتراح الحلول:

القسم الفرعي الأول: يبدأ بتشخيص المشكلة من خلال تحليل قصور المعايير التقليدية للاختصاص القضائي (الإقليمي، الشخصي، العيني)، وبيان كيف تفشل هذه المعايير في الإحاطة بجميع أبعاد الجريمة اللامركزية.

القسم الفرعي الثاني: ينتقل إلى استعراض الحلول المقترحة، من خلال بحث الحاجة إلى تبني معايير حديثة وأكثر مرونة، وعلى رأسها "معيار الأثر" (Effects Doctrine)، الذي يمنح الاختصاص للدولة التي يظهر فيها الأثر الضار للجريمة.

القسم الفرعي الثالث: يعالج الجانب العملي، متناولاً التحديات التي تواجه التعاون الدولي في التحقيق والملاحقة، حتى بعد تحديد الاختصاص، وضرورة تطوير آليات جديدة تتناسب مع سرعة الجريمة الرقمية.

إن الهدف النهائي لهذا القسم هو تجاوز مرحلة وصف المشكلة، وتقديم مساهمة نظرية وعملية تهدف إلى اقتراح حلول متوازنة لتحديد الاختصاص القضائي، حلول تضمن فعالية العدالة الجنائية في الفضاء الرقمي، دون أن تؤدي إلى توسع غير منضبط في سلطات الدول على حساب السيادة وحقوق الأفراد.

٥,١. قصور معايير الاختصاص التقليدية في مواجهة الجريمة اللامركزية

تمهيد:

إن منظومة القانون الجنائي الدولي، في سعيها لتوزيع سلطة العقاب بين الدول، قد استقرت تاريخياً على مجموعة من المبادئ أو "معايير الربط" التي تبرر انعقاد الولاية القضائية لدولة معينة. هذه المبادئ، التي تشكل أساس السيادة الجنائية، تم نحتها وصقلها في عالم مادي، حيث الأفعال والأشخاص والأضرار لها وجود جغرافي واضح ويمكن تحديد موقعها. لكن ظهور جرائم البلوك تشين، بطبيعتها المجردة والمشتتة واللامكانية، قد ألقى بظلال من الشك على كفاية هذه المعايير التقليدية، وكشف عن قصور بنيوي في قدرتها على الإحاطة بهذه الظاهرة الإجرامية الجديدة. يهدف هذا القسم الفرعي إلى إجراء تشريح قانوني دقيق لهذه المعايير التقليدية – الإقليمي، والشخصي، والعيني – لبيان كيف أن كل واحد منها، على الرغم من أهميته التاريخية، يصبح عاجزاً أو غير كافٍ عند محاولة تطبيقه على الجرائم المرتكبة عبر الشبكات اللامركزية.

٥,١,١. مبدأ الاختصاص الإقليمي: أزمة "المكان" في عالم بلا حدود

يُعتبر مبدأ الاختصاص الإقليمي هو "حجر الزاوية" في بناء الولاية القضائية الجنائية، وهو الأكثر قبولاً واحتراماً في القانون الدولي. فبموجبه، تمارس الدولة سلطتها العقابية على جميع الجرائم التي ترتكب، كلاً أو جزءاً، داخل حدودها الإقليمية، بغض النظر عن جنسية الجاني أو المجني عليه. هذا المبدأ، الذي يرتكز على مفهوم السيادة المطلقة للدولة على إقليمها، يواجه أزمة وجودية حقيقية أمام جرائم البلوك تشين.

أولاً: تفكك ركن "المكان" في الجريمة اللامركزية

إن تطبيق مبدأ الإقليمية يفترض القدرة على الإجابة على سؤال يسير: "أين وقعت الجريمة؟". لكن في بيئة البلوك تشين، تصبح هذه الإجابة شبه مستحيلة. لنأخذ مثالاً على عقد ذكي احتيالي:

مبرمج الجريمة (الفاعل المعنوي): قد يكون في دولة (أ).

الجهاز الذي استخدمه لبث المعاملة: قد يكون متصلاً بالإنترنت عبر خادم وكيل في دولة (ب).

العقدة (Node) التي قامت بالتحقق من المعاملة وإضافتها إلى الكتلة: قد تكون في دولة (ج).

الضحية الذي تفاعل مع العقد وخسر أمواله: قد يكون في دولة (د).

بقية العُقد التي تحتفظ بنسخة من السجل: موزعة في عشرات الدول الأخرى.

أمام هذا "التفتت الجغرافي" لعناصر الجريمة، أي دولة يمكنها أن تدعي الاختصاص الإقليمي؟ هل هي دولة المبرمج (مكان التخطيط)؟ أم دولة الخادم الوكيل (مكان البث الظاهري)؟ أم دولة العقدة (مكان التنفيذ الخوارزمي)؟ أم دولة الضحية (مكان تحقق النتيجة)؟ إن كل دولة من هذه الدول لديها رابط "إقليمي" ما بالجريمة، مما قد يؤدي إلى "تنازع إيجابي للاختصاص"، فتدعي كل دولة حقها في الملاحقة، مما يخلق فوضى قانونية (Brenner & Koops, 2019).

ثانياً: قصور النظريات المفسرة لمبدأ الإقليمية

لتوسيع نطاق مبدأ الإقليمية ليشمل الجرائم العابرة للحدود، طور الفقه والقضاء نظريتين تفسيريتين:

نظرية الإقليمية الذاتية: تمنح الاختصاص للدولة التي "بدأ" فيها السلوك الإجرامي. في مثالنا، قد تكون هذه دولة (أ) حيث كتب المبرمج الكود. لكن هذا يثير صعوبات إثباتية هائلة، خاصة إذا استخدم المبرمج تقنيات إخفاء الهوية.

نظرية الإقليمية الموضوعية: تمنح الاختصاص للدولة التي "تحققت" فيها النتيجة الإجرامية أو اكتمل فيها الفعل. في مثالنا، قد تكون هذه دولة (د) حيث خسر الضحية أمواله. هذه النظرية، التي تطورت لتشمل "مبدأ الأثر"، هي الأكثر مرونة، ولكنها أيضاً تثير إشكاليات. فماذا لو كان هناك آلاف الضحايا في عشرات الدول؟ هل يعني هذا أن كل دولة من هذه الدول لها اختصاص؟ هذا قد يؤدي إلى ملاحقات قضائية متعددة وانتهاك لمبدأ "عدم جواز المحاكمة عن ذات الفعل مرتين" (Tziakouris, 2021).

إن محاولة تطبيق هذه النظريات، التي صممت لجرائم مادية تعبر الحدود (مثل إطلاق رصاصة عبر الحدود)، على جرائم رقمية لا "تعبر" الحدود بل "توجد" في كل مكان وفي لا مكان في نفس الوقت، هي محاولة غير كافية. إنها تظهر أن مبدأ الإقليمية، في شكله التقليدي، لم يعد قادراً على توفير إجابة واضحة وحاسمة في عالم البلوك تشين (Ferguson, 2017).

٥,١,٢. مبدأ الاختصاص الشخصي: تحدي إخفاء الهوية

عندما يفشل مبدأ الإقليمية، تلجأ الدول إلى مبدأ الاختصاص الشخصي، الذي يربط الولاية القضائية بـ "جنسية" أطراف الجريمة. ولهذا المبدأ صورتان:

أولاً: الاختصاص الشخصي الإيجابي

بموجب هذا المبدأ، تمارس الدولة سلطتها العقابية على الجرائم التي يرتكبها "رعاياها" حتى لو كانوا خارج إقليمها. هذا المبدأ مفيد نظرياً، حيث يمكن لدولة (أ) في مثالنا السابق أن تحاكم المبرمج لأنه يحمل جنسيتها. لكن التحدي هنا ليس قانونياً، بل هو "إثباتي" في المقام الأول.

إن العقبة الكأداء هي "مشكلة الإسناد" التي تم تحليلها سابقاً. فقبل أن تتمكن الدولة من تطبيق اختصاصها الشخصي، يجب عليها أولاً أن تثبت بشكل قاطع أن "العنوان" الرقمي الذي ارتكب الجريمة يعود إلى أحد مواطنيها. إن تقنيات إخفاء الهوية، مثل استخدام الشبكات الخاصة الافتراضية (VPNs)،

وشبكة تور (Tor)، والعملات الرقمية الموجهة للخصوصية، تجعل من عملية ربط الهوية الرقمية بالهوية الحقيقية مهمة استخباراتية وتحقيقية معقدة للغاية، وغالباً ما تكون مستحيلة دون تعاون دولي فعال (Fan et al., 2020).

ثانياً: الاختصاص الشخصي السلبي

هذا المبدأ، وهو أقل قبولاً في القانون الدولي، يمنح الدولة الاختصاص عندما يكون "المجني عليه" (الضحية) أحد رعاياها، حتى لو وقعت الجريمة بالكامل في الخارج وارتكبها أجنبي. في سياق البلوك تشين، يبدو هذا المبدأ جذاباً، فيمكن للدولة (د) في مثالنا أن تدعي الاختصاص لأن الضحية من مواطنيها.

لكن هذا المبدأ يواجه انتقادات قانونية شديدة:

– عدم القدرة على التنبؤ القانوني: إنه يجعل الجاني عرضة للملاحقة بموجب قوانين دول قد لا يعرف عنها شيئاً، لمجرد أن ضحيته يحمل جنسيتها. هذا يتعارض مع مبدأ "شرعية الجرائم والعقوبات"، الذي يتطلب أن يكون القانون واضحاً ومتوقعاً.

– التوسع المفرط في الولاية القضائية: إذا كان هناك ضحايا من ١٠٠ دولة مختلفة، فإن تطبيق هذا المبدأ يعني أن ١٠٠ دولة مختلفة لها الحق في ملاحقة نفس الجاني، مما يخلق فوضى قضائية دولية.

– السيادة والكياسة الدولية: يعتبر العديد من الدول أن هذا المبدأ يمثل تعدياً على سيادة الدولة التي وقع فيها الفعل أو التي ينتمي إليها الجاني (Sheyn, 2018).

لذلك، وعلى الرغم من أن مبدأ الاختصاص الشخصي قد يوفر حلاً في بعض الحالات، إلا أنه يعاني من ضعف جوهري يتمثل في اعتماده على القدرة على تحديد هوية الأطراف، وهي بالضبط المعلومة التي تسعى تقنيات البلوك تشين إلى حجبها.

٥.١.٣. مبدأ الاختصاص العيني ومبدأ العالمية: حلول استثنائية لجرائم استثنائية

عندما تفشل المبادئ السابقة، هناك مبدآن احتياطيان يمكن اللجوء إليهما، ولكنهما يطبقان في نطاق ضيق جداً.

أولاً: مبدأ الاختصاص العيني أو الوقائي

يسمح هذا المبدأ للدولة بممارسة ولايتها القضائية على الجرائم التي ترتكب في الخارج من قبل أجانب، ولكنها تمس "المصالح الأساسية" للدولة وأمنها القومي (مثل تزييف عملتها، أو التجسس، أو الإرهاب).

هل يمكن تطبيق هذا المبدأ على جرائم البلوك تشين؟ الإجابة تعتمد على تكييف الجريمة:

الجرائم المالية العادية: من الصعب القول إن عملية احتيال بالعملات المشفرة، حتى لو كانت كبيرة، تمس "المصلحة الأساسية" للدولة بالمعنى التقليدي.

الجرائم التي تهدد الأمن القومي: الوضع يختلف إذا تم استخدام البلوك تشين في جرائم أكثر خطورة، مثل:

تمويل الإرهاب: استخدام العملات المشفرة لتمويل عمليات إرهابية.

الهجمات على البنية التحتية الحيوية: استخدام عقود ذكية لشن هجمات على شبكات الكهرباء أو الأنظمة المالية.

التأثير على الانتخابات: استخدام البلوك تشين لنشر معلومات مضللة بهدف التأثير على العمليات الديمقراطية.

في هذه الحالات، يمكن للدولة المتضررة أن تدعي الاختصاص العيني بقوة، لأن الجريمة لم تعد مجرد اعتداء على أفراد، بل أصبحت تهديداً لكيان الدولة نفسه (Kshetri, 2021).

ثانياً: مبدأ الاختصاص العالمي

هذا هو المبدأ الأكثر استثنائية، حيث يمنح "أي دولة" الحق في ملاحقة مرتكبي بعض الجرائم الدولية الجسيمة، بغض النظر عن مكان وقوع الجريمة أو جنسية الجاني أو المجني عليه. والهدف هو ضمان عدم وجود "ملاذ آمن" لمرتكبي أفظع الجرائم التي يصدم بها الضمير الإنساني. (أيوب، ٢٠١٧)

تاريخياً، تم تطبيق هذا المبدأ على جرائم مثل القرصنة في أعالي البحار، وتجارة الرقيق، والإبادة الجماعية، وجرائم الحرب. هل يمكن توسيع نطاقه ليشمل بعض جرائم البلوك تشين؟

الحجة المؤيدة للتوسيع: يرى بعض الفقهاء أن بعض الجرائم السيبرانية واسعة النطاق، مثل هجمات برامج الفدية التي تشل المستشفيات والخدمات الحيوية في دول متعددة، أو عمليات الاحتيال التي تسرق المليارات من ملايين الضحايا حول العالم، قد وصلت إلى درجة من الخطورة تجعلها "جرائم ضد المجتمع الدولي بأسره".

الحجة المعارضة: يرى الرأي الغالب أن هذا التوسيع خطير وغير مبرر. فالاختصاص العالمي يجب أن يظل محصوراً في أضيق نطاق ممكن للجرائم التي تمثل انتهاكاً للقواعد الآمرة في القانون الدولي. إن التوسع فيه ليشمل الجرائم السيبرانية، مهما كانت خطورتها، قد يؤدي إلى فوضى واستغلال سياسي، فتبدأ الدول في ملاحقة مواطني دول أخرى لأسباب سياسية تحت غطاء مكافحة الجريمة السيبرانية (Goldsmith, 2018).

الخلاصة:

إن هذا التحليل يكشف عن وجود "فجوة اختصاص" حقيقية. فالمعايير التقليدية، التي تشكل أساس النظام القانوني الدولي، إما أنها غير قادرة على تحديد "مكان" الجريمة (مبدأ الإقليمية)، أو أنها تعتمد على تحديد "هوية" الأطراف وهو أمر صعب (مبدأ الشخصية)، أو أنها لا تنطبق إلا على فئة ضيقة جداً من الجرائم الاستثنائية (مبدأ العينية والعالمية). هذا القصور البنيوي يفرض على الفكر القانوني البحث عن

معايير جديدة وأكثر مرونة، قادرة على التكيف مع طبيعة الجريمة في العصر اللامركزي، وهو ما سيتناوله القسم الفرعي التالي.

٥,٢. نحو تبني معايير حديثة للاختصاص (معيار الأثر نموذجاً).

تمهيد

أمام القصور البنيوي الذي أظهرته معايير الاختصاص التقليدية في مواجهة الجريمة اللامركزية، يجد الفكر القانوني الجنائي نفسه مضطراً للبحث عن أسس جديدة وأكثر مرونة لتأسيس الولاية القضائية. لا يمكن ترك الفضاء الرقمي ليصبح "منطقة خارجة عن القانون" لمجرد أن أدواتنا القانونية الحالية لم تعد مناسبة. من بين المعايير الحديثة التي برزت كحل محتمل لهذه الأزمة، يظهر "معيار الأثر" بوصفه أحد أكثر النماذج الواعدة والقابلة للتطبيق. هذا القسم الفرعي سيقوم بتحليل هذا المعيار من منظور جنائي دقيق، مستكشفاً أصوله، وتطبيقاته القضائية، والتحديات التي تواجه استخدامه في سياق جرائم البلوك تشين، وصولاً إلى تقييم مدى صلاحيته بوصفه ركيزة أساسية لبناء نظرية حديثة للاختصاص القضائي في العصر الرقمي.

٥,٢,١. مفهوم معيار الأثر في القانون الجنائي وتطوره

إن معيار الأثر، في جوهره، هو امتداد منطقي لنظرية الإقليمية الموضوعية، لكنه يركز بشكل حصري على "مكان تحقق الأثر الضار" للجريمة بوصفه أساسا لانعقاد الاختصاص. فبموجبه، تكتسب الدولة ولاية قضائية على فعل ارتكب بالكامل خارج إقليمها، إذا كان هذا الفعل قد أُعِدَّ لينتج، أو أنتج بالفعل، "أثراً جوهرياً" داخل إقليمها (Johnson, 2019). هذا المعيار ينقل بؤرة التحليل من "مكان سلوك الجاني" إلى "مكان معاناة المجتمع" من هذا السلوك. (Tsagourias, 2017)

إن تبني هذا المعيار في السياق الجنائي يتطلب إثبات ثلاثة عناصر رئيسة:

العنصر الأول: فعل خارجي: أن يكون السلوك الإجرامي قد وقع خارج إقليم الدولة التي تدعي الاختصاص. نحو تبني معايير حديثة للاختصاص (معيار الأثر نموذجاً).

تمهيد

أمام القصور البنيوي الذي أظهرته معايير الاختصاص التقليدية في مواجهة الجريمة اللامركزية، يجد الفكر القانوني الجنائي نفسه مضطراً للبحث عن أسس جديدة وأكثر مرونة لتأسيس الولاية القضائية. لا يمكن ترك الفضاء الرقمي ليصبح "منطقة خارجة عن القانون" لمجرد أن أدواتنا القانونية الحالية لم تعد مناسبة. من بين المعايير الحديثة التي برزت بوصفها حلا محتملا لهذه الأزمة، يظهر "معيار الأثر" بوصفه أحد أكثر النماذج الواعدة والقابلة للتطبيق. هذا القسم الفرعي سيقوم بتحليل هذا المعيار من منظور جنائي دقيق، مستكشفاً أصوله، وتطبيقاته القضائية، والتحديات التي تواجه استخدامه في سياق جرائم البلوك تشين، وصولاً إلى تقييم مدى صلاحيته بوصفه ركيزة أساسية لبناء نظرية حديثة للاختصاص القضائي في العصر الرقمي.

٥,٢,١. مفهوم معيار الأثر في القانون الجنائي وتطوره

إن معيار الأثر، في جوهره، هو امتداد منطقي لنظرية الإقليمية الموضوعية، لكنه يركز بشكل حصري على "مكان تحقق الأثر الضار" للجريمة بوصفه أساسا لانعقاد الاختصاص. فبموجبه، تكتسب الدولة ولاية قضائية على فعل ارتكب بالكامل خارج إقليمها، إذا كان هذا الفعل قد أُعِدَّ لينتج، أو أنتج بالفعل، "أثراً جوهرياً" داخل إقليمها (Johnson, 2019). هذا المعيار ينقل بؤرة التحليل من "مكان سلوك الجاني" إلى "مكان معاناة المجتمع" من هذا السلوك. (Tsagourias, 2017)

إن تبني هذا المعيار في السياق الجنائي يتطلب إثبات ثلاثة عناصر رئيسة:

العنصر الأول: فعل خارجي: أن يكون السلوك الإجرامي قد وقع خارج إقليم الدولة التي تدعي الاختصاص.

العنصر الثاني: أثر داخلي: أن يكون لهذا الفعل أثر مادي أو اقتصادي ملموس داخل إقليم الدولة.

العنصر الثالث: رابطة سببية: وجود علاقة سببية مباشرة ومعقولة بين الفعل الخارجي والأثر الداخلي.

هذا الإطار يوفر مرونة كبيرة للتعامل مع جرائم البلوك تشين، إذ يمكن لدولة الضحية أن تدعي الاختصاص لأن الأثر المالي (خسارة الأموال) قد تحقق على أراضيها، بغض النظر عن مكان وجود الجاني أو العُقد التي عالجت المعاملة.

٥,٢,٢. تطبيقات معيار الأثر في القضاء الجنائي المقارن

بدأت المحاكم في مختلف النظم القانونية، وإن كان بتردد، في تبني منطق "معيار الأثر" للتعامل مع الجرائم العابرة للحدود. في الولايات المتحدة، على سبيل المثال، تم استخدام هذا المعيار لتأسيس

الاختصاص في قضايا الاحتيال عبر الإنترنت، فقد اعتبرت المحاكم أن الاختصاص ينعقد في الولاية التي يوجد فيها الخادم الذي استقبل الرسالة الاحتيالية أو التي يوجد فيها الضحية الذي تعرض للضرر المالي.

في السياق الأوروبي، وعلى الرغم من أن "اتفاقية بودابست بشأن الجرائم السيبرانية" لم تتبنَ معيار الأثر بشكل صريح، إلا أن الممارسة القضائية في العديد من الدول الأعضاء تتجه نحو تفسير موسع لمبدأ الإقليمية يشمل مكان تحقق النتيجة الضارة. على سبيل المثال، قضت محكمة العدل الأوروبية في قضايا تتعلق بالتشهير عبر الإنترنت بأن الاختصاص يمكن أن ينعقد أمام محاكم الدولة التي يقع فيها "مركز مصالح" الضحية، وهو مفهوم قريب جداً من منطق معيار الأثر . (De-Strooper, 2018)

إن تطبيق هذا المعيار على جرائم البلوك تشين يبدو استنتاجاً منطقياً لهذا التطور القضائي. فإذا تمكن الادعاء العام من إثبات أن ضحية عملية احتيال باستخدام عقد ذكي يقيم في إقليم الدولة، وأن أمواله قد خرجت من حساب بنكي أو منصة تبادل مرخصة في نفس الدولة، فإن هذا يشكل "أثراً جوهرياً" كافياً لتأسيس الاختصاص القضائي، حتى لو كان الجاني والعقد الذكي موجودين في الفضاء الرقمي العالمي .(Zetzsche et al., 2018)

٥,٢,٣. تحديات تطبيق المعيار في سياق البلوك تشين

على الرغم من المزايا الواضحة لمعيار الأثر، فإن تطبيقه في البيئة اللامركزية لا يخلو من تحديات قانونية دقيقة، يجب التعامل معها بحذر لتجنب التوسع المفرط في الولاية القضائية.

أولاً: إثبات "الأثر الجوهري"

لا يكفي مجرد حدوث أي أثر، بل تشترط معظم التفسيرات أن يكون الأثر "جوهرياً" أو "ذا شأن". فما هو المعيار لتحديد ذلك؟ هل خسارة بضع دولارات من قبل مواطن واحد تعتبر أثراً جوهرياً؟ أم يجب أن يكون الضرر واسع النطاق ويؤثر على عدد كبير من الضحايا أو على استقرار السوق المالي في الدولة؟ إن غياب معيار واضح ومحدد قد يفتح الباب أمام الادعاءات التعسفية بالاختصاص. يجب على الفقه والقضاء تطوير معايير كمية ونوعية لتحديد متى يرقى الأثر إلى درجة "الجسامة" التي تبرر التدخل الجنائي للدولة .(Lin, 2019)

ثانياً: إشكالية الركن المعنوي

إن أحد أهم الانتقادات الموجهة لمعيار الأثر هو أنه قد يؤدي إلى مساءلة أشخاص لم يكن لديهم أي نية أو توقع بأن أفعالهم ستنتج أثراً في دولة معينة. القانون الجنائي يتطلب وجود "قصد جنائي" ، وهذا القصد يجب أن يشمل، على الأقل، "توقع" إمكانية حدوث النتيجة الضارة في مكان معين.

لذلك، يجب على الادعاء العام ألا يثبت فقط وقوع الأثر، بل يجب أن يثبت أيضاً أن الجاني كان "يعلم" أو كان "من المعقول أن يعلم" أن سلوكه سيؤثر على ضحايا في تلك الدولة المحددة.

يمكن الاستدلال على هذا العلم من خلال عدة قرائن، مثل: اللغة التي استخدمها في الترويج لمخططه الاحتيالي، أو العملات التي قبلها، أو المنصات التي روج من خلالها. إن اشتراط إثبات هذا "الارتباط الذهني" بين الجاني ومكان الأثر هو ضمانة أساسية لمنع تطبيق الاختصاص بشكل غير عادل (Bambauer, 2017).

ثالثاً: خطر التنازع الإيجابي للاختصاص

كما ذكرنا سابقاً، فإن أكبر خطر يترتب على التطبيق الواسع لمعيار الأثر هو "التنازع الإيجابي للاختصاص"، إذ تدعي كل دولة يوجد فيها ضحية واحدة حقها في الملاحقة، هذا لا يخلق فقط فوضى قانونية، بل يعرض المتهم لخطر المحاكمات المتعددة. لمواجهة هذا الخطر، يجب تطوير مبادئ للترجيح بين الولايات القضائية المتنازعة، مثل مبدأ "الصلة الأوثق" (، فتعطى الأولوية في الملاحقة للدولة التي لها "الصلة الأقوى" بالجريمة (مثلاً، الدولة التي يوجد فيها أغلب الضحايا، أو التي يوجد فيها الجاني، أو التي يمكن فيها جمع معظم الأدلة) (Svantesson, 2017).

الخلاصة: معيار الأثر بوصفه حلا ضروريٌّ ولكن غير كافٍ

يخلص هذا التحليل إلى أن "معيار الأثر" يمثل خطوة ضرورية ومهمة إلى الأمام في تكييف القانون الجنائي مع تحديات العصر الرقمي. فهو يوفر أساساً منطقياً ومرناً لتأسيس الولاية القضائية في الحالات التي تفشل فيها المعايير التقليدية. ومع ذلك، فهو ليس حلاً سحرياً أو كاملاً.

إن تطبيقه الفعال والآمن يتطلب تطويراً مزدوجاً:

على المستوى الوطني: يجب على التشريعات والمحاكم الوطنية أن تضع ضوابط واضحة لتطبيقه، تشمل تعريفاً دقيقاً لـ "الأثر الجوهري"، واشتراط إثبات "الارتباط الذهني" للجاني بمكان الأثر.

على المستوى الدولي: يجب تطوير مبادئ دولية متفق عليها لحل تنازع الاختصاصات الذي سينشأ حتماً عن تطبيقه، مثل مبدأ "الصلة الأوثق" أو إنشاء آليات للتحقيق والملاحقة المشتركة.

إن معيار الأثر هو أداة قوية، ولكن كأي أداة قوية، يجب استخدامها بحكمة ودقة، لضمان أن تكون وسيلة لتحقيق العدالة، لا أداة للتوسع غير المبرر في سلطة الدولة العقابية.

٥,٣. تحديات التعاون الدولي في التحقيق والملاحقة في البيئة اللامركزية

١ ـ مقدمة تحليلية: الإطار النظري للتعاون الدولي في المجال الجنائي

إن مبدأ السيادة الإقليمية، الذي يمنح كل دولة سلطة مطلقة على إقليمها، يفرض في الوقت ذاته قيداً جوهرياً: وهو أن سلطات إنفاذ القانون في دولة ما لا يمكنها، من حيث المبدأ، أن تمارس أي عمل من أعمال التحقيق أو الملاحقة على إقليم دولة أخرى دون موافقتها. من هذا القيد، نشأ مفهوم "التعاون الدولي في المسائل الجنائية" بوصفه ضرورة حتمية لمكافحة الجريمة العابرة للحدود. يقوم هذا المفهوم على فكرة أن الدول، على الرغم من تمسكها بسيادتها، تدرك أن مصالحها المشتركة في تحقيق العدالة تتطلب منها تقديم

المساعدة لبعضها البعض. وقد تبلور هذا التعاون في مجموعة من الآليات القانونية المنظمة بموجب اتفاقيات دولية ثنائية ومتعددة الأطراف، أهمها: "المساعدة القانونية المتبادلة"، التي تشمل إجراءات مثل جمع الأدلة وسماع الشهود وتنفيذ أوامر التفتيش، و"تسليم المجرمين"، الذي يهدف إلى نقل شخص متهم أو مدان من الدولة التي يوجد فيها إلى الدولة التي تطلب محاكمته أو تنفيذ العقوبة عليه. إن هذه الآليات تشكل العمود الفقري لنظام العدالة الجنائية الدولي، ولكنها، كما سنرى، تواجه تحديات وجودية في مواجهة الجرائم اللامركزية (Bassiouni, 2019).

٢ ـ التحديات القانونية: صدام السيادة مع ضرورات المكافحة

إن تطبيق آليات التعاون الدولي التقليدية على جرائم البلوك تشين يصطدم بعقبات قانونية بنيوية، تحول دون تحقيق الفعالية المطلوبة.

تنازع القوانين الجنائية الوطنية مع الالتزامات الدولية:

أحد أكبر التحديات هو مبدأ "التجريم المزدوج"، الذي تشترطه معظم اتفاقيات التسليم والمساعدة القانونية. بموجب هذا المبدأ، لا تلتزم الدولة بتقديم المساعدة إلا إذا كان الفعل المطلوب بشأنه التعاون مجرماً في قانونها الوطني أيضاً. في سياق جرائم البلوك تشين، قد لا يكون هذا الشرط متوفراً دائماً. فبعض الأفعال، مثل إنشاء "خلاط عملات" أو تشغيل "منظمة مستقلة لا مركزية" (DAO) لأغراض مشبوهة، قد تكون غير مجرمة صراحة في تشريعات بعض الدول، مما يسمح لها برفض طلبات التعاون المقدمة من دول أخرى تعتبر هذه الأفعال جرائم. هذا الاختلاف في التجريم يخلق "ثغرات" قانونية تستغلها الشبكات الإجرامية لاختيار الدول ذات التشريعات المتساهلة كقواعد لعملياتها (Johnson, 2020).

اختلاف المعايير الإجرائية بين الأنظمة القانونية:

حتى لو كان الفعل مجرماً في كلتا الدولتين، فإن الاختلاف في الإجراءات قد يعوق التعاون. على سبيل المثال، قد تطلب دولة (أ) تفتيش جهاز كمبيوتر وضبط بياناته، ولكن معايير الإثبات المطلوبة لإصدار إذن التفتيش في دولة (ب) قد تكون أعلى بكثير. كما أن قواعد قبول الأدلة الرقمية تختلف بشكل كبير بين النظم الأنجلو-أمريكية (التي تركز على قواعد الإثبات التفصيلية) والنظم اللاتينية (التي تتبنى مبدأ الاقتناع القضائي الحر). هذا الاختلاف في "اللغة الإجرائية" بين الدول يمكن أن يؤدي إلى رفض تنفيذ الطلبات أو إلى جمع أدلة لا تكون مقبولة لاحقاً أمام المحكمة الطالبة (Lee, 2021).

صعوبات الإثبات في القضايا العابرة للحدود:

إن الطبيعة المجردة والمشتتة للأدلة في جرائم البلوك تشين تزيد من صعوبة إقناع السلطات القضائية في الدولة المطلوب منها التعاون بوجود "أساس معقول" لتنفيذ الإجراء المطلوب. فتقديم طلب مساعدة قانونية يعتمد على مجرد "عناوين" مشفرة وتدفقات مالية معقدة قد لا يكون كافياً لإقناع قاضٍ أجنبي، معتاد

على الأدلة المادية، بضرورة اتخاذ إجراءات تمس خصوصية أفراد على إقليمه. هذا العبء الإثباتي المرتفع في المرحلة الأولية للتعاون قد يجهض العديد من التحقيقات الدولية في مهدها (Martinez, 2018).

٣ ـ الجوانب العملية: بطء الإجراءات في مواجهة سرعة الجريمة

إلى جانب التحديات القانونية، تواجه آليات التعاون الدولي عقبات عملية وبيروقراطية تجعلها غير متناسبة على الإطلاق مع سرعة الجريمة الرقمية.

عقبات تنفيذ طلبات المساعدة القانونية المتبادلة:

تستغرق عملية المساعدة القانونية المتبادلة وقتاً طويلاً بشكل كارثي. فالطلب يجب أن يمر عبر قنوات دبلوماسية متعددة (من وزارة العدل في الدولة الطالبة إلى وزارة الخارجية، ثم إلى سفارتها، ثم إلى وزارة خارجية الدولة المطلوبة، ثم إلى وزارة العدل فيها، وأخيراً إلى النيابة العامة المختصة). هذه الرحلة البيروقراطية قد تستغرق شهوراً، بل سنوات في بعض الحالات. خلال هذه الفترة، يكون المجرم قد قام بنقل أصوله الرقمية، أو تدمير الأدلة، أو تغيير هويته الرقمية بالكامل. إن هذا البطء المنهجي يجعل من آليات المساعدة القانونية المتبادلة أداة غير فعالة في التعامل مع الأدلة الرقمية التي يمكن إتلافها بنقرة زر واحدة (UNODC, 2022).

تأخيرات إجراءات تسليم المجرمين:

تتسم إجراءات تسليم المجرمين بتعقيد إجرائي وبطء منهجي. فهي لا تتضمن فقط فحص الشروط القانونية (كالتجريم المزدوج واستثناء الجرائم السياسية)، بل تتضمن أيضاً إجراءات قضائية كاملة في الدولة المطلوب منها التسليم، قد تصل إلى أعلى محكمة فيها. كما أن العديد من الدول ترفض تسليم مواطنيها. هذا يعني أنه حتى لو تم تحديد هوية الجاني ومكانه، فإن إحضاره للمحاكمة قد يكون عملية طويلة ومحفوفة بالشكوك. هذا البطء يشجع المجرمين على اللجوء إلى الدول التي لديها إجراءات تسليم معقدة أو التي لا ترتبط باتفاقيات تسليم مع الدول التي تستهدفها أنشطتهم (Williams, 2021).

٤ ـ الحلول المقترحة: نحو تعاون دولي فعال ومرن

لمواجهة هذه التحديات، لا بد من إعادة التفكير بشكل جذري في آليات التعاون الدولي.

توحيد المعايير الإجرائية والموضوعية:

إن الحل الأكثر جذرية هو العمل على توحيد القواعد الموضوعية (تعريف الجرائم السيبرانية) والإجرائية (قواعد جمع الأدلة الرقمية) بين الدول. يمكن تحقيق ذلك من خلال اتفاقيات دولية جديدة، على غرار اتفاقية بودابست، ولكن بنطاق أوسع ومشاركة عالمية أكبر. إن وجود "لغة قانونية مشتركة" سيسهل بشكل كبير عملية التعاون ويقلل من أسباب رفض الطلبات. يجب أن تهدف هذه الاتفاقيات إلى تيسير الشروط، مثل تخفيف شرط التجريم المزدوج في بعض الحالات، ووضع معايير دنيا موحدة لقبول الأدلة الرقمية (Hague Conference on Private International Law, 2020).

تعزيز آليات التنسيق القضائي المباشر:

بدلاً من الاعتماد الحصري على القنوات الدبلوماسية البطيئة، يجب تعزيز آليات التنسيق المباشر بين أجهزة إنفاذ القانون والقضاء في الدول المختلفة. يمكن تحقيق ذلك من خلال:

إنشاء شبكات قضائية متخصصة: على غرار "شبكة العدالة الأوروبية" ، يمكن إنشاء شبكات إقليمية أو دولية متخصصة في الجرائم السيبرانية، تعمل كنقاط اتصال لتسهيل تبادل المعلومات والطلبات بشكل سريع.

فرق التحقيق المشتركة: تسمح هذه الآلية، المطبقة بنجاح في أوروبا، بتشكيل فريق تحقيق واحد يضم محققين وقضاة من عدة دول معنية، ويعمل بموجب إطار قانوني واحد، مما يسمح بجمع الأدلة بشكل متزامن وفعال عبر الحدود (Brown, 2019).

الخلاصة: مستقبل التعاون الجنائي في العصر الرقمي

يخلص هذا التحليل إلى أن آليات التعاون الدولي التقليدية، التي صممت لعصر مختلف، أصبحت غير قادرة على مواكبة تحديات الجريمة في البيئات اللامركزية. إن الفجوة بين سرعة الجريمة وبطء العدالة تتسع بشكل خطير، مما يهدد بتقويض سيادة القانون في الفضاء الرقمي.

إن المستقبل يتطلب تحولاً نموذجياً من "التعاون القائم على الطلبات" إلى "التعاون القائم على الشبكات". يجب بناء بنية تحتية دولية للعدالة الجنائية تكون بنفس درجة التشبيك والسرعة التي تتمتع بها الشبكات الإجرامية. هذا يتطلب إرادة سياسية قوية من الدول للتنازل عن جزء من شكليات السيادة لصالح فعالية المكافحة، والاستثمار في بناء الثقة المتبادلة بين أجهزتها القضائية. ففي عالم لا تعترف فيه الجريمة بالحدود، يجب على العدالة أيضاً أن تتعلم كيف تتجاوزها بفعالية ومرونة. ((Anderson, 2023

٦. الخاتمة العامة: نحو إعادة بناء المفاهيم الجنائية في عصر اللامركزية

في ختام هذا البحث، الذي حاول أن يسبر أغوار العلاقة المعقدة بين المبادئ الراسخة للقانون الجنائي والطبيعة الثورية لتقنية البلوك تشين، نصل إلى عتبة تتجاوز مجرد استعراض التحديات التقنية لتلامس جوهر الفلسفة الجنائية نفسها. لم تكن هذه الدراسة رحلة في عالم التكنولوجيا بقدر ما كانت رحلة في عالم المفاهيم، فقد تم إخضاع المقولات القانونية المستقرة – كالفعل، والإسناد، والإثبات، والسيادة – لاختبار قاسٍ في مواجهة واقع جديد يتسم باللامركزية، واللامكانية، واللامادية. إن النتيجة الأبرز التي تتبلور من هذا التحليل ليست مجرد الحاجة إلى تعديلات تشريعية جزئية، بل هي ضرورة إعادة التفكير بشكل نقدي في مدى كفاية الأدوات المفاهيمية التي ورثناها من العصر الصناعي للتعامل مع جرائم العصر الخوارزمي.

لقد كشف البحث أن تقنية البلوك تشين، بما تحمله من وعود بالشفافية والأمان، تخلق في الوقت ذاته "مفارقات قانونية" عميقة. ففي مجال الإثبات، وجدنا أنفسنا أمام دليل يتمتع بدرجة غير مسبوقة من السلامة الداخلية ومقاومة التلاعب، ولكنه في الوقت ذاته يعاني من هشاشة بنيوية عند نقطة تفاعله مع العالم الخارجي، فيما يعرف بـ "مشكلة الأوراكل". هذه المفارقة تفرض على الفكر الإثباتي الجنائي تحولاً جوهرياً: من التركيز على "سلامة الوعاء" إلى التدقيق النقدي في "صحة المحتوى" وحُجِّيَّة مصدره. إن القبول الأعمى لبيانات البلوك تشين بوصفه "حقيقة مطلقة" دون فحص دقيق لعملية إنتاجها هو تنازل عن الوظيفة القضائية في البحث عن الحقيقة الموضوعية، وتحول خطير نحو "العدالة الخوارزمية" التي قد تكون سليمة تقنياً لكنها جائرة موضوعياً.

وعلى صعيد المسؤولية الجنائية، أظهر التحليل أن اللامركزية لا تؤدي فقط إلى صعوبة في تحديد هوية الفاعل، بل إلى تفكك مفهوم "الفاعل" نفسه. فالجريمة في بيئة البلوك تشين لم تعد نتاج فعل فردي معزول، بل هي غالباً نتيجة لتفاعل معقد بين أطراف متعددة وموزعة: المبرمج الذي يكتب الكود، والمستخدم الذي يستدعيه، ومشغل العقدة الذي يتحقق منه، ومنصة التبادل التي تسهل تسييل عائداته. إن محاولة تطبيق نظرية "الفاعل الأصلي" التقليدية على هذه الشبكة من المساهمات هي محاولة قاصرة. هذا يفرض على القانون الجنائي ضرورة الانتقال من نموذج "المسؤولية الخطية" إلى نموذج "المسؤولية الشبكية" ، وهو نموذج أكثر تعقيداً يتطلب تطوير نظريات المساهمة الجنائية لتشمل أدواراً جديدة لم تكن معروفة من قبل، مع وضع معايير دقيقة للتفريق بين المساهمة الإجرامية المتعمدة وتوفير البنية التحتية التقنية المحايدة.

أما في مجال الولاية القضائية، فقد كشف البحث أن الطبيعة العابرة للحدود واللامكانية لجرائم البلوك تشين قد أحدثت "أزمة مكانية" لمبدأ الإقليمية، الذي يشكل حجر الزاوية في السيادة الجنائية للدول. إن محاولة تحديد "مكان" وقوع جريمة لا توجد في مكان واحد، بل توجد نسخ منها في كل مكان، هي مهمة عبثية. هذا العجز لا يمثل مجرد مشكلة إجرائية، بل هو تحدٍ وجودي للنظام القانوني الدولي القائم على

تقسيم العالم إلى ولايات قضائية إقليمية منفصلة. إن الفراغ الذي يخلقه هذا العجز يهدد بتحويل الفضاء اللامركزي إلى "غرب متوحش رقمي" ، إذ يمكن للجريمة المنظمة أن تعمل بحرية نسبية، مستغلة بطء وتعقيد آليات التعاون الدولي التقليدية.

إن هذه الأزمات المفاهيمية الثلاث – في الإثبات، والمسؤولية، والولاية القضائية – ليست مجرد مشاكل تقنية يمكن حلها بتحديثات برمجية، بل هي تحديات قانونية وفلسفية عميقة. إنها تجبرنا على مواجهة حقيقة أن القانون، في جوهره، هو نظام مركزي مصمم لحكم عالم مركزي. وعندما تتغير بنية الواقع الذي يحكمه القانون ليصبح لا مركزياً، فإن القانون نفسه يجب أن يتكيف أو يفقد أهميته. إن الفشل في بناء جسور مفاهيمية وتشريعية بين عالم القانون المادي وعالم البلوك تشين الرقمي لن يؤدي فقط إلى إعاقة مكافحة غش الأدوية، بل سيترك منظومة العدالة الجنائية بأكملها غير مستعدة لمواجهة الجيل القادم من الجرائم التي ستشكلها التقنيات اللامركزية.

انطلاقاً من هذا التشخيص النقدي، سيقوم الجزء التالي من هذه الخاتمة ببلورة النتائج التفصيلية التي توصل إليها البحث، وتقديم مجموعة من التوصيات المنهجية والمحددة التي تهدف إلى الإسهام في بناء هذا الإطار القانوني الجديد.

٦,١ النتائج الرئيسة للبحث: تلخيص لأهم ما توصلت إليه الدراسة من نتائج بخصوص الإشكاليات المطروحة.

لقد توصلت هذه الدراسة، عبر تحليلها المعمق للتقاطع الإشكالي بين تقنية البلوك تشين والقانون الجنائي، إلى مجموعة من النتائج الجوهرية التي تكشف عن حجم وعمق التحولات التي تفرضها هذه التقنية على منظومة العدالة الجنائية. لا يمكن اختزال هذه النتائج في مجرد قائمة من التحديات التقنية، بل هي تمثل إعادة تشكيل بنيوية للمفاهيم التي يقوم عليها التجريم والعقاب والإثبات.

النتيجة الأولى: تآكل المصلحة المحمية جنائياً في جريمة غش الأدوية وتحولها نحو نموذج الجريمة المستقلة.

كشف التحليل في الفصل التمهيدي أن التوصيفات الجنائية التقليدية لجريمة غش الأدوية، التي تتأرجح بين اعتبارها اعتداءً على الملكية الفكرية أو شكلاً من أشكال الغش التجاري، تعاني من قصور بنيوي. فهذه التوصيفات تفشل في إدراك جوهر المصلحة المحمية جنائياً، وهي "الحق في الحياة والسلامة الجسدية" و"الثقة العامة في النظام الصحي". وقد خلص البحث إلى أن الاستجابة الجنائية الفعالة، سواء كانت تقليدية أو معززة بالتكنولوجيا، تتطلب بالضرورة تبني نموذج "الجريمة المستقلة"، كما فعلت اتفاقية ميديكرايم. هذا التوصيف المستقل هو الذي يبرر فرض عقوبات رادعة، ويوسع نطاق التجريم ليشمل كافة حلقات السلسلة الإجرامية، ويؤسس لسياسة جنائية لا تتسامح مطلقاً مع هذا الشكل من أشكال الإرهاب الصحي.

النتيجة الثانية: مفارقة البلوك تشين الإثباتية: بين اليقين التشفيري والهشاشة البشرية.

أثبت البحث أن دليل البلوك تشين يطرح "مفارقة إثباتية" فريدة. فمن ناحية، يتمتع السجل بدرجة غير مسبوقة من "السلامة الداخلية بفضل خصائص الثبات والتشفير، مما يجعله محصناً ضد التلاعب اللاحق. ولكن من ناحية أخرى، يعاني من "هشاشة خارجية" قاتلة بسبب "مشكلة الأوراكل". وقد خلص البحث إلى أن حجية الدليل المستمد من البلوك تشين لا يمكن أن تكون مطلقة أو مفترضة، بل هي "حجية مشروطة" تتوقف على قدرة الادعاء العام على إثبات حُجِّيَّة مصدر البيانات (الأوراكل) بأدلة مستقلة. هذه النتيجة تعني أن البلوك تشين لا تلغي الحاجة إلى التحقيق التقليدي، بل تعيد توجيهه وتزيد من تعقيده، وتفرض على القضاء الجنائي واجب عدم الافتتان باليقين التقني الظاهري على حساب البحث عن الحقيقة الموضوعية.

النتيجة الثالثة: تفكك أركان الإسناد الجنائي وحتمية الانتقال نحو نماذج المسؤولية الموسعة.

لعل النتيجة الأخطر التي توصلت إليها الدراسة هي أن البنية اللامركزية للبلوك تشين تؤدي إلى "تفكك" أركان الإسناد الجنائي التقليدية.

على مستوى الفعل المادي: لم يعد من الممكن تحديد "مكان" واحد للجريمة، مما يقوض فعالية مبدأ الاختصاص الإقليمي.

على مستوى الفاعل: لقد أدى إخفاء الهوية اسمياً إلى خلق فجوة عميقة بين "الهوية الرقمية" (العنوان) و"الهوية الحقيقية" (الشخص)، مما يجعل من تطبيق مبدأ شخصية المسؤولية الجنائية تحدياً إثباتياً هائلاً.

على مستوى القصد الجنائي: أدت أتمتة "العقود الذكية" إلى فصل الإرادة عن الفعل، مما يتطلب من الفقه الجنائي تطوير نظريات جديدة حول استمرارية القصد الجنائي في البيئات الخوارزمية.

وقد خلص البحث إلى أن مواجهة هذا التفكك تتطلب تجاوز التركيز الحصري على "الفاعل المادي المباشر"، وتبني نماذج مسؤولية موسعة تستهدف كافة حلقات الشبكة الإجرامية. وهذا يشمل تفعيل نظريات "الفاعل المعنوي" لمساءلة المبرمجين الذين يصممون أدوات الجريمة، وتطبيق نظريات "المساهمة الجنائية" القائمة على "العمى المتعمد" لمساءلة الأطراف الوسيطة (كمشغلي خلاطات العملات) التي تسهل الجريمة عن علم احتمالي.

النتيجة الرابعة: قصور آليات التعاون الدولي التقليدية وحتمية التحول نحو نماذج "التعاون الشبكي".

أخيراً، أظهر التحليل أن آليات التعاون الدولي التقليدية، كالمساعدة القانونية المتبادلة والتسليم، مصممة لعالم مركزي وبطيء، وهي تعاني من "عجز بنيوي" في مواجهة الطبيعة الفورية والعالمية

واللامركزية لجرائم البلوك تشين. إن الفجوة الزمنية الهائلة بين سرعة الجريمة الرقمية وبطء الإجراءات القانونية الدولية تخلق "فجوة إنفاذ" تستغلها الجريمة المنظمة. وقد خلص البحث إلى أن الحل لا يكمن في مجرد تسريع الإجراءات القائمة، بل في التحول النموذجي من "التعاون الثنائي البيروقراطي" إلى "التعاون الشبكي المباشر" بين وحدات الجرائم السيبرانية المتخصصة، وتفعيل آليات أكثر مرونة كفرق التحقيق المشتركة.

إن هذه النتائج مجتمعة ترسم صورة واضحة: أننا أمام تحدٍ لا يقتصر على تكييف نص قانوني هنا أو هناك، بل يتطلب إعادة نظر شاملة في الأدوات المفاهيمية والإجرائية التي يستخدمها القانون الجنائي لمواجهة واقع تقني لم يعد يتناسب مع افتراضاته الأساسية.

٦,٢. التوصيات

انطلاقاً من النتائج التحليلية التي كشفت عن وجود فجوات مفاهيمية وتشريعية وإجرائية عميقة، وفي ضوء المبادئ الأساسية للسياسة الجنائية الحديثة التي تسعى إلى الموازنة بين فعالية المكافحة وضمانات حقوق الإنسان، تقدم هذه الدراسة مجموعة من التوصيات المنهجية التي تهدف إلى بناء إطار قانوني جنائي متكامل وقادر على استيعاب تحديات تقنية البلوك تشين. لا تهدف هذه التوصيات إلى تقديم حلول نهائية، بل إلى فتح حوار تشريعي وقضائي جاد، ووضع لبنات أولى لمنظومة عدالة جنائية تتناسب مع متطلبات العصر الرقمي اللامركزي.

أ- على المستوى التشريعي: من الترقيع إلى إعادة البناء

إن الاستجابة التشريعية يجب أن تتجاوز منطق "الترقيع" أو تعديل النصوص القائمة بشكل جزئي، لتتبنى نهجاً شاملاً يعيد بناء أجزاء من المنظومة الجنائية لتتواءم مع الواقع الجديد.

١ - ضرورة إصدار قانون خاص بالجرائم المرتبطة بالأنظمة اللامركزية:

ندعو المشرع إلى عدم الاكتفاء بتطبيق النصوص التقليدية لجرائم النصب أو غسل الأموال، بل إلى إصدار تشريع خاص يعالج الأبعاد الفريدة لجرائم البلوك تشين. يجب أن يتضمن هذا التشريع:

- باباً للتعريفات: يقدم تعريفات قانونية دقيقة للمصطلحات التقنية الأساسية (مثل: الأصل الافتراضي، العقد الذكي، المنظمة المستقلة اللامركزية، خدمة الخلط)، وذلك لقطع دابر أي خلاف في التفسير القضائي وتوفير اليقين القانوني.

- تجريم أفعال جديدة: يجب أن ينص القانون صراحة على تجريم أفعال لم تكن معروفة من قبل، وأهمها:

- جريمة "إنشاء أو توفير أداة إجرامية رقمية": تجريم فعل تصميم أو نشر أو تسويق كود برمجي (كعقد ذكي أو بروتوكول) يكون غرضه الأساس أو الوحيد هو ارتكاب أو تسهيل الجرائم. هذا النص يستهدف "صناع أسلحة الجريمة الرقمية" بشكل مباشر.

- جريمة "إعاقة التعقب الرقمي": تجريم الاستخدام المتعمد لخدمات "خلط العملات" (mixers) أو العملات الموجهة للخصوصية بهدف إخفاء مصدر أو وجهة أموال متحصلة من جريمة، واعتبار هذا الفعل جريمة مستقلة (على غرار جريمة غسل الأموال) وليس مجرد قرينة.

٢ ـ تحديث قواعد المساهمة الجنائية لتشمل "المساعدة التقنية":

يجب تعديل نصوص الاشتراك الجنائي لتنص صراحة على أن "تقديم المساعدة التقنية الجوهرية" يعتبر صورة من صور الاشتراك، حتى لو كانت الأداة المقدمة محايدة ظاهرياً. يجب أن يضع المشرع معايير واضحة للتفريق بين المساعدة المشروعة وغير المشروعة، استناداً إلى قرائن موضوعية مثل: (١) تصميم الخدمة وتجاهلها المتعمد للضوابط الأمنية، (٢) نموذج الربح المعتمد على تشجيع الاستخدام غير المشروع، (٣) المعرفة الفعلية أو المفترضة بالاستخدامات الإجرامية الواسعة النطاق للخدمة.

٣ ـ تبني قواعد اختصاص جنائي مرنة ومضبوطة:

نوصي بأن يتبنى المشرع صراحة "معيار الأثر" بوصفه قاعدة تكميلية للاختصاص في الجرائم السيبرانية. ولكن لمنع التوسع المفرط، يجب تقييد هذا المعيار بشرطين صارمين:

شرط "الأثر الجوهري والمباشر": لا يكفي أي أثر عابر، بل يجب أن يكون الضرر الذي لحق بالضحايا أو بالمصالح الوطنية داخل إقليم الدولة جوهرياً ومباشراً.

شرط "الاستهداف المعقول": يجب على الادعاء العام أن يثبت أن الجاني، من خلال سلوكه (مثل اللغة المستخدمة، أو المنصات التي روج عليها)، كان "يستهدف" بشكل معقول إحداث الأثر في إقليم الدولة، أو على الأقل كان يتوقع حدوثه بوصفه أثرا محتملا لأفعاله.

بـ على المستوى القضائي: نحو فقه قضائي مستنير

يلعب القضاء دوراً حيوياً في سد الفجوات التشريعية من خلال التفسير الخلاق.

١ ـ إرساء مبادئ توجيهية لقبول ووزن الأدلة الرقمية:

ندعو المحاكم العليا (كمحكمة النقض) إلى إصدار مبادئ توجيهية واضحة بشأن حجية الأدلة المستمدة من البلوك تشين. يجب أن تؤكد هذه المبادئ على:

- "الحجية المشروطة" للدليل: لا يتمتع سجل البلوك تشين بحجية مطلقة، بل حجيته مشروطة بإثبات الادعاء لسلامة و حُجِّيَّة "الأوراكل" (مصدر البيانات) بأدلة مستقلة.

- "عبء الإثبات على الادعاء": يقع على عاتق الادعاء العام عبء تقديم شهادة خبير فني مفصلة تشرح آلية عمل البلوك تشين المستخدمة وتؤكد سلامتها التقنية.

٢ ـ تكريس حقوق الدفاع في العصر الرقمي:

يجب على القضاء أن يكرس من خلال أحكامه حقوقاً إجرائية جديدة للدفاع تتناسب مع طبيعة الدليل الرقمي، وأهمها:

- "الحق في تدقيق الكود": تمكين الدفاع من فحص الكود المصدري للبلوك تشين والعقود الذكية من خلال خبير فني من اختياره.

- "الحق في مواجهة الخبير": ضمان حق الدفاع الكامل في استجواب خبير الادعاء وتقديم خبير مضاد.

- "الحق في استجواب الأوراكل": التأكيد على أن "الأوراكل" (البشري أو الآلي) هو الشاهد الحقيقي الذي يجب أن يخضع للاستجواب، وليس السجل الرقمي الأصم.

٣ ـ التخصص القضائي والتدريب المستمر:

إن تعقيد هذه القضايا يحتم إنشاء دوائر قضائية متخصصة في الجرائم السيبرانية والاقتصادية الرقمية، وتوفير برامج تدريب مستمر وعميق للقضاة وأعضاء النيابة العامة حول الجوانب التقنية والقانونية لهذه التقنيات، بالتعاون مع خبراء فنيين متخصصين.

ج- على المستوى الدولي والمؤسسي: بناء بنية تحتية للعدالة العالمية

لا يمكن لأي دولة بمفردها أن تواجه جريمة لا تعترف بالحدود.

١ - تطوير آليات التعاون الدولي:

- الدعوة إلى بروتوكول دولي ملزم بشأن الأنظمة اللامركزية: يجب على المجتمع الدولي العمل على تطوير بروتوكول ملحق باتفاقيات قائمة (كاتفاقية بودابست أو اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة) يضع قواعد موحدة للاختصاص، والمساعدة القانونية المتبادلة، وتسليم المجرمين في الجرائم المرتبطة بالبلوك تشين.

- تفعيل فرق التحقيق المشتركة: يجب تشجيع الدول على استخدام هذه الآلية الفعالة التي تسمح بجمع الأدلة بشكل متزامن عبر الحدود وتجاوز الإجراءات البيروقراطية الطويلة.

٢ ـ تعزيز الشراكة بين القطاعين العام والخاص:

إن مكافحة هذه الجرائم تتطلب تعاوناً وثيقاً بين أجهزة إنفاذ القانون والقطاع الخاص (منصات التبادل، شركات تحليل البلوك تشين، مطورو البرامج). يجب إنشاء أطر قانونية وتشغيلية لهذه الشراكة تضمن تبادل المعلومات بشكل سريع وآمن، مع الحفاظ على ضوابط حماية البيانات والخصوصية.

في المحصلة، إن بناء إطار قانوني جنائي شامل لمكافحة الجرائم في عصر البلوك تشين ليس مهمة سهلة، بل هو مشروع طويل الأمد يتطلب رؤية تشريعية واضحة، وفقها قضائيا مستنيرا، وتعاونا دوليا فعالا. إن التوصيات المقدمة هنا ليست سوى خطوة أولى على هذا الطريق، ولكنها خطوة ضرورية لضمان ألا تسبق سرعة التكنولوجيا قدرة القانون على تحقيق العدالة.

٦,٣. نحو بناء إطار قانوني جنائي متكامل:

مسودة مقترح قانون بشأن تنظيم المسؤولية الجنائية ومكافحة الجرائم المرتبطة بتقنيات السجلات الموزعة (البلوك تشين)

المذكرة الإيضاحية العامة:

في ظل التحولات الجذرية التي أحدثتها الثورة الرقمية، برزت تقنيات السجلات الموزعة (البلوك تشين) كواحدة من أكثر الابتكارات تأثيراً على البنى الاقتصادية والاجتماعية. وعلى الرغم مما تحمله هذه التقنيات من وعود هائلة بالشفافية والكفاءة والأمان، فقد أفرزت في الوقت ذاته أنماطاً إجرامية جديدة ومستحدثة، وخلقت تحديات غير مسبوقة لمنظومة العدالة الجنائية التي لا تزال مفاهيمها وقواعدها متجذرة في عالم مادي ومادي.

لقد كشف الواقع العملي والتطور الفقهي عن وجود "فجوة تشريعية" عميقة. فالنصوص الجنائية التقليدية، كنصوص جرائم النصب والسرقة وغسل الأموال، على الرغم من إمكانية تكييفها في بعض الحالات، إلا أنها تبدو قاصرة عن الإحاطة بالطبيعة الفريدة لهذه الجرائم. فهي لم تصمم للتعامل مع أصول افتراضية لا مادية، أو فاعلين مجهولي الهوية اسمياً، أو عقود ذكية ذاتية التنفيذ، أو كيانات لا مركزية عابرة للحدود. هذا القصور يهدد إما بالإفلات من العقاب بسبب صعوبة الإثبات والإسناد، أو بالتوسع غير المنضبط في التجريم بما يمس استقرار المعاملات ويخنق الابتكار المشروع.

من هذا المنطلق، يأتي هذا المقترح بقانون ليسد هذه الفجوة، وليقدم إطاراً تشريعياً خاصاً ومتكاملاً، يرتكز على فلسفة جنائية حديثة تهدف إلى تحقيق توازن دقيق بين أهداف متعارضة:

الفعالية والردع: توفير الأدوات القانونية اللازمة لمكافحة الأنماط الإجرامية الجديدة بشكل فعال، وتحقيق الردع العام والخاص.

اليقين القانوني: وضع تعريفات واضحة ومحددة للأفعال المجرمة، بما يتوافق مع مبدأ الشرعية الجنائية.

حماية الابتكار: التمييز الدقيق بين الاستخدام المشروع وغير المشروع للتقنية، وتوفير "ملاذات آمنة" للابتكار والبحث العلمي المشروع.

ضمانات المحاكمة العادلة: تكريس حقوق الدفاع في البيئة الرقمية، وضمان عدم المساس بالمبادئ الدستورية الراسخة.

ويستند هذا المقترح إلى تحليل معمق لأوجه القصور في المنظومة الحالية، مع الاسترشاد بأفضل الممارسات الدولية والتوصيات الصادرة عن المنظمات المتخصصة كمجموعة العمل المالي (FATF) ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، ليقدم حلاً تشريعياً عصرياً وفعالاً، قادراً على مواكبة الحاضر والاستعداد للمستقبل.

الباب الأول: أحكام تمهيدية وتعريفات

مادة (١): نطاق السريان

تسري أحكام هذا القانون على كافة الجرائم المنصوص عليها فيه، وتلك التي ترتكب باستخدام تقنيات السجلات الموزعة بوصفها وسيلة أساسية، إذا وقع أي عنصر من عناصر ركنها المادي على إقليم الدولة، أو ارتكبها أحد مواطنيها، أو مست آثارها الجوهرية والمباشرة مصالح الدولة الأساسية أو مصالح أحد مواطنيها أو المقيمين فيها.

المذكرة الإيضاحية للمادة (١): تهدف هذه المادة إلى تأسيس ولاية قضائية واسعة ومرنة تتناسب مع الطبيعة العابرة للحدود لهذه الجرائم. هي لا تكتفي بمبدأ الإقليمية التقليدي، بل تتبنى صراحة "معيار الأثر" كأساس تكميلي للاختصاص، مع تقييده بشرط "الأثر الجوهري والمباشر" لمنع التوسع غير المنضبط. هذا النص يمنح الادعاء العام أساساً قانونياً واضحاً لملاحقة الجرائم التي ترتكب من الخارج وتؤثر على الداخل، وهو الوضع الغالب في هذا النوع من الجرائم.

مادة (٢): تعريفات

في تطبيق أحكام هذا القانون، يقصد بالمصطلحات التالية المعاني المبينة قرين كل منها:

تقنية السجلات الموزعة (البلوك تشين): قاعدة بيانات لامركزية وموزعة، محمية بالتشفير، تستخدم لتسجيل المعاملات بشكل ثابت ومقاوم للتلاعب.

الأصل الافتراضي: تمثيل رقمي مشفر لقيمة يمكن تداولها أو نقلها أو تخزينها رقمياً، ويشمل على سبيل المثال لا الحصر، العملات المشفرة، والرموز المميزة (Tokens) القابلة للاستبدال وغير القابلة للاستبدال.

العقد الذكي: كود برمجي ذاتي التنفيذ يتم تخزينه على سجل موزع، ومصمم لتنفيذ شروط محددة مسبقاً بشكل آلي عند استيفاء شروط معينة.

الأوراكل (مصدر البيانات): أي قناة، بشرية أو آلية، تقوم بتزويد عقد ذكي ببيانات من خارج السجل الموزع للتأثير على تنفيذه.

خدمة الخلط (Mixer/Tumbler): أي خدمة، آلية أو يدوية، تهدف إلى قطع الصلة بين المرسل والمستقبل في معاملات الأصول الافتراضية لإخفاء مصدرها أو وجهتها.

المنظمة المستقلة اللامركزية (DAO): كيان يتم تنسيق عملياته وإدارته من خلال قواعد مبرمجة في عقود ذكية، وتتم المشاركة في حوكمته عادةً من خلال حيازة رموز مميزة.

مشكلة الأوراكل: هي التعبير القانوني عن حقيقة أن البلوك تشين تضمن سلامة الذاكرة، ولكنها لا تضمن صدق الرواية. ومن منظور جنائي، هي نقطة الضعف التي يمكن من خلالها للخطأ البشري أو النية

الإجرامية أن "تُعدي" (infect) نظاماً آمناً وموثوقاً ظاهرياً، مما يفرض على القضاء واجب التعامل مع أدلته بحذر منهجي، والبحث دائماً عن أدلة تعزيزية من خارج السلسلة لتأكيد صحة ما هو مسجل عليها.

المذكرة الإيضاحية للمادة (٢): يعد هذا الباب حجر الزاوية في القانون، إذ يوفر "اليقين القانوني" من خلال تعريف المصطلحات التقنية بلغة قانونية واضحة. هذا يمنع أي التباس في التفسير القضائي ويضمن تطبيق القانون بشكل موحد. التعريفات مستقاة من أفضل الممارسات الدولية وتهدف إلى أن تكون مرنة بما يكفي لتشمل التطورات المستقبلية.

الباب الثاني: الجرائم والعقوبات

الفصل الأول: جرائم تزييف البيانات والمساس بالثقة الرقمية

مادة (٣): جريمة الإدخال العمدي لبيانات كاذبة في نظام تتبع دوائي

يُعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسمائة ألف ريال ولا تجاوز خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل من أدخل عمداً بيانات كاذبة أو مضللة في نظام تتبع دوائي قائم على تقنية السجلات الموزعة.

وتتوافر حالة العمد إذا كان الجاني يعلم بأن البيانات التي يدخلها غير مطابقة للحقيقة، وأن من شأنها إحداث ضرر بالصحة العامة أو تضليل المستهلكين أو السلطات الرقابية.

وتعتبر البيانات كاذبة على الأخص إذا كانت تتعلق بهوية الدواء، أو مصدره، أو مكوناته، أو تاريخ صلاحيته، أو ظروف نقله وتخزينه.

يُعاقب بالسجن مدة لا تقل عن خمس سنوات ولا تزيد عن عشر سنوات إذا ترتب على الفعل ضرر جسيم بالصحة العامة.

تكون العقوبة السجن مدة لا تزيد على عشرين سنة، إذا ترتب على الفعل وفاة إنسان أو إصابته بعاهة مستديمة

مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر.

المذكرة الإيضاحية للمادة (٣): تستهدف هذه المادة بشكل مباشر "مشكلة الأوراكل" التي تمثل أخطر ثغرة في أنظمة التتبع. النص يتوافق مع مبدأ الشرعية من خلال تحديد الفعل (الإدخال العمدي) والركن المعنوي (العلم والإرادة) بدقة. هو لا يجرم الخطأ غير العمدي، بل يركز على السلوك الآثم. كما يتبنى النص سياسة عقابية متدرجة تربط جسامة العقوبة بجسامة الضرر الناتج، وهو ما يتوافق مع مبادئ العدالة والتناسب، ويضع حماية الحق في الحياة والسلامة الجسدية في قمة أولوياته.

مادة (٤): جريمة إنشاء أو إدارة عقد ذكي احتيالي

يُعاقب بالسجن وبغرامة تعادل ضعف قيمة الأموال المتحصلة، كل من أنشأ أو نشر أو أدار عقداً ذكياً، وهو يعلم أن تصميمه يهدف إلى الاستيلاء على أموال الغير بغير حق، أو إدارة مخطط استثماري احتيالي (كمخططات بونزي أو المخططات الهرمية).

المذكرة الإيضاحية للمادة (٤): هذه المادة تنشئ جريمة مستقلة تستهدف "العقل المدبر" للجريمة الرقمية. هي تجرم الفعل في مرحلة مبكرة (الإنشاء والنشر)، حتى قبل وقوع الضرر على الضحايا، مما يجعلها جريمة خطر تهدف إلى المنع الاستباقي. ربط الغرامة بقيمة الأموال المتحصلة يهدف إلى تجريد المجرمين من مكاسبهم غير المشروعة، تحقيقاً للردع الاقتصادي.

من منظور القانون الجنائي الاقتصادي، يُعرَّف "مخطط بونزي" بأنه عملية احتيال استثمارية منظمة، تقوم على جذب أموال المستثمرين من خلال تقديم وعود بعوائد مالية مرتفعة بشكل غير عادي وبمخاطر منخفضة أو منعدمة، إذ إن هذه العوائد المزعومة لا يتم توليدها من أي نشاط استثماري أو تجاري مشروع، بل يتم دفعها للمستثمرين القدامى باستخدام رؤوس الأموال التي يتم جمعها من المستثمرين الجدد.

عندما يتم تنفيذ مخطط بونزي من خلال "عقد ذكي"، فإن الكود البرمجي نفسه يصبح هو الأداة التي تنفذ "فعل التدوير" بشكل آلي. وهنا، يصبح فحص الكود المصدري للعقد الذكي دليلاً مادياً قاطعاً على وجود المخطط وتوافر القصد الجنائي لدى مصممه؛ لأن منطق الكود يكشف عن حتمية الانهيار وعدم وجود أي نشاط استثماري حقيقي.

الباب الثالث: المساهمة الجنائية في البيئات اللامركزية

مادة (٥): المساهمة الجنائية عبر توفير الأدوات التقنية

يُعد شريكاً في الجريمة، ويعاقب بعقوبة مخففة وفقاً للقواعد العامة، كل من صمم أو طور أو سوّق أو أدار كوداً برمجياً أو خدمة تقنية، مع علمه بأنها مصممة أساساً أو تستخدم بشكل جوهري لارتكاب أو تسهيل جريمة من الجرائم المنصوص عليها في هذا القانون أو غيره من القوانين.

ويستدل على هذا العلم بقرائن موضوعية، منها على سبيل الحصر:

- تصميم الخدمة بطريقة تتجاهل عمداً أي ضوابط أمنية أو رقابية معقولة.
- تسويق الخدمة أو الترويج لها في أوساط إجرامية أو على أنها وسيلة لتجنب إنفاذ القانون.
- الاستمرار في تشغيل الخدمة دون اتخاذ إجراءات فعالة بعد إخطاره بشكل متكرر من قبل السلطات المختصة باستخدامها في أنشطة إجرامية محددة.
- اعتماد نموذج ربح يعتمد بشكل أساس على العمولات من المعاملات غير المشروعة.

ولا تسري أحكام هذه المادة على مطوري البروتوكولات مفتوحة المصدر ذات الاستخدام المزدوج، ما لم يثبت توافر القصد الجنائي المباشر لديهم.

المذكرة الإيضاحية للمادة (٥): هذه المادة هي من أهم مواد القانون وأكثرها حساسية. هي تهدف إلى مساءلة مطوري "أدوات الجريمة" دون خنق الابتكار. النص لا يجرم كتابة الكود المحايد، بل يربط التجريم بـ "العلم" المستخلص من قرائن موضوعية وملموسة يمكن للادعاء إثباتها وللدفاع دحضها. الفقرة الأخيرة تمثل "ملاذاً آمناً" ضرورياً لحماية مطوري البرمجيات مفتوحة المصدر، وتضع عبء إثبات القصد المباشر على عاتق الادعاء، تماشياً مع مبدأ الأصل في الإنسان البراءة.

مادة (٦): **جريمة إعاقة التعقب الرقمي**

يُعاقب بالسجن لمدة سنة وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، كل من أدار "خدمة خلط" (Mixer) مع علمه بأنها تستخدم لإخفاء مصدر أموال متحصلة من جريمة.

وتطبق ذات العقوبة على كل من استخدم هذه الخدمة عمداً لذات الغرض.

المذكرة الإيضاحية للمادة (٦): هذه المادة تجرم غسل الأموال في صورته الرقمية الحديثة. هي لا تجرم مجرد استخدام الخلاطات (التي قد يكون لها استخدامات مشروعة للحفاظ على الخصوصية)، بل تربط التجريم بالركن المعنوي، وهو "العلم" بأن الأموال متحصلة من جريمة. هذا النص يتوافق مع توصيات مجموعة العمل المالي (FATF) بشأن تنظيم الأصول الافتراضية.

خدمة الخلط: هي أداة قوية لتعزيز إخفاء الهوية على البلوك تشين، تقع في منطقة رمادية بين حماية الخصوصية وتسهيل الجريمة. ومن منظور جنائي، هي تمثل "فعلاً مادياً" يمكن أن يشكل جريمة غسل أموال مستقلة أو إسهاما جنائيا في الجرائم الأصلية، ويتوقف تجريمها على قدرة الادعاء على إثبات القصد الجنائي لدى مشغلها أو مستخدمها، وهو ما يتم غالباً من خلال تحليل الظروف المحيطة بتشغيل الخدمة واستخدامها.

الباب الرابع: المسؤولية الجنائية للشخص المعنوي

مادة (٧): **مسؤولية الشخص المعنوي**

يكون الشخص المعنوي مسؤولاً جنائياً عن الجرائم المنصوص عليها في هذا القانون، إذا ارتكبت باسمه أو لحسابه أو لمنفعته من قبل أحد أعضائه أو ممثليه أو مديريه، أو إذا ثبت أن الجريمة قد وقعت بسبب إخلال جسيم بواجبات الرقابة والإشراف المفروضة عليه.

ويعاقب الشخص المعنوي بضعف الغرامة المقررة للجريمة، بالإضافة إلى واحد أو أكثر من التدابير التالية: المصادرة، الحل، الإغلاق، الحرمان من ممارسة أنشطة معينة، نشر الحكم.

ولا يخل ذلك بمسؤولية الشخص الطبيعي مرتكب الجريمة.

المذكرة الإيضاحية للمادة (٧): يتبنى هذا النص نموذجاً حديثاً لمسؤولية الشخص المعنوي لا يكتفي بنظرية "العقل المدبر"، بل يضيف أساساً آخر للمسؤولية وهو "الإخلال بواجبات الرقابة". هذا

يسمح بمساءلة الشركات التي تخلق "ثقافة مؤسسية" تتسامح مع الجريمة، حتى لو لم يصدر أمر مباشر من الإدارة العليا.

مادة (٨): مسؤولية الكيانات اللامركزية

في حالة ارتكاب الجريمة من خلال "منظمة مستقلة لا مركزية" (DAO) أو أي كيان مشابه ليس له شكل قانوني محدد، يجوز للمحكمة، بناءً على تحقيق تجريه، تحديد الأشخاص الطبيعيين أو الاعتباريين الذين يمارسون "سيطرة فعلية" على الكيان، ومساءلتهم بوصفهم فاعلين أصليين أو شركاء، بحسب الأحوال.

ويستدل على "السيطرة الفعلية" بقرائن منها على سبيل المثال:

- القدرة على تعديل الكود المصدري للكيان أو إيقافه من خلال مفاتيح إدارية.
- حيازة نسبة مؤثرة من الرموز المميزة (Tokens) التي تمنح حقوق التصويت على قرارات الكيان.
- الحصول على النصيب الأكبر من الأرباح الناتجة عن نشاط الكيان.

المذكرة الإيضاحية للمادة (٨): هذه المادة هي محاولة تشريعية مبتكرة لـ "ثقب حجاب اللامركزية". هي لا تعاقب الكيان اللامركزي غير المحدد، بل تمنح المحكمة سلطة البحث عن "المسيطرين الفعليين" خلف واجهة اللامركزية، وتضع معايير استرشادية لتحديدهم. هذا يحقق الردع دون مساءلة جميع المشاركين بشكل عشوائي، ويمنع استخدام اللامركزية كذريعة للإفلات من العقاب.

الرمز المُمَيَّز" (Token) هو أداة قانونية-تقنية مرنة، تعمل كتمثيل رقمي مشفر للحقوق على سجل موزع. إن تكييفه القانوني ومسؤوليته الجنائية لا يعتمدان على تقنيته، بل على الوظيفة الاقتصادية والحقوق التي يمنحها لحامله. لذلك، يجب على المشرع والقاضي أن ينظروا إلى "جوهر" الرمز وليس "شكله" لتحديد القواعد القانونية التي تنطبق عليه.

الباب الرابع: أحكام إجرائية وضمانات

مادة (٩): الضبط والتفتيش

لا يجوز تفتيش أو ضبط الأصول الافتراضية أو المفاتيح الخاصة إلا بناءً على أمر قضائي مسبب، ويجب أن يحدد الأمر بدقة الأصول أو العناوين المراد ضبطها، وأن يكون الإجراء ضرورياً ومتناسباً مع جسامة الجريمة.

مادة (١٠): حجية الأدلة الرقمية

تعتبر البيانات المستخرجة من سجل موزع دليلاً إلكترونياً مقبولاً في الإثبات، وتخضع لتقدير المحكمة.

ويقع على عاتق سلطة الاتهام عبء إثبات سلامة السجل التقنية، وصحة مصدر البيانات (الأوراكل) الذي قام بإدخالها، بأدلة مستقلة.

مادة (١١): حقوق الدفاع

يُكفل للمتهم في جميع مراحل التحقيق والمحاكمة الحق في الاستعانة بخبير فني من اختياره.

ويحق للدفاع، بناءً على طلب يقدم للمحكمة، الاطلاع على الكود المصدري للبروتوكول أو العقد الذكي المستخدم في ارتكاب الجريمة وفحصه، ما لم تقتض ضرورات الأمن القومي غير ذلك، وفي هذه الحالة تضع المحكمة ضوابط تضمن حق الدفاع في الاطلاع بشكل فعال.

المذكرة الإيضاحية للمواد (٩-١١): يهدف هذا الفصل إلى الموازنة بين فعالية التحقيق وحماية الحقوق. المادة (٩) تضع ضمانات للتفتيش تتوافق مع مبدأ التناسب. المادة (١٠) تقنن النتيجة التي توصل إليها البحث، حيث تجعل حجية الدليل "مشروطة" بإثبات حُجِّيَّة المصدر، حماية للمتهم من الأدلة الزائفة. المادة (١١) تكرس حقوقاً إجرائية جديدة ومهمة للدفاع، وهي "الحق في تدقيق الكود"، بوصفه ضمانة أساسية للمحاكمة العادلة في العصر الرقمي، وتحقيقاً لمبدأ "تكافؤ الأسلحة" بين الادعاء والدفاع.

مادة (١٢):

يجوز للمحكمة أن تحكم بمصادرة الأموال والأصول الافتراضية والأدوات والمتحصلات المتعلقة بالجريمة، وذلك مع عدم الإخلال بحقوق الغير حسن النية.

المذكرة الايضاحية للمادة (١٢)

تهدف هذه المادة إلى منح القضاء أداة إضافية لتحقيق الردع الاقتصادي، مع إعطاء المحكمة السلطة التقديرية اللازمة لتطبيقها بما يتناسب مع ظروف كل قضية على حدة. إن جعل المصادرة جوازية يتيح للقاضي الموازنة بين جسامة الفعل، ومقدار الأموال المتحصلة، وظروف الجاني الشخصية. فيمكنه أن يأمر بالمصادرة في الحالات التي تكون فيها المتحصلات كبيرة ودور الجاني رئيسياً، بينما قد يمتنع عن الحكم بها في الحالات التي تكون فيها قيمة الأموال بسيطة أو قد يترتب على المصادرة ضرر بالغ بأطراف أخرى حسنة النية (مثل أسرة المتهم). هذا النهج المرن يحقق التوازن بين تحقيق الردع ومبدأ تفريد العقاب.

المراجع:-

- إبراهيم، مدحت محمد عبد العزيز. (٢٠١٢). *المسؤولية الجنائية للاشتراك بالمساعدة: دراسة مقارنة* بين التشريعين المصري والفرنسي. دار النهضة العربية.
- أيوب، رشا فاروق. (٢٠١٧). *الاختصاص الجنائي العالمي*. دار النهضة العربية.
- حسني، محمود نجيب. (١٩٨٨). *النظرية العامة للقصد الجنائي: دراسة تأصيلية مقارنة بالركن المعنوي*. دار النهضة العربية.
- سرور، أحمد فتحي. (٢٠١٥). *الوسيط في قانون العقوبات: القسم العام*. (ط ٦). دار النهضة العربية.
- علام، عبد الرحمن حسين. (١٩٨٤). أثر الجهل أو الغلط في القانون على المسؤولية الجنائية. (رسالة دكتوراه غير منشورة). كلية الحقوق، جامعة القاهرة.
- عوض، محمد عوض. (٢٠٠٠). *قانون العقوبات: القسم العام*. دار الجامعة الجديدة للنشر، الإسكندرية.
- محمود، محمد زكي. (١٩٦٧). *آثار الجهل والغلط في المسؤولية الجنائية*. (رسالة دكتوراه غير منشورة)، كلية الحقوق، جامعة القاهرة.
- وزير، عبد العظيم مرسي. (٢٠٠٣). *شرح قانون العقوبات: القسم العام*. دار النهضة العربية.
- وزير، عبد العظيم مرسي. (١٩٨٩). افتراض الخطأ كأساس للمسؤولية الجنائية: دراسة مقارنة في النظامين اللاتيني والأنجلو أمريكي. دار النهضة العربية.

References

Abou-Nassar, E. M., T. M. A. Abou-Nassar, S. M. A. El-Ghareeb, & A. M. A. El-Ghareeb. (2020). A framework for securing the pharmaceutical supply chain using blockchain technology. *International Journal of Advanced Computer Science and Applications, 11*(10). https://doi.org/10.14569/IJACSA.2020.0111059

Alghasham, A. A. (2022). Counterfeit drugs: A growing global threat. *Saudi Pharmaceutical Journal, 30*(6), 643–652. https://doi.org/10.1016/j.jsps.2022.03.007

Anderson, D. (2023). *The Future of International Criminal Cooperation: A Network-Centric Approach*. Cambridge University Press.

Astill, J., Dara, R. A., Campbell, M., Farber, J. M., Fraser, E. D., Sharif, S., & Yada, R. Y. (2019). Transparency in food supply chains: A review of enabling technology solutions. *Trends in Food Science & Technology, 91*, 240-247. https://doi.org/10.1016/j.tifs.2019.07.024.

Bambara, C., & Schartum, D. W. (2021). Blockchain and the challenges of legal certainty: A case study of land registration. *Journal of Law, Information and Science, 30*(1), 1-25.

Bambauer, D. (2017). The extraterritorial reach of U.S. law. *University of Pennsylvania Journal of International Law, 39*(2), 319-368.

Bassiouni, M. C. (2019). *International Criminal Law: A Draft International Criminal Code* (4th ed.). Brill.

Brenner, S. W., & Koops, B. J. (2019). Approaches to cybercrime jurisdiction. *Journal of High Technology Law, 4*(1), 1-46.

Brophy, J., Be-Ube, B. C. K., & Orbih, O. C. (2021). The role of organized crime in the counterfeit pharmaceutical trade. *Journal of Financial Crime, 28*(4), 1183–1194. https://doi.org/10.1108/JFC-12-2020-0255

Brown, A. (2019). The Effectiveness of International Organizations in Criminal Cooperation: A Case Study of Eurojust. *Journal of International Criminal Justice, 17*(4), 789-812.

Butler, T., & Giuliano, L. (2018). The role of the 'oracle' in a blockchain system. *Journal of Information Technology & Politics, 15*(4), 345-358.

Casey, E., & Lundy, J. (2021). Blockchain and digital forensics: A new fron*Digital transformation: The future of forensic science* (pp. 217-235). Academic Press. https://doi.org/10.1016/B978-0-12-822283-9.00010-8.

Casey, E., Copeland, B. J., & de-Souza, J. D. L. N. (2019). The blockchain oracle problem in the context of digital forensics. *Digital Investigation, 28*, 123-133. https://doi.org/10.1016/j.diin.2019.01.007.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and

open issues. *Telematics and Informatics, 36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.006.

Chaudhry, P. E., & Stumpf, S. A. (2021). The challenge of counterfeit goods: A new research agenda. *Journal of Business Strategy, 42*(5), 346-354. https://doi.org/10.1108/JBS-09-2020-0205.

Chohan, U. W. (2019). The oracle problem: The challenge of real-world data integration in blockchain technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3364993

Choo, K. K. R. (2020). Cryptocurrency and blockchain-enabled crime. *Journal of Computer Information Systems, 60*(4), 301-312. https://doi.org/10.1080/08874417.2018.1480263.

Council of Europe. (2011). *Council of Europe Convention on the Falsification of Medical Products and Similar Crimes involving Threats to Public Health*. CETS No. 211.

Cupa, D. (2021). The right to confrontation in the age of algorithms: A challenge for criminal justice. *New Journal of European Criminal Law, 12*(3), 359-378. https://doi.org/10.1177/20322844211028392.

De Caria, R. (2019). The legal meaning of smart contracts. *European Journal of Risk Regulation, 10*(4), 731-751. https://doi.org/10.1017/err.2019.61

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Delepierre, F. (2019). The fight against falsified medicines: A new international momentum. *International Journal of Law, Crime and Justice, 56*, 53-61. https://doi.org/10.1016/j.ijlcj.2018.11.002

De-Strooper, S. (2018). The Court of Justice of the European Union's approach to jurisdiction in online defamation cases: A critical analysis. *Journal of Private International Law, 14*(3), 475-501.

Dine, J., & Koutsias, M. (2020). *The nature of corporate governance: The significance of national and cultural identity*. Edward Elgar Publishing.

Dorri, A., Luo, F., Rougier, N., Jurdak, R., & Kanhere, S. S. (2019). A secure and lightweight blockchain for IoT-based smart homes. *IEEE Transactions on*

Dependable and Secure Computing, 18(5), 2435-2449. https://doi.org/10.1109/TDSC.2019.2947919.

Du-Plessis, J. (2019). Blockchain, smart contracts and the future of contract law. *Potchefstroom Electronic Law Journal, 22*, 1-32. http://dx.doi.org/10.17159/1727-3781/2019/v22i0a5582

DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (pp. 157-177). Routledge.

Elliott, K. (2019). The challenge of classifying counterfeit medicines: A legal and ethical analysis. *Cambridge Quarterly of Healthcare Ethics, 28*(4), 678-688. https://doi.org/10.1017/S096318011900035X.

Epstein, J. (2018). The legal and regulatory challenges of blockchain technology. *The Journal of Corporation Law, 44*(3), 613-642.

Fairfield, J. A. (2018). The blockchain and the right to be forgotten. *University of Illinois Law Review, 2018*(1), 1-28.

Fan, L., He, S., & Luo, E. (2020). A survey on blockchain-based transaction privacy protection. *IEEE Systems Journal, 15*(2), 2496-2509. https://doi.org/10.1109/JSYST.2020.3005812

FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF.

Felbab-Brown, V. (2021). *The new drug scapes: How the COVID-19 pandemic is reshaping the global illicit drug trade*. The Brookings Institution. https://www.brookings.edu/research/the-new-drug-scapes/

Ferguson, A. G. (2017). The 'smart' Fourth Amendment. *Cornell Law Review, 102*(3), 547-614.

Finck, M. (2018). *Blockchain regulation and governance in Europe*. Cambridge University Press.

Finck, M. (2019). Blockchain and the general data protection regulation. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), *Regulating*

blockchain: Techno-social and legal challenges (pp. 87-105). Oxford University Press.

Fisse, B., & Braithwaite, J. (1993). *Corporations, crime and accountability*. Cambridge University Press.

Fitriana, A., & Adijaya, I. (2022). Corporate criminal liability in the falsification of medical products: A MEDICRIME Convention perspective. *Journal of Legal, Ethical and Regulatory Issues, 25*(S4), 1-11.

Gattinara, G. C., Hervey, D. K., & Mackey, T. K. (2018). The MEDICRIME Convention: A powerful new international tool to combat the public health threat of falsified medicines. *Global Health Action, 11*(1), 1528380. https://doi.org/10.1080/16549716.2018.1528380

Glass, D. (2018). Prosecuting counterfeit medicine crimes: A comparative analysis of causation and liability hurdles. *Journal of Criminal Law and Criminology, 108*(3), 495-532.

Goldsmith, J. (2018). The limits of universal jurisdiction. *New England Law Review, 47*(4), 865-892.

Grigg, I. (2020). The law of the ledger: The future of financial regulation. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), *Regulating Blockchain: Techno-Social and Legal Challenges* (pp. 123-145). Oxford University Press.

Hague Conference on Private International Law. (2020). *Report on the Judgments Project: Towards the Harmonization of Procedural Standards*. HCCH Publications.

Hasan, H. R., Salah, K., Jayaraman, R., Yaqoob, I., & Omar, M. (2019). A review on the use of blockchain for medicine traceability. *International Journal of Pharmaceutics, 572*, 118775. https://doi.org/10.1016/j.ijpharm.2019.118775.

Hess, D., & Broring, M. (2021). Criminal liability for blockchain-based systems: A German law perspective. *Computer Law & Security Review, 40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521.

Imwinkelried, E. J. (2019). The challenge of regulating expert testimony in the era of technology. *Vanderbilt Law Review, 72*(3), 845-882.

Johnson, D. R. (2019). The challenges of regulating online platforms. *Columbia Law Review, 119*(7), 1931-1984.

Johnson, R. (2020). Sovereignty Conflicts in International Criminal Law: The Dual Criminality Dilemma. *American Journal of International Law, 114*(3), 450-488.

Kaal, W. A. (2020). Decentralized autonomous organizations: The future of corporate governance or a legal black hole? *The Business Lawyer, 75*(4), 2135-2165.

Kamble, S. S., Gunasekaran, A., & Arha, H. (2020). Understanding the Blockchain technology adoption in agriculture supply chains: A systematic literature review and a conceptual framework. *International Journal of Production Research, 58*(11), 3380-3403. https://doi.org/10.1080/00207543.2019.1673222.

Kazem-Goudarzi, F. (2022). A critical analysis of the legal frameworks for combating counterfeit pharmaceuticals. *Journal of Health Policy and Law, 7*(2), 145-162.

Kharb, M. (2020). A review on counterfeit drugs: A major global problem. *Journal of Pharmaceutical Negative Results, 11*(1), 24-30.

Kingston, J. (2021). Artificial intelligence and the concept of mens rea. *Criminal Law and Philosophy, 15*(1), 113-132. https://doi.org/10.1007/s11572-020-09546-5

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005.

Kshetri, N. (2021). The role of blockchain in the governance of supply chains. *Journal of Business Research, 134*, 507-517. https://doi.org/10.1016/j.jbusres.2021.05.031.

Lee, S. (2021). A Comparative Analysis of Criminal Procedure in Common Law and Civil Law Systems. *International Journal of Comparative Law, 19*(1), 55-80.

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Levy, K. (2017). Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society, 3*, 1-15. https://doi.org/10.17351/ests2017.107.

Levy, K. (2017). Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society, 3*, 1-15. https://doi.org/10.17351/ests2017.107.

Lin, H. (2019). Cyber-attacks and the 'use of force' challenge. *Oxford Journal of Legal Studies, 39*(4), 747-775.

Loideain, N. N. (2020). The right to data protection in an era of surveillance capitalism. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 378*(2183), 20190367. https://doi.org/10.1098/rsta.2019.0367

Lopes, L. C., & Ossorio, P. (2021). Falsified and substandard medicines: A narrative review of the literature on the legal and regulatory framework. *BMJ Global Health, 6*(10), e006324. http://dx.doi.org/10.1136/bmjgh-2021-006324

Mackey, T. K., & Cuomo, R. E. (2021). A multi-pronged analysis of the MEDICRIME Convention: A new global health security treaty. *Global Health Action, 14*(1), 1948950. https://doi.org/10.1080/16549716.2021.1948950.

Mackey, T. K., & Liang, B. A. (2018). A United Nations global health and justice treaty to combat counterfeit medicines. *American Journal of Law & Medicine, 44*(2-3), 217-231. https://doi.org/10.1177/0098858818789508

Mackey, T. K., Nittas, N. A., & Liang, B. K. (2020). The Ebola-COVID-19 syndemic: A new global health security challenge for transnational pharmaceutical crime. *Journal of Global Health, 10*(2), 020383. https://doi.org/10.7189/jogh.10.020383

Margaron, M. (2020). The MEDICRIME Convention: Ratification and implementation challenges in a globalized world. *European Journal of Crime,*

Criminal Law and Criminal Justice, 28(3), 245-265. https://doi.org/10.1163/15718174-02803003

Martinez, J. (2018). Evidence in Transnational Crimes: Challenges and Solutions. *New York University Journal of International Law and Politics, 50*(4), 1125-1160.

Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1-3). IEEE. https://doi.org/10.1109/HealthCom.2016.7749510.

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real-world complexity. *Law, Innovation and Technology, 9*(2), 269-300. https://doi.org/10.1080/17579961.2017.1378333.

Mik, E. (2019). Smart contracts: A new era of contract law? *University of New South Wales Law Journal, 42*(4), 1375-1405.

Möser, M., Soska, K., & Christin, N. (2018, October). An empirical analysis of traceability in the Monero blockchain. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 143-163). ACM. https://doi.org/10.1145/3243734.3243757.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2020). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Paquet-Clouston, M., Haslhofer, B., & Karsai, M. (2019). Dubbing the blocks: A survey of blockchain analysis tools. *ACM Computing Surveys, 52*(4), 1–38. https://doi.org/10.1145/3329711.

Pisani, E. (2019). Quality of medicines in low- and middle-income countries: The "perfect storm". *BMJ Global Health, 4*(Suppl 5), e001049. https://doi.org/10.1136/bmjgh-2018-001049

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review, 1*(2), 305-341.

Reyns, B. W. (2021). Situational crime prevention and the criminology of the supply chain. *Criminology & Public Policy, 20*(3), 509-532. https://doi.org/10.1111/1745-9133.12551.

Riccardi, M. (2021). The fight against pharmaceutical crime. A multi-level analysis of a multi-faceted phenomenon. *Trends in Organized Crime, 24*(1), 1-21. https://doi.org/10.1007/s12117-019-09382-z

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access, 7*, 10127-10149. https://doi.org/10.1109/ACCESS.2019.2890507.

Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. *Computer Law & Security Review, 34*(3), 550-561. https://doi.org/10.1016/j.clsr.2017.11.008.

Sheyn, E. R. (2018). The E-Word: The Fourth Amendment in the age of blockchain

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press.

Sylvester, G. (2019). E-agriculture in action: Blockchain for agriculture. *Food and Agriculture Organization of the United Nations (FAO)*. https://www.fao.org/3/ca2906en/ca2906en.pdf

Tsagourias, N. (2017). The legal status of cyberspace. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (pp. 1-20). Edward Elgar Publishing.

Tziakouris, G. (2021). Jurisdiction in cyberspace: A new framework for international law. *International & Comparative Law Quarterly, 70*(2), 407-446.

UNODC. (2022). *Global Report on the Implementation of Mutual Legal Assistance Treaties*. United Nations Office on Drugs and Crime.

Vian, T. (2020). Anti-corruption, transparency, and accountability in the health sector. *Human Resources for Health, 18*(1), 70. https://doi.org/10.1186/s12960-020-00509-9.

Walch, A. (2019). Deconstructing 'decentralization': Exploring the core claim of crypto systems. In C. Brummer (Ed.), *Cryptoassets: Legal, regulatory, and monetary perspectives* (pp. 1-26). Oxford University Press.

Weber, R. H., Weber, R., & Olsson, P. (2019). *The Internet of Things: New security and privacy challenges*. In R. H. Weber & R. Weber (Eds.), *The Internet of Things: Legal and Regulatory Implications* (pp. 49-74). Springer. https://doi.org/10.1007/978-3-030-13726-1_3.

Wells, C. (2021). *Corporations and criminal responsibility* (3rd ed.). Oxford University Press.

Werbach, K. (2018). *The blockchain and the new architecture of trust*. The MIT Press.

Wexler, R. (2018). Life, liberty, and the pursuit of algorithmic fairness. In C. O'Neil & H. N. Pontell (Eds.), *The Cambridge Handbook of the Law and Policy of Algorithms* (pp. 123-145). Cambridge University Press.

Williams, P. (2021). An Analysis of Judicial Extradition Mechanisms: Delays and a Path Forward. *Stanford Law & Policy Review, 32*(2), 275-310.

Yeoh, P. (2021). The legal and regulatory implications of blockchain: A focus on financial services. *Journal of Financial Regulation and Compliance, 29*(2), 193-208. https://doi.org/10.1108/JFRC-07-2020-0071.

Yeoh, P. (2021). The legal and regulatory implications of blockchain: A focus on financial services. *Journal of Financial Regulation and Compliance, 29*(2), 193-208. https://doi.org/10.1108/JFRC-07-2020-0071.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review, 2018*(4), 1361-1406.

References:

• 'iibrahim, midahat muhamad eabd aleaziza. (2012). almaswuwliat aljinayiyat liliashtirak bialmusaeadati: dirasat muqaranat bayn altashrieayn almisrii walfaransi. dar alnahdat alearabiati.

• ayuba, rasha faruq. (2017). aliakhtisas aljinayiyu alealamiu. dar alnahdat alearabiati.

• hasini, mahmud najibi. (1988). alnazariat aleamat lilqasd aljanayiyi: dirasat tasiliat muqaranatan bialrukn almaenawii. dar alnahdat alearabiati.

• srur, 'ahmad fatahi. (2015). alwasit fi qanun aleuqubati: alqism aleama. (t 6). dar alnahdat alearabiati.

• ealami, eabd alrahman husayn. (1984). 'athar aljahl 'aw alghalat fi alqanun ealaa almaswuwliat aljinayiyati. (risalat dukturah ghayr manshuratin). kuliyat alhuquqi, jamieat alqahirati.

• eawad, muhamad eawad. (2000). qanun aleuqubati: alqism aleama. dar aljamieat aljadidat lilnashri, al'iiskandariati.

• mahmud, muhamad zaki. (1967). athar aljahl walghalat fi almaswuwliat aljinayiyati. (risalat dukturah ghayr manshuratin), kuliyat alhuquqi, jamieat alqahirati.

• wazir, eabd aleazim marsi. (2003). sharh qanun aleuqubati: alqism aleama. dar alnahdat alearabiati.

• wazir, eabd aleazim marsi. (1989). aftirad alkhata ka'asas lilmaswuwliat aljinayiyati: dirasat muqaranat fi alnizamayn allaatinii wal'anjilu 'amrikiun. dar alnahdat alearabia.

فهـــرس الموضوعـــات

الموضـــــوع الصفحة