ISSN: 1994-4217 (Print) 2518-5586(online)

Journal of College of Education

Available online at: https://eduj.uowasit.edu.iq

Asst. Lect. Abeer Tarif Razzaq

University of Wasit, College of Administration and Economics

Email: Arazak@uowasit.edu.iq

Keywords:

Cybercrime, Digital Evidence, Cybersecurity, Legal Technology

A r t i c l e i n f o

Article history:

Received 20. Apr 2026

Accepted 25. May.2026

Published 25. Aug.2026

Reconstructing the Legal Concept of Cybercrime in the Age of Artificial Intelligence: An Analytical Study of the Gap Between Law and Technology

A B S T R A C T

This study examines cybercrime as a complex legal–technological phenomenon that extends beyond the traditional framework of criminal law, raising fundamental questions regarding the redefinition of the core concepts of crime in the context of rapid digital transformation. The study is based on the premise that cybercrime is no longer merely a technological extension of conventional crime; rather, it has evolved into a hybrid ontological construct in which legal dimensions intersect with algorithmic and technological structures. This transformation has reshaped the fundamental concepts of the offender, criminal conduct, digital evidence, and criminal liability. The research adopts an analytical–comparative approach to deconstruct the conceptual framework of cybercrime through four principal dimensions: the theoretical foundation of cybercrime as a dual legal–technological entity, the legal ontology of cybercrime, the algorithmic reality of cybercrime in the era of artificial intelligence, and the evidentiary challenges posed by digital evidence in relation to traditional legal standards. Furthermore, the study explores the structural, epistemological, and practical gaps between law and technology and analyzes their impact on the effectiveness of conventional legal systems in addressing emerging cyber threats. The findings reveal an expanding gap between the normative logic of law, which is founded on relative stability and legal certainty, and the dynamic logic of technology, characterized by continuous innovation and algorithmic evolution. This discrepancy necessitates the reconstruction of fundamental legal concepts and the development of a more adaptive and integrated legal–technological framework capable of responding to the complexities of the digital environment.

DOI: https://doi.org/10.31185/eduj.Vol64.Iss2.5293

إعادة بناء المفهوم القانوني للجريمة السيبرانية في عصر الذكاء الاصطناعي: دراسة تحليلية في الفجوة بين القانون والتكنولوجيا

م.م. عبير ترف رزاق
جامعة واسط ـ كلية الإدارة والاقتصاد

الملخص

تتناول هذه الدراسة الجريمة السيبرانية بوصفها ظاهرة قانونية–تقنية مركّبة تتجاوز الإطار التقليدي للقانون الجنائي، لتطرح إشكاليات عميقة تتعلق بإعادة تعريف المفاهيم الأساسية للجريمة في ظل التحول الرقمي المتسارع. تنطلق الدراسة من فرضية مفادها أن الجريمة السيبرانية لم تعد مجرد امتداد تقني للجريمة التقليدية، بل أصبحت بنية أنطولوجية هجينة تتداخل فيها الأبعاد القانونية مع البنى الخوارزمية والتكنولوجية، مما أدى إلى إعادة تشكيل مفاهيم الفاعل، والفعل الإجرامي، والدليل، والمسؤولية الجنائية. اعتمدت الدراسة منهجًا تحليليًا–مقارنًا يهدف إلى تفكيك البنية المفاهيمية للجريمة السيبرانية من خلال أربعة محاور رئيسية: الإطار النظري للجريمة بوصفها كيانًا مزدوجًا قانونيًا وتقنيًا، الأنطولوجيا القانونية للجريمة السيبرانية، الواقع الخوارزمي للجريمة في ظل الذكاء الاصطناعي، وأزمة الإثبات الرقمي في مواجهة المعايير القانونية التقليدية. كما تناولت الدراسة الفجوة البنيوية والمعرفية والتطبيقية بين القانون والتكنولوجيا، وأثرها في إضعاف فعالية النظم القانونية التقليدية في مواجهة الجرائم الرقمية. وتوصلت الدراسة إلى أن هناك فجوة جوهرية متزايدة بين منطق القانون القائم على الثبات النسبي والمعيارية، ومنطق التكنولوجيا القائم على الديناميكية والتطور المستمر، مما يستدعي إعادة بناء المفاهيم القانونية وتطوير نموذج قانوني– تقني جديد أكثر مرونة وتكاملًا.

الكلمات المفتاحية: الجريمة السيبرانية، ، الأدلة الرقمية، الأمن السيبراني، التكنولوجيا القانونية.

١. المقدمة

شهد العالم خلال العقود الأخيرة تحوّلًا جذريًا في طبيعة الفعل الإجرامي نتيجة التوسع الهائل في استخدام التكنولوجيا الرقمية وتغلغلها في مختلف مجالات الحياة الإنسانية. فلم تعد الجريمة حبيسة الحيز المادي أو مرتبطة بحدود جغرافية واضحة، بل أصبحت تمارس في فضاء افتراضي مفتوح يتجاوز مفاهيم السيادة التقليدية، الأمر الذي أفرز نمطًا جديدًا من الجرائم يُعرف بالجريمة السيبرانية. هذا التحول لم يكن مجرد تطور تقني، بل يمثل نقلة نوعية في البنية المفاهيمية للجريمة ذاتها، حيث انتقل الفعل الإجرامي من كونه سلوكًا ماديًا محسوسًا إلى نشاط رقمي قائم على الخوارزميات والأنظمة المعلوماتية. إن المقاربات القانونية التقليدية، التي تأسست على مفاهيم مثل الركن المادي والركن المعنوي والعلاقة السببية، تواجه تحديات عميقة عند محاولة استيعاب هذا النمط المستحدث من الجرائم. فالفعل الإجرامي في البيئة الرقمية قد لا يكون مرئيًا أو ملموسًا، وقد يُنفّذ بواسطة أدوات برمجية أو أنظمة مؤتمتة دون تدخل بشري مباشر، مما يثير تساؤلات جوهرية حول مفهوم "الفاعل" وحدود المسؤولية الجنائية. كما أن الطبيعة اللامركزية للفضاء السيبراني تعقّد من مسألة الاختصاص القضائي، إذ يمكن أن تُرتكب الجريمة في بيئة موزعة عبر عدة دول في آنٍ واحد، وهو ما يضعف من فعالية الأطر القانونية الوطنية التقليدية ويستدعي إعادة النظر في مفهوم السيادة القانونية. وفي هذا السياق، برزت محاولات دولية لوضع إطار قانوني ناظم للجريمة السيبرانية، من أبرزها اتفاقية(Budapest Convention on Cybercrime) التي تُعد أول صك دولي ملزم يسعى إلى توحيد الجهود في مكافحة الجرائم الرقمية. كما تضطلع منظمات دولية مثل:

(United Nations) و (INTERPOL) بدور مهم في تعزيز التعاون الدولي وتطوير آليات المواجهة. ومع ذلك، فإن هذه الجهود لا تزال تواجه تحديات تتعلق بسرعة تطور التكنولوجيا مقارنة ببطء الاستجابة التشريعية، فضلًا عن اختلاف

الأنظمة القانونية بين الدول. تتجلى الإشكالية المركزية لهذه الدراسة في الفجوة المتنامية بين "الإدراك القانوني" للجريمة، الذي لا يزال يستند إلى تصورات تقليدية، و"الواقع التقني" الذي تحكمه بنى خوارزمية معقدة ومتغيرة باستمرار. فمع ظهور تقنيات الذكاء الاصطناعي والتعلم الآلي، لم يعد الفعل الإجرامي بالضرورة نتاج قرار بشري مباشر، بل قد يكون نتيجة تفاعل خوارزمي ذاتي، الأمر الذي يطرح تساؤلات غير مسبوقة حول القصد الجنائي وإمكانية إسناد المسؤولية. كما أن استخدام تقنيات التشفير وإخفاء الهوية يزيد من صعوبة تتبع الجناة وجمع الأدلة، مما يهدد فعالية النظام العدلي برمّته. انطلاقًا من ذلك، تهدف هذه الدراسة إلى إعادة مساءلة المفاهيم القانونية التقليدية للجريمة في ضوء التحولات الرقمية، ومحاولة بناء إطار تحليلي جديد يستوعب التداخل بين القانون والتكنولوجيا. كما تسعى إلى استكشاف مدى قدرة النظم القانونية الحالية على التكيف مع التحديات التقنية المتسارعة، وطرح تساؤلات نقدية حول الحاجة إلى تطوير نماذج قانونية أكثر مرونة وابتكارًا تتلاءم مع طبيعة الفضاء السيبراني.

أن الدراسة لا تقتصر على إعادة تعريف الجريمة، وإنما تمتد إلى تحليل المسؤولية والإثبات والاختصاص والحوكمة الرقمية لأنها ترتبط عضوياً بإعادة بناء المفهوم القانوني للجريمة.

المفاهيم والمصطلحات

الجريمة السيبرانية: تُعد الجريمة السيبرانية من أكثر المفاهيم القانونية تطورًا وتعقيدًا في العصر الرقمي، ويرجع ذلك إلى ارتباطها المباشر بالتطور المتسارع لتكنولوجيا المعلومات والاتصالات. ولا يوجد تعريف موحد متفق عليه عالميًا (محمد،٢٠٢٣، ص.٣١٠)، إلا أن معظم الفقه القانوني والاتفاقيات الدولية تجمع على أنها كل فعل غير مشروع يُرتكب باستخدام الحاسوب أو الشبكات الرقمية أو يكون موجهًا ضدها، ويترتب عليه الإضرار بسرية المعلومات أو سلامتها أو توافرها، أو الاعتداء على الحقوق والمصالح المحمية قانونًا (Council of Europe, 2001,pp.7–12).

ويعرفها Brenner (2010) بأنها مجموعة الأفعال الإجرامية التي تعتمد على البيئة الرقمية سواء بوصفها وسيلة لارتكاب الجريمة أو هدفًا لها، بحيث تصبح الأنظمة الحاسوبية والبيانات الإلكترونية جزءًا أساسيًا من النشاط الإجرامي.

أما Wall (2007) فيرى أن الجريمة السيبرانية تمثل تحولًا نوعيًا في مفهوم الجريمة، لأنها لا تعتمد على المكان المادي وإنما على فضاء افتراضي عابر للحدود، الأمر الذي يجعلها تختلف جذريًا عن الجرائم التقليدية من حيث طبيعتها ووسائل مكافحتها.

الأنطولوجيا القانونية: يقصد بالأنطولوجيا القانونية دراسة طبيعة الكيانات القانونية ووجودها وعلاقاتها داخل النظام القانوني، أي البحث في ماهية المفاهيم القانونية الأساسية مثل الشخص، والحق، والالتزام، والمسؤولية، والجريمة، وكيفية بنائها معرفيًا داخل القانون. ويعود أصل مفهوم الأنطولوجيا إلى الفلسفة، حيث يهتم بدراسة الوجود، ثم انتقل إلى الدراسات القانونية لتحليل البنية المفاهيمية للقواعد القانونية (Valente, 2005,p.42).

وفي سياق الجريمة السيبرانية، تعني الأنطولوجيا القانونية إعادة تحليل مفهوم الجريمة في ضوء البيئة الرقمية، وتحديد ما إذا كانت المفاهيم التقليدية لا تزال قادرة على تفسير الجرائم التي تنشأ داخل الفضاء السيبراني أو تحتاج إلى إعادة بناء (Breuker et al., 2009,p.15).

الواقع الخوارزمي: يشير الواقع الخوارزمي إلى البيئة التي تصبح فيها الخوارزميات العنصر الرئيس في تنظيم السلوك واتخاذ القرار داخل الأنظمة الرقمية، بحيث تؤثر في إنتاج الأفعال والنتائج بصورة قد تفوق التدخل البشري المباشر

(عايد،٢٠٢١، ص.٢٠١). وفي هذا الواقع لا تعمل الخوارزمية باعتبارها أداة تقنية فقط، وإنما باعتبارها منظومة تنظيمية تؤثر في العلاقات القانونية والاجتماعية(Yeung, 2018,p.505) .

وقد أصبح هذا المفهوم أكثر أهمية مع تطور الذكاء الاصطناعي، حيث أصبحت الخوارزميات قادرة على التعلم الذاتي وتحليل البيانات واتخاذ قرارات مستقلة نسبيًا، وهو ما يثير إشكاليات قانونية تتعلق بالمسؤولية والإسناد الجنائي (حسني،٢٠٢١) الخوارزمية: الخوارزمية هي مجموعة مرتبة من التعليمات أو الخطوات المنطقية المصممة لمعالجة البيانات أو حل مشكلة معينة أو تنفيذ مهمة محددة داخل النظام الحاسوبي. وتتميز الخوارزميات الحديثة بإمكانية تطوير أدائها من خلال التعلم الآلي وتحليل البيانات الضخمة، الأمر الذي يجعلها قادرة على إنتاج قرارات معقدة دون تدخل بشري مباشر (Russell & Norvig, 2021,p.704) .

وفي المجال القانوني أصبحت الخوارزميات تؤدي دورًا مؤثرًا في اتخاذ القرارات المتعلقة بالأمن السيبراني والتحقيقات الرقمية، كما أصبحت تستخدم أحيانًا في تنفيذ الهجمات الإلكترونية (عايد،٢٠٢١، ص.٢٠٣)

الذكاء الاصطناعي: يعرف الذكاء الاصطناعي بأنه فرع من علوم الحاسوب يهدف إلى تصميم أنظمة قادرة على محاكاة القدرات الذهنية البشرية، مثل التعلم والاستنتاج والتخطيط واتخاذ القرار(حسني،٢٠٢١). وقد تطور المفهوم ليشمل الأنظمة القادرة على التعلم الذاتي والتكيف مع البيئة المحيطة دون الحاجة إلى إعادة برمجتها بصورة مستمرة.
(Russell & Norvig, 2021, p.720) .

وفي سياق الجريمة السيبرانية، لا يمثل الذكاء الاصطناعي مجرد وسيلة تقنية، بل أصبح عنصرًا قادرًا على تطوير الهجمات الإلكترونية وتحليل الثغرات الأمنية وتنفيذ عمليات الاختراق بصورة مؤتمتة (Goodman, 2015,p.240).

الفاعل الخوارزمي:

الفاعل الخوارزمي هو نظام رقمي يعتمد على خوارزميات متقدمة أو تقنيات الذكاء الاصطناعي لتنفيذ قرارات أو أفعال بصورة مستقلة نسبيًا عن التدخل البشري المباشر (تيسير،٢٠٢٠). ولا يقصد بهذا المصطلح الاعتراف للخوارزمية بالشخصية القانونية، وإنما الإقرار بدورها المؤثر في إنتاج السلوك محل التقييم القانوني.
(Hilgendorf, 2019,p.810) .
ويُعد هذا المفهوم من أكثر المفاهيم إثارة للجدل في الفقه الجنائي الحديث، لأنه يثير تساؤلات حول إمكانية إسناد المسؤولية القانونية للأفعال التي تنتجها الأنظمة الذكية.

الأدلة الرقمية:

الأدلة الرقمية هي جميع المعلومات أو البيانات التي يتم إنشاؤها أو تخزينها أو نقلها بصيغة رقمية، والتي يمكن استخدامها لإثبات أو نفي واقعة قانونية أمام القضاء. وتشمل سجلات الأنظمة، ورسائل البريد الإلكتروني، وملفات الحاسوب، وسجلات الخوادم، والبيانات المستخرجة من الهواتف الذكية أو الشبكات الإلكترونية.
(Casey, 2011, pp. 18–34) .

وتتميز الأدلة الرقمية بسهولة نسخها أو تعديلها أو حذفها، الأمر الذي يفرض إجراءات تقنية وقانونية دقيقة لضمان سلامتها وحجيتها أمام القضاء.

سلسلة حفظ الدليل:

يقصد بسلسلة حفظ الدليل مجموعة الإجراءات القانونية والفنية التي توثق انتقال الدليل الرقمي منذ لحظة جمعه وحتى تقديمه أمام المحكمة، مع بيان الأشخاص الذين تعاملوا معه والوسائل المستخدمة في حفظه، بهدف ضمان عدم تعرضه للتغيير أو العبث (Casey, 2011, pp. 89–105) ، وتُعد سلامة سلسلة حفظ الدليل من الشروط الأساسية لقبول الأدلة الرقمية أمام المحاكم.

التكنولوجيا القانونية:

يقصد بالتكنولوجيا القانونية توظيف التقنيات الرقمية والذكاء الاصطناعي وتحليل البيانات في تقديم الخدمات القانونية ودعم عمليات التقاضي والتحقيق وصنع القرار القانوني(حسني،٢٠٢١) ويشمل ذلك استخدام الأنظمة الذكية في تحليل السوابق القضائية، وإدارة العقود، وتحليل الأدلة الرقمية، والتنبؤ بالمخاطر القانونية.
. (Susskind, 2019,p.253)

وأصبحت التكنولوجيا القانونية أحد المحاور الرئيسة في تحديث منظومة العدالة وتعزيز كفاءة المؤسسات القضائية.

الحوكمة الرقمية:

تشير الحوكمة الرقمية إلى مجموعة القواعد والمؤسسات والآليات التي تنظم استخدام التكنولوجيا والفضاء الرقمي بما يحقق التوازن بين الأمن الرقمي، وحماية الحقوق والحريات (ثامر،٢٠٢٢، ص.١٢)، وتعزيز التعاون الدولي في إدارة الفضاء السيبراني. وتمثل الحوكمة الرقمية إطارًا شاملًا لإدارة المخاطر القانونية والتقنية المرتبطة بالتحول الرقمي. .(United Nations, 2021,pp.7–9)

الإطار المنهجي للدراسة

أدت الثورة الرقمية المتسارعة إلى إحداث تحول جذري في طبيعة الجريمة، فلم تعد الجريمة السيبرانية مجرد امتداد إلكتروني للجرائم التقليدية، بل أصبحت ظاهرة قانونية وتقنية معقدة تمتلك خصائص مستقلة فرضتها البيئة الرقمية والأنظمة الذكية (محمد،٢٠٢٣، ص.٣١٣). وقد ساهم الانتشار الواسع للذكاء الاصطناعي، والتعلم الآلي، والخوارزميات الذاتية ، والحوسبة السحابية، وسلاسل الكتل، في ظهور أنماط جديدة من الجرائم تجاوزت حدود التصنيفات الجنائية التقليدية (عايد،٢٠٢١، ص.٢٠٥)، الأمر الذي أوجد تحديات غير مسبوقة أمام التشريعات الوطنية والدولية (Brenner, 2010, pp. 17–29؛ Wall, 2007, pp. 28–36).

وتتمثل الإشكالية الجوهرية للدراسة في أن القانون الجنائي لا يزال يستند إلى مفاهيم تأسست في ظل البيئة المادية التقليدية، حيث يقوم على افتراض أن الجريمة هي فعل مادي يصدر عن شخص طبيعي داخل نطاق إقليمي محدد، في حين أن الجريمة السيبرانية الحديثة أصبحت تُرتكب داخل فضاء افتراضي يتجاوز الحدود الجغرافية، وقد تنفذها أنظمة ذكية أو برمجيات ذاتية التشغيل، الأمر الذي يجعل مفاهيم الفاعل الجنائي، والقصد الجرمي، والاختصاص القضائي، والأدلة الجنائية، بحاجة إلى إعادة قراءة في ضوء الواقع الرقمي الجديد (Lessig, 2006, pp. 120–138؛ Yar, 2013, pp. 52–68).

وتزداد أهمية هذه الإشكالية مع تزايد الاعتماد العالمي على تقنيات الذكاء الاصطناعي في القطاعات الاقتصادية والأمنية والإدارية (تيسير،٢٠٢٠)، إذ لم يعد الخطر مقتصرًا على استخدام التكنولوجيا في ارتكاب الجريمة، وإنما أصبح يتمثل في إمكانية أن تكون التكنولوجيا نفسها عنصرًا فاعلًا في إنتاج السلوك الإجرامي أو تسهيله أو تطويره، وهو ما يفرض على الفقه الجنائي إعادة النظر في الأسس النظرية التي يقوم عليها مفهوم الجريمة ذاته.
. (Goodman, 2015, pp. 71–89)

وانطلاقًا من ذلك، تسعى هذه الدراسة إلى معالجة الفجوة القائمة بين البنية القانونية التقليدية والواقع التقني المعاصر، من خلال إعادة بناء المفهوم القانوني للجريمة السيبرانية في ضوء التطورات الخوارزمية والذكاء الاصطناعي، وتحليل مدى قدرة التشريعات الحالية على استيعاب هذا التحول.

تستمد هذه الدراسة أهميتها من التحولات الجوهرية التي يشهدها القانون الجنائي نتيجة الثورة الرقمية، إذ لم تعد الجريمة السيبرانية مجرد موضوع متخصص في مجال أمن المعلومات، وإنما أصبحت إحدى أكثر القضايا القانونية تعقيدًا على المستويين الوطني والدولي. فمع تطور التقنيات الرقمية وظهور أنظمة الذكاء الاصطناعي القادرة على اتخاذ قرارات مستقلة، برزت تحديات جديدة تتعلق بتحديد المسؤولية الجنائية، وإثبات الأفعال الرقمية، وتحديد الاختصاص القضائي، الأمر الذي جعل إعادة تقييم المفاهيم القانونية التقليدية ضرورة علمية وتشريعية ملحة.
. (Brenner, 2010, pp. 33–40)

وتبرز أهمية الدراسة من الناحية النظرية في أنها تقدم قراءة فلسفية وقانونية حديثة للجريمة السيبرانية بوصفها ظاهرة هجينة تجمع بين القانون والتكنولوجيا، وتتجاوز التصورات التقليدية التي تنظر إلى التكنولوجيا باعتبارها مجرد وسيلة لارتكاب الجريمة. كما تسهم الدراسة في تطوير الأدبيات القانونية المتعلقة بالأنطولوجيا القانونية للجريمة الرقمية، وإعادة تفسير مفاهيم الفاعل الجنائي، والقصد الإجرامي، والدليل الرقمي، في ضوء التحولات التي فرضها الذكاء الاصطناعي .(Lessig, 2006, pp. 5–15)

أما من الناحية التطبيقية، فإن الدراسة تقدم إطارًا تحليليًا يمكن أن يفيد المشرعين، والسلطات القضائية، وواضعي السياسات العامة (عبد الله، ٢٠٢٣، ص.١١٥)، في تطوير تشريعات أكثر مرونة وقادرة على مواكبة التطور التقني، كما تدعم جهود التعاون الدولي في مكافحة الجرائم السيبرانية من خلال اقتراح نموذج قانوني أكثر تكاملًا بين البعدين القانوني والتقني (Casey, 2011, pp. 25–39؛Wall, 2007, pp. 181–196).

تهدف هذه الدراسة إلى إعادة تحليل المفهوم القانوني للجريمة السيبرانية في ضوء التحولات التي فرضها الذكاء الاصطناعي والأنظمة الخوارزمية، وبيان أوجه القصور التي تعاني منها النظرية الجنائية التقليدية في تفسير الجرائم الرقمية المستحدثة (محمد،٢٠٢٣، ص.٣١٧). كما تسعى إلى تحليل العلاقة بين القانون والتكنولوجيا، والكشف عن طبيعة الفجوة البنيوية والمعرفية بينهما، وتقييم مدى كفاية التشريعات الوطنية والدولية في مواجهة التحديات الرقمية (مجيد،٢٠٢٤). وتهدف الدراسة كذلك إلى بناء إطار قانوني–تقني جديد يقوم على التكامل بين المبادئ القانونية والتطورات التقنية، بما يعزز من كفاءة المنظومة القانونية في مواجهة الجرائم السيبرانية المستقبلية.

.(Yar, 2013, pp. 101–118)

تنطلق الدراسة من مجموعة من التساؤلات الرئيسة التي تشكل محور التحليل، وفي مقدمتها: هل ما تزال المفاهيم التقليدية للجريمة قادرة على تفسير طبيعة الجريمة السيبرانية في عصر الذكاء الاصطناعي؟ وهل يمكن اعتبار الأنظمة الخوارزمية عنصرًا مؤثرًا في المسؤولية الجنائية؟ وما طبيعة الفجوة البنيوية والمعرفية بين القانون والتكنولوجيا؟ وإلى أي

مدى تستطيع التشريعات الحالية مواكبة التحولات المتسارعة في البيئة الرقمية؟ وهل أصبح من الضروري إعادة بناء المفهوم القانوني للجريمة بما يتلاءم مع الواقع الخوارزمي الجديد؟

تنطلق الدراسة من فرضية رئيسة مؤداها أن التطور التقني المتسارع قد أدى إلى تجاوز الإطار المفاهيمي التقليدي للجريمة، الأمر الذي أوجد فجوة بنيوية بين القانون والتكنولوجيا. كما تفترض الدراسة أن الأنظمة الذكية والخوارزميات أصبحت تؤدي دورًا مؤثرًا في إنتاج السلوك الإجرامي، وأن التشريعات الحالية لم تعد كافية لمعالجة هذا التحول، وهو ما يستوجب تطوير نموذج قانوني جديد أكثر مرونة وتكاملاً مع التطورات التقنية(Goodman, 2015, pp. 212–227) .

اعتمدت الدراسة المنهج التحليلي النقدي بوصفه المنهج الرئيس، لتحليل المفاهيم القانونية المرتبطة بالجريمة السيبرانية، والكشف عن أوجه القصور التي تعاني منها النظرية الجنائية التقليدية عند تطبيقها على البيئة الرقمية. كما استعانت بالمنهج المقارن لتحليل أوجه الاختلاف والتشابه بين النماذج القانونية الأوروبية والأنجلوسكسونية والعربية، وتقييم مدى كفاءة كل منها في مواجهة الجرائم السيبرانية (عبد الله، ٢٠٢٣، ص.١١٦). وإلى جانب ذلك، اعتمدت الدراسة على استقراء مستقبل التنظيم القانوني في ظل التطورات المتسارعة للذكاء الاصطناعي والخوارزميات (نايف،٢٠٢٢)، مع الاستناد إلى الأدبيات القانونية الحديثة، والاتفاقيات الدولية، والدراسات المقارنة لبناء نموذج تحليلي متكامل. . (Kerr, 2003, pp. 357)

تركز هذه الدراسة على تحليل الجريمة السيبرانية من منظور قانوني وتقني، مع الاهتمام بإعادة بناء المفاهيم القانونية المرتبطة بالفاعل والمسؤولية والإثبات والاختصاص القضائي في ضوء التحولات الرقمية. ولا تتناول الدراسة الجوانب البرمجية أو الهندسية الخاصة بتصميم الأنظمة أو تطوير البرمجيات، إلا بالقدر الذي يخدم التحليل القانوني ويُسهم في تفسير طبيعة الجريمة السيبرانية.

يتكون البحث من مجموعة من المحاور المترابطة تبدأ بالمقدمة والإطار المنهجي، ثم الإطار النظري، فالأنطولوجيا القانونية للجريمة السيبرانية، وتحليل الواقع الخوارزمي، وأزمة الإثبات الرقمي، والفجوة بين القانون والتكنولوجيا، ثم عرض النموذج القانوني– التقني المقترح، يليه التحليل المقارن للنماذج القانونية المختلفة، ثم مناقشة مستقبل الجريمة في عصر الذكاء الاصطناعي، وصولًا إلى النتائج والتوصيات.

٢. إعادة التأطير النظري: الجريمة السيبرانية كظاهرة أنطولوجية هجينة

تفرض التحولات الرقمية المتسارعة إعادة نظر جذرية في الأطر النظرية التي طالما استند إليها الفكر القانوني في تعريف الجريمة وتحليل عناصرها، إذ لم يعد بالإمكان التعامل مع الجريمة السيبرانية بوصفها امتدادًا بسيطًا للجريمة التقليدية، بل أضحت تمثل نمطًا وجوديًا (أنطولوجيًا) مغايرًا يتداخل فيه القانوني مع التقني بصورة مركّبة (محمد،٢٠٢٣، ص.٨٦). فالجريمة في هذا السياق لا تتحدد فقط من خلال النصوص القانونية، وإنما أيضًا من خلال البنية الخوارزمية التي تُنتج الفعل الإجرامي وتشكّل شروط إمكانه، وهو ما يستدعي تبني مقاربة تحليلية تتجاوز الثنائية التقليدية بين الفعل والفاعل نحو فهم أكثر تعقيدًا قائم على التفاعل بين الإنسان والتكنولوجيا(Wall, 2007,p.10; Yar, 2013,p.6) .

الجريمة السيبرانية ككيان مزدوج (قانوني–تقني)

ينطلق المفهوم التقليدي للجريمة من اعتبارها سلوكًا إنسانيًا إراديًا يخالف قاعدة قانونية ويستوجب جزاءً، وهو تصور راسخ في الفقه الجنائي. غير أن هذا الفهم يصبح محدودًا عند نقله إلى الفضاء السيبراني، حيث يتراجع الدور المباشر للفاعل البشري لصالح أنماط من التفاعل الرقمي المعقد الذي قد يتم عبر وسائط برمجية أو أنظمة مؤتمتة (محمد،٢٠٢٣،

ص.٨٨). فالفعل الإجرامي لم يعد بالضرورة نتيجة قرار بشري مباشر في لحظة زمنية محددة، بل قد يكون نتيجة سلسلة من العمليات الرقمية التي تبدأ بتدخل بشري وتنتهي بتنفيذ آلي داخل نظام معلوماتي(Brenner, 2010,p.21) .

من هنا، يمكن النظر إلى الجريمة السيبرانية بوصفها كيانًا مزدوجًا يجمع بين بعدين متلازمين: البعد القانوني الذي يحدد الإطار المعياري للسلوك، والبعد التقني الذي يحدد كيفية تحقق هذا السلوك داخل البيئة الرقمية. وهذا التداخل يجعل من الضروري تحليل الجريمة ليس فقط من زاوية النص القانوني، بل أيضًا من خلال فهم البنية التقنية التي تُنتجها، بما في ذلك الخوارزميات والأنظمة المعلوماتية. (Kerr, 2003,p.358) .

وتبرز في هذا السياق إشكالية "الفاعل" بوصفها نقطة ارتكاز في إعادة بناء النظرية الجنائية للجريمة السيبرانية. ففي حين يفترض القانون الجنائي التقليدي أن الفاعل هو شخص طبيعي يتمتع بالإرادة والوعي، فإن البيئة الرقمية تطرح نموذجًا جديدًا يتمثل في "الفاعل الخوارزمي"، أي النظام البرمجي القادر على تنفيذ أفعال واتخاذ قرارات ضمن نطاق معين دون تدخل بشري مباشر. وقد أشار (Lawrence Lessig) إلى أن "الكود" لا يُعد مجرد أداة تقنية، بل يمثل بنية تنظيمية تتحكم في السلوك داخل الفضاء الرقمي، بحيث يمكن اعتباره نظيرًا وظيفيًا للقانون نفسه(Lessig, 2006,p.3) . هذا الطرح يفتح المجال أمام تساؤلات عميقة حول مدى إمكانية إسناد المسؤولية الجنائية إلى كيانات غير بشرية، أو على الأقل إعادة توزيع المسؤولية بين المبرمج والمستخدم والنظام (علي، ٢٠٢٢).

من الفعل الإجرامي إلى السلوك البرمجي

يمثل الانتقال من الفعل الإجرامي التقليدي إلى "السلوك البرمجي" أحد أبرز التحولات المفاهيمية التي تفرضها الجريمة السيبرانية (محمد،٢٠٢٣، ص.٩١). فالفعل الإجرامي في البيئة الرقمية لا يتجسد في حركة مادية ملموسة، بل في تعليمات برمجية تُنفذ داخل أنظمة معلوماتية، مما يجعل "الكود" هو الوحدة الأساسية للتحليل. فالهجمات السيبرانية، على سبيل المثال، تتم من خلال تنفيذ أوامر رقمية تستهدف اختراق الأنظمة أو تعطيلها أو التلاعب ببياناتها، وهو ما يعكس تحولًا من الفعل المادي إلى الفعل الرقمي (Brenner, 2010,p.23; Wall, 2007,p.12).

في هذا السياق، يطرح مفهوم "Code as Conduct" الذي صاغه (Lawrence Lessig)رؤية مفادها أن الكود لا يقتصر على تنفيذ الأوامر، بل يحدد أيضًا حدود السلوك الممكن داخل الفضاء الرقمي، وبالتالي فإنه يشكل نمطًا من التنظيم السلوكي(Lessig, 2006,p.4) . وبذلك، فإن الجريمة السيبرانية لا تُفهم فقط من خلال نية الفاعل، بل أيضًا من خلال تصميم النظام البرمجي الذي يتيح أو يقيّد هذا السلوك.

وتزداد هذه المسألة تعقيدًا مع ظهور الأنظمة الذاتية التشغيل، مثل أنظمة الذكاء الاصطناعي، التي تمتلك القدرة على التعلم واتخاذ القرارات بناءً على تحليل البيانات دون تدخل بشري مباشر (متولي،٢٠٢١). ففي مثل هذه الحالات، قد يصبح من الصعب تحديد ما إذا كان الفعل الإجرامي ناتجًا عن إرادة بشرية أم عن سلوك مستقل للنظام، وهو ما يطرح تحديات غير مسبوقة أمام القانون الجنائي، خاصة فيما يتعلق بإثبات القصد الجنائي وتحديد المسؤولية.
. (Hilgendorf, 2019,p.921)

وعليه، فإن إعادة تأطير الجريمة السيبرانية بوصفها "سلوكًا برمجيًا" يقتضي تطوير أدوات تحليل جديدة تدمج بين الفهم القانوني والتحليل التقني، وتأخذ في الاعتبار الطبيعة الخوارزمية للفعل الإجرامي. كما يستدعي ذلك إعادة النظر في المفاهيم الأساسية للقانون الجنائي، بحيث تصبح أكثر قدرة على استيعاب واقع رقمي يتسم بالتعقيد والتغير المستمر.

. (Yar, 2013,p.9)

٣. الأنطولوجيا القانونية للجريمة السيبرانية

يُعدّ البحث في الأنطولوجيا القانونية للجريمة السيبرانية مدخلًا تحليليًا ضروريًا لفهم طبيعة هذا النمط المستحدث من الجرائم، إذ لا يتعلق الأمر بمجرد تطبيق قواعد قانونية قائمة على وقائع جديدة، بل بإعادة مساءلة الأسس المفاهيمية التي يقوم عليها القانون الجنائي ذاته. فالجريمة السيبرانية تطرح تحديًا مزدوجًا يتمثل في تفكيك البنية التقليدية للمفاهيم القانونية، وفي الوقت ذاته فرض واقع تقني يتطلب إعادة بناء هذه المفاهيم بما يتلاءم مع بيئة رقمية معقدة وعابرة للحدود.

قصور البنية القانونية التقليدية

تُظهر الجريمة السيبرانية بوضوح حدود البنية القانونية التقليدية التي صُممت أساسًا للتعامل مع أفعال مادية تقع ضمن نطاق جغرافي محدد. فعند محاولة تطبيق هذه البنية على الجرائم الرقمية، تبرز إشكالية "التكييف القانوني"، أي صعوبة إدراج الفعل السيبراني ضمن أوصاف قانونية قائمة. فاختراق نظام معلوماتي، على سبيل المثال، قد لا يندرج بسهولة ضمن جرائم السرقة أو الاعتداء التقليدية، نظرًا لغياب العنصر المادي الملموس، وهو ما يؤدي إلى فجوات تشريعية أو إلى تأويلات موسعة قد تفتقر إلى الدقة(Kerr, 2003,p.359) .

وتتعمق هذه الإشكالية عند النظر إلى أزمة المفاهيم الأساسية في القانون الجنائي، مثل النية، والفعل، والضرر. فالنية، التي تُعد ركنًا جوهريًا في المسؤولية الجنائية (علي،٢٠٢٢، ص.٤٥)، تصبح أكثر تعقيدًا في البيئة الرقمية، حيث يمكن أن تُنفذ الأفعال بواسطة برامج أو خوارزميات تعمل بشكل مستقل أو شبه مستقل (عايد،٢٠٢١، ص.٢٠٧)، مما يثير التساؤل حول مدى إمكانية إسناد القصد الجنائي إلى الفاعل البشري في كل الحالات. كما أن مفهوم "الفعل" ذاته يتعرض لإعادة تعريف، إذ لم يعد يقتصر على سلوك مادي، بل يشمل أيضًا أوامر برمجية غير مرئية.

. (Brenner, 2010,p.33)

أما الضرر، وهو عنصر أساسي في تجريم السلوك، فإنه في الجريمة السيبرانية قد يكون غير ملموس أو مؤجل الظهور، كما في حالات اختراق البيانات أو سرقة المعلومات، حيث لا يكون الضرر فوريًا أو ماديًا بالمعنى التقليدي (محمد،٢٠٢٣، ص.٩٣). هذا التحول يفرض على القانون إعادة التفكير في معايير تقدير الضرر ومدى كفايته لقيام الجريمة. (Wall, 2007,p.43) .

قراءة نقدية للاتفاقيات الدولية

في مواجهة هذه التحديات، سعت الأسرة الدولية إلى تطوير أطر قانونية مشتركة لتنظيم الفضاء السيبراني، ويُعد من أبرزها اتفاقية (Budapest Convention on Cybercrime)، التي تمثل أول محاولة دولية شاملة لتوحيد التشريعات المتعلقة بالجريمة السيبرانية (مجيد،٢٠٢٤) وقد هدفت هذه الاتفاقية إلى وضع تعريفات موحدة للجرائم الرقمية، وتعزيز التعاون الدولي في مجالات التحقيق وتسليم المجرمين وتبادل الأدلة.

ورغم الأهمية البالغة لهذه الاتفاقية، إلا أنها لم تسلم من النقد، خاصة فيما يتعلق بطابعها الأوروبي وعدم شمولها لكافة الدول، فضلًا عن محدودية قدرتها على مواكبة التطورات التقنية المتسارعة. كما أن بعض أحكامها تثير إشكاليات تتعلق بالسيادة الوطنية، خصوصًا فيما يتعلق بآليات الوصول إلى البيانات عبر الحدود(Yar, 2013,p.13) .

من جهة أخرى، تضطلع (United Nations) بدور متزايد في تنظيم الفضاء السيبراني من خلال مبادرات متعددة تهدف إلى تعزيز الأمن السيبراني ووضع معايير دولية للسلوك المسؤول في الفضاء الرقمي. ومع ذلك، فإن جهود الأمم المتحدة لا تزال تواجه تحديات تتعلق بتباين مواقف الدول واختلاف أولوياتها، مما يحد من إمكانية التوصل إلى إطار قانوني دولي ملزم وموحد(Goodman, 2015,p.45) .

إشكالية الاختصاص والسيادة الرقمية

تُعد مسألة الاختصاص القضائي من أكثر القضايا تعقيدًا في سياق الجريمة السيبرانية، نظرًا لطبيعتها العابرة للحدود. فالجريمة قد تُرتكب من دولة، وتستهدف ضحية في دولة أخرى، بينما تُخزن البيانات في دولة ثالثة، وهو ما يخلق تداخلًا بين عدة أنظمة قانونية ويطرح تساؤلات حول الجهة المختصة بالتحقيق والمحاكمة(Kerr, 2003,p.359) .

هذا الوضع يؤدي إلى ما يمكن تسميته بـ" السيادة الرقمية"، حيث تجد الدول نفسها غير قادرة على فرض قوانينها بشكل فعال داخل الفضاء السيبراني. كما أن تعارض الأنظمة القانونية بين الدول، سواء من حيث تعريف الجريمة أو الإجراءات الجنائية، يزيد من تعقيد التعاون الدولي ويؤدي في بعض الأحيان إلى إفلات الجناة من العقاب.

. (Brenner, 2010,p.35)

وعلاوة على ذلك، فإن غياب إطار دولي موحد ينظم مسألة الاختصاص يفتح المجال أمام ممارسات قد تمس حقوق الأفراد، مثل الوصول غير المشروع إلى البيانات أو انتهاك الخصوصية بحجة مكافحة الجريمة. ومن ثمّ، فإن معالجة هذه الإشكالية تتطلب إعادة التفكير في مفهوم السيادة في العصر الرقمي، والانتقال نحو نماذج أكثر مرونة تقوم على التعاون والتنسيق الدولي بدلًا من الانغلاق القانوني(Wall, 2007,p.46) .

٤. الواقع الخوارزمي للجريمة السيبرانية

لم تعد الجريمة السيبرانية تُفهم بوصفها مجرد نشاط بشري يستخدم أدوات رقمية، بل أصبحت اليوم تتخذ شكلًا أكثر تعقيدًا يتمثل في "واقع خوارزمي" تتحكم فيه الأنظمة الذكية، وتعيد فيه البرمجيات المتقدمة تشكيل طبيعة الفعل الإجرامي ذاته (محمد،٢٠٢٣، ص.٣٢١). هذا التحول يعكس انتقال الجريمة من كونها فعلًا فرديًا محدودًا إلى منظومة تقنية–اقتصادية–معرفية تتداخل فيها الخوارزميات، والبيانات، والذكاء الاصطناعي، مما يفرض إعادة صياغة المفاهيم التقليدية للجريمة والأدلة والمسؤولية. (Wall, 2007,p.65; Brenner, 2010,p.75) .

الجريمة المؤتمتة

تشير الجريمة المؤتمتة إلى ذلك النمط من الأفعال الإجرامية التي تُنفذ بشكل كلي أو جزئي بواسطة أنظمة ذكية أو برمجيات مؤتمتة دون تدخل بشري مباشر في كل مرحلة من مراحل التنفيذ. في هذا السياق، لم يعد الإنسان هو الفاعل الوحيد، بل أصبح الذكاء الاصطناعي عنصرًا فاعلًا في إنتاج السلوك الإجرامي أو توسيعه أو تحسين كفاءته (حسني،٢٠٢١).

إن بروز الذكاء الاصطناعي كفاعل غير بشري يطرح إشكالية قانونية وفلسفية عميقة تتعلق بإعادة تعريف مفهوم "الفاعل الجنائي". فالنظام الذكي، خاصة عندما يكون قائمًا على التعلم العميق (علي،٢٠٢٢، ص.٤٧)، قد يقوم بتنفيذ عمليات معقدة مثل تحليل الثغرات الأمنية أو تنفيذ هجمات سيبرانية موجهة دون تدخل بشري مباشر في كل خطوة. هذا ما يجعل تحديد المسؤولية الجنائية أكثر تعقيدًا، إذ يتداخل دور المبرمج والمستخدم والنظام ذاته في إنتاج الفعل الإجرامي .(Goodman, 2015,p.47)

كما أن الهجمات القائمة على التعلم الآلي تمثل تطورًا نوعيًا في طبيعة الجريمة السيبرانية، حيث يتم استخدام خوارزميات قادرة على تحليل الأنظمة المستهدفة وتكييف الهجوم بشكل ديناميكي وفقًا لردود الفعل الدفاعية (عايد،٢٠٢١، ص.٢١٠). وهذا النوع من الجرائم لا يعتمد على نمط ثابت، بل يتغير باستمرار، مما يجعل اكتشافه أو التنبؤ به أكثر صعوبة، ويحد من فعالية أدوات المكافحة التقليدية(Brenner, 2010,p.80) .

إخفاء الهوية والتشفير

يشكل إخفاء الهوية وتقنيات التشفير أحد أبرز التحديات التي تواجه أنظمة العدالة الجنائية في العصر الرقمي. فهذه التقنيات، رغم أهميتها في حماية الخصوصية وتعزيز الأمن الرقمي، تُستخدم أيضًا كوسائل فعالة لإخفاء هوية الجناة وإعاقة عمليات التتبع والتحقيق.

إن القدرة على إخفاء الهوية داخل الفضاء السيبراني تؤدي إلى إعادة تشكيل العلاقة بين الجريمة والفاعل، حيث يصبح من الصعب ربط الفعل الإجرامي بشخص محدد أو جهة معينة (تيسير،٢٠٢٠). وهذا ما يؤدي إلى ما يمكن تسميته بـ"تآكل قابلية الإسناد الجنائي"، أي ضعف القدرة على إسناد الفعل إلى فاعل قانوني واضح، وهو ما يمثل تحديًا جوهريًا في القانون الجنائي التقليدي(Kerr, 2003,p.360) .

وفي السياق ذاته، يؤدي التشفير القوي إلى ما يشبه "انهيار مفهوم الدليل التقليدي"، إذ لم تعد الأدلة المادية أو الرقمية قابلة للوصول أو الفهم بسهولة دون مفاتيح خاصة أو أدوات تحليل متقدمة. وهذا يضعف من فعالية أنظمة الإثبات القائمة على الوصول المباشر إلى البيانات، ويفرض الحاجة إلى تطوير نماذج جديدة في التعامل مع الأدلة الرقمية تأخذ في الاعتبار طبيعتها الديناميكية والمعقدة(Yar, 2013,p.19) .

الاقتصاد الخفي للجريمة السيبرانية

لا يمكن فهم الجريمة السيبرانية المعاصرة دون تحليل البعد الاقتصادي الذي أصبح جزءًا أساسيًا من بنيتها. فقد نشأت في الفضاء الرقمي ما يمكن تسميته بـ"الاقتصاد الخفي للجريمة السيبرانية"، وهو نظام اقتصادي غير رسمي يعتمد على تبادل الخدمات والبيانات والبرمجيات الخبيثة في بيئات رقمية مغلقة أو شبه مغلقة(Wall, 2007,p.155).

تتجلى أبرز مظاهر هذا الاقتصاد في الأسواق السوداء الرقمية، التي تُستعمل لتجارة البيانات المسروقة، وأدوات الاختراق، والخدمات الإجرامية مثل الهجمات الموزعة أو الابتزاز الإلكتروني. هذه الأسواق تعمل وفق منطق اقتصادي متكامل يشبه الأسواق التقليدية من حيث العرض والطلب، لكنها تتميز بغياب التنظيم القانوني والرقابي(Wall, 2007,p.157) .

كما تلعب العملات المشفرة دورًا محوريًا في هذا الاقتصاد غير المشروع، حيث توفر وسيلة شبه مجهولة لتحويل الأموال، مما يسهل عمليات الدفع بين الأطراف الإجرامية دون ترك أثر مالي واضح. وقد ساهمت هذه العملات في تعزيز استدامة الاقتصاد الإجرامي الرقمي، وأعطته قدرة أكبر على التوسع والتكيف مع آليات المكافحة التقليدية.

. (Goodman, 2015,p.51)

وبذلك، فإن الجريمة السيبرانية لم تعد مجرد فعل قانوني مخالف، بل أصبحت جزءًا من منظومة اقتصادية رقمية متكاملة، تتداخل فيها التكنولوجيا مع السوق والجريمة، مما يستدعي إعادة النظر في مقاربات المكافحة القانونية والأمنية، وتبني استراتيجيات متعددة الأبعاد تأخذ في الاعتبار هذا التعقيد البنيوي.

مسؤولية أنظمة الذكاء الاصطناعي المستقلة

يُعد ظهور أنظمة الذكاء الاصطناعي المستقلة من أكثر التطورات التقنية تأثيرًا في النظرية الجنائية الحديثة، إذ تجاوزت هذه الأنظمة مرحلة تنفيذ الأوامر البرمجية التقليدية لتصبح قادرة على التعلم الذاتي، وتحليل البيانات، واتخاذ القرارات بصورة مستقلة نسبيًا دون تدخل بشري مباشر. وقد أدى هذا التحول إلى إثارة تساؤلات قانونية غير مسبوقة حول إمكانية إسناد المسؤولية الجنائية إلى الأنظمة الذكية (علي،٢٠٢٢، ص.٤٩)، أو إلى الأشخاص الطبيعيين أو الاعتباريين المرتبطين بها، خاصة عندما تسفر قرارات هذه الأنظمة عن نتائج إجرامية أو أضرار جسيمة.

. (Hilgendorf, 2019, pp. 12–21)

وترتكز النظرية الجنائية التقليدية على افتراض أن الجريمة لا يمكن أن تصدر إلا عن إرادة إنسانية واعية تتمتع بالإدراك والتمييز، وهو ما يجعل عناصر المسؤولية الجنائية، وفي مقدمتها الركن المعنوي، مرتبطة بالشخص الطبيعي (متولي،٢٠٢١). إلا أن التطورات الحديثة في مجال الذكاء الاصطناعي أوجدت أنظمة قادرة على تعديل سلوكها استنادًا إلى الخبرة المكتسبة والبيانات المتاحة، الأمر الذي يضعف إمكانية تفسير جميع الأفعال الناتجة عنها وفق المفاهيم التقليدية للقصد الجنائي والإرادة الحرة.(Russell & Norvig, 2021, pp. 33–41)

وقد انقسم الفقه القانوني إلى ثلاث اتجاهات رئيسة في معالجة هذه الإشكالية. يتمثل الاتجاه الأول في رفض منح الذكاء الاصطناعي أي مركز قانوني مستقل، واعتبار المسؤولية الجنائية مسؤولية بشرية خالصة تقع على عاتق المبرمج أو المصنع أو المستخدم بحسب درجة سيطرته على النظام (متولي،٢٠٢١). أما الاتجاه الثاني، فيدعو إلى تطوير مفهوم "الفاعل الخوارزمي" بوصفه عنصرًا قانونيًا جديدًا يسمح بإعادة توزيع المسؤولية بين الإنسان والنظام الذكي وفقًا لدرجة استقلالية القرار. في حين يقترح الاتجاه الثالث تبني نموذج المسؤولية المشتركة، الذي يوزع المسؤولية بين جميع الأطراف المساهمة في تطوير النظام وتشغيله وإدارته، مع مراعاة مستوى التنبؤ بالمخاطر وإمكانية السيطرة عليها.
(Pagallo, 2013, pp. 145–162)

وتخلص الدراسة إلى أن الاعتراف بالذكاء الاصطناعي بوصفه "فاعلًا قانونيًا" مستقلًا لا يزال يفتقر إلى الأساس التشريعي والفقهي، إلا أن استمرار التطور في الأنظمة الذاتية التشغيل يفرض على المشرعين إعادة النظر في قواعد المسؤولية الجنائية، بما يضمن تحقيق التوازن بين الابتكار التكنولوجي ومتطلبات العدالة الجنائية.

٥. أزمة الإثبات: الدليل الرقمي مقابل المعايير القانونية

تمثل مسألة الإثبات في الجرائم السيبرانية إحدى أكثر الإشكاليات تعقيدًا في القانون الجنائي المعاصر، إذ لم يعد الدليل في صورته التقليدية (المادية والمحسوسة) كافيًا لاستيعاب طبيعة الجريمة الرقمية (عبد الله، ٢٠٢٣، ص.١١٨). فالبيئة السيبرانية تُنتج نوعًا جديدًا من الأدلة يُعرف بالدليل الرقمي، وهو دليل غير ملموس، قابل للتعديل، سريع الزوال، ويعتمد بشكل كبير على البنى التقنية والبرمجية التي أنتجته. هذا التحول أدى إلى نشوء ما يمكن تسميته بـ"أزمة الإثبات الرقمية"، حيث تتصادم خصائص الدليل الرقمي مع المعايير القانونية التقليدية للإثبات الجنائي.
. (Brenner, 2010,p.87; Casey, 2011,p.45)

هشاشة الأدلة الرقمية

تتميز الأدلة الرقمية بطبيعتها الهشة مقارنة بالأدلة المادية التقليدية، إذ يمكن تعديلها أو حذفها أو إعادة إنتاجها دون ترك أثر واضح. فعلى سبيل المثال، يمكن تغيير سجلات الدخول إلى الأنظمة، أو تعديل البيانات المخزنة، أو حتى محاكاة نشاط رقمي يبدو أصليًا بينما هو في الحقيقة مزيف. هذه الخصائص تجعل الدليل الرقمي عرضة للتلاعب، وتضعف من قيمته الإثباتية إذا لم يتم التعامل معه وفق إجراءات تقنية دقيقة(Casey, 2011,p.47) .
كما أن الطبيعة الديناميكية للبيئة الرقمية تعني أن الدليل لا يكون ثابتًا، بل يتغير باستمرار مع تحديث الأنظمة أو إعادة تشغيلها أو حتى مع مرور الوقت. وهذا يتعارض مع أحد أهم مبادئ الإثبات الجنائي، وهو استقرار الدليل وإمكانية التحقق منه بشكل مستقل. لذلك، فإن الاعتماد على الأدلة الرقمية يتطلب أدوات تقنية متقدمة لضمان سلامتها وموثوقيتها، مثل أنظمة التحقق الرقمي والتوقيع الإلكتروني وسجلات التدقيق (Wall, 2007,p.159).

إشكالية السلسلة الزمنية للأدلة

تُعد سلسلة الحيازة أو السلسلة الزمنية للأدلة من المبادئ الأساسية في قانون الإثبات الجنائي، حيث تهدف إلى ضمان عدم التلاعب بالدليل منذ لحظة جمعه وحتى تقديمه أمام المحكمة. غير أن تطبيق هذا المبدأ في البيئة الرقمية يواجه تحديات كبيرة، نظرًا للطبيعة غير الملموسة للأدلة وسهولة نسخها وتعديلها دون اكتشاف ذلك بسهولة.

في السياق السيبراني، قد يتم نقل الدليل الرقمي عبر عدة خوادم أو أجهزة أو حتى دول مختلفة خلال أجزاء من الثانية، مما يجعل تتبع مساره الكامل أمرًا بالغ الصعوبة. كما أن عمليات النسخ الرقمية لا تؤدي إلى فقدان النسخة الأصلية، بل تنتج نسخًا متطابقة، وهو ما يثير إشكالية تحديد "الأصل" من "النسخة"، ويضعف من القدرة على إثبات سلامة الدليل (Kerr, 2003,p.362).

وعليه، فإن ضمان سلامة السلسلة الزمنية للأدلة الرقمية يتطلب تطبيق بروتوكولات تقنية دقيقة، مثل التشفير، والتوثيق الزمني، واستخدام تقنيات البلوك تشين في بعض الحالات لضمان عدم التلاعب بالسجلات(Goodman, 2015,p.54) .

التحديات في قبول الأدلة أمام القضاء

تواجه الأدلة الرقمية تحديات كبيرة في مرحلة قبولها أمام القضاء، إذ تختلف الأنظمة القانونية في مدى اعترافها بهذا النوع من الأدلة وشروط قبولها. ففي بعض الحالات، يشترط القضاء توفر معايير صارمة تتعلق بسلامة جمع الدليل، وموثوقية الوسيلة التقنية المستخدمة، وإمكانية التحقق المستقل من البيانات.

إلا أن هذه المتطلبات تصطدم بواقع تقني معقد، حيث تعتمد الأدلة الرقمية غالبًا على أنظمة تشغيل وبرمجيات قد تكون غير مفهومة بالكامل للقاضي أو حتى لخبراء القانون. هذا ما يخلق فجوة معرفية بين القانون والتكنولوجيا، تؤثر على تقييم المحكمة لقيمة الدليل ومدى حجّيته(Brenner, 2010,p.140) .

كما أن اختلاف التشريعات بين الدول يزيد من تعقيد المشكلة، خاصة في القضايا العابرة للحدود، حيث قد يُقبل الدليل الرقمي في دولة معينة بينما يُرفض في دولة أخرى بسبب اختلاف المعايير الإجرائية أو التقنية. هذا التباين يضعف من فعالية التعاون القضائي الدولي في مكافحة الجريمة السيبرانية(Wall, 2007,p.161) .

وبالتالي، فإن أزمة الإثبات في الجرائم السيبرانية لا تتعلق فقط بغياب الأدلة، بل بقدرة النظام القانوني على فهمها وتقييمها وفق معايير عادلة وموحدة. وهذا يستدعي تطوير أطر قانونية وتقنية مشتركة تضمن موثوقية الأدلة الرقمية وتقلل من الفجوة بين القانون والتكنولوجيا.

٧. الفجوة بين القانون والتكنولوجيا: الأبعاد البنيوية والمعرفية

تمثل العلاقة بين القانون والتكنولوجيا إحدى أكثر العلاقات إشكالية في العصر الرقمي، إذ لم يعد القانون يعمل في بيئة مستقرة نسبيًا، بل في فضاء تقني متغير بسرعة فائقة تتجاوز قدرة الأنظمة التشريعية التقليدية على الاستجابة. وقد أدى هذا التباين إلى ظهور ما يُعرف بـ"الفجوة بين القانون والتكنولوجيا"، وهي فجوة متعددة الأبعاد لا تقتصر على الجانب التشريعي فقط، بل تمتد لتشمل البنية المعرفية للمشرّع وآليات التطبيق القضائي. ويؤكد الفقه الحديث أن هذه الفجوة أصبحت أحد الأسباب الجوهرية لضعف فعالية القانون في مواجهة الجرائم السيبرانية (Brenner, 2010,p.142; Wall, 2007,p.163).

الفجوة البنيوية: بطء التشريع مقابل سرعة التقنية

تتمثل الفجوة البنيوية في التفاوت الزمني بين سرعة التطور التقني وبطء العملية التشريعية. فبينما تتطور التقنيات الرقمية، مثل الذكاء الاصطناعي والحوسبة السحابية والهجمات السيبرانية، بوتيرة متسارعة قد تتغير خلالها طبيعة التهديدات خلال أشهر أو حتى أسابيع، فإن العملية التشريعية غالبًا ما تتطلب سنوات من النقاش والإقرار والتعديل.

هذا البطء يجعل القوانين في كثير من الأحيان متأخرة عن الواقع التقني، أي أنها تأتي لمعالجة مشكلات أصبحت بالفعل متجاوزة أو تم تطوير وسائل جديدة للتحايل عليها. ونتيجة لذلك، يظهر ما يمكن تسميته بـ"قانون متأخر زمنيًا"، أي قانون لا يعكس الحالة الفعلية للتقنيات المستخدمة في ارتكاب الجرائم (Kerr, 2003,p.363).

كما أن الطبيعة العالمية للتكنولوجيا تزيد من حدة هذه الفجوة، إذ قد تتطور تقنيات جديدة في بيئات لا تخضع لنفس الأطر التنظيمية، مما يجعل التشريعات الوطنية غير قادرة على مواكبة التحولات العالمية في الفضاء السيبراني. وهذا يخلق حالة من عدم التوازن بين مرونة التكنولوجيا وجمود القانون النسبي(Yar, 2013,p.20) .

الفجوة المعرفية: نقص الفهم التقني لدى المشرّع

تتعلق الفجوة المعرفية بمدى إدراك المشرّع أو صانع السياسة القانونية لطبيعة التقنيات التي يسعى إلى تنظيمها. فالقانون التقليدي يعتمد على صياغات معيارية عامة، بينما تتطلب الجريمة السيبرانية فهمًا تقنيًا دقيقًا لبنية الأنظمة الرقمية وآليات عملها.

في العديد من الحالات، يفتقر المشرّعون إلى المعرفة التقنية الكافية لفهم كيفية عمل الخوارزميات، أو آليات التشفير، أو أنظمة الذكاء الاصطناعي (حسني،٢٠٢١)، مما يؤدي إلى صياغة قوانين قد تكون إما فضفاضة جدًا أو تقنية بشكل مفرط دون فهم دقيق لآثارها العملية. هذا النقص المعرفي يخلق فجوة بين النص القانوني والواقع التقني، ويؤدي إلى ضعف في فعالية التشريع(Brenner, 2010,p.153) .

وقد أشار بعض الباحثين إلى أن معالجة هذه الفجوة تتطلب دمج الخبرات التقنية داخل العملية التشريعية، من خلال إشراك خبراء التكنولوجيا في صياغة القوانين، أو إنشاء هيئات استشارية تقنية دائمة تدعم المشرّع في فهم التطورات الرقمية (Goodman, 2015,p.61).

الفجوة التطبيقية: صعوبات التنفيذ القضائي

تتمثل الفجوة التطبيقية في التحديات التي تواجه السلطات القضائية عند محاولة تطبيق القوانين القائمة على الوقائع الرقمية. فحتى في حال وجود نصوص قانونية مناسبة نسبيًا، فإن تنفيذها يواجه عقبات عملية تتعلق بجمع الأدلة، وتحديد الاختصاص، وفهم طبيعة الفعل الإجرامي.

من أبرز هذه التحديات الاعتماد المتزايد على الأدلة الرقمية، التي تتطلب خبرات تقنية متقدمة لفحصها وتفسيرها. وغالبًا ما يفتقر القضاة وأعضاء النيابة إلى الخلفية التقنية الكافية لفهم التفاصيل المعقدة المرتبطة بالجرائم السيبرانية، مما يجعلهم يعتمدون بشكل كبير على الخبراء الفنيين، وهو ما قد يثير إشكاليات تتعلق بحجية الخبرة وحدودها.

. (Casey, 2011,p.49)

كما أن الطابع العابر للحدود للجريمة السيبرانية يؤدي إلى صعوبات في تنفيذ الأحكام القضائية، خاصة عندما تكون الأدلة أو الجناة أو البيانات موزعة عبر عدة دول (هادي، ٢٠٢٣) هذا الوضع يتطلب تعاونًا دوليًا معقدًا قد لا يكون دائمًا فعالًا بسبب اختلاف الأنظمة القانونية والإجرائية(Wall, 2007p.163) .

وبالتالي، فإن الفجوة التطبيقية تعكس عدم قدرة النظام القضائي التقليدي على التكيف الكامل مع طبيعة الجريمة الرقمية، مما يستدعي تطوير أدوات قضائية وتقنية جديدة، مثل المحاكم المتخصصة في الجرائم السيبرانية، وتعزيز التدريب التقني للقضاة وأجهزة إنفاذ القانون.

٧. نحو نموذج قانوني–تقني جديد

لم يعد من الممكن التعامل مع الجريمة السيبرانية ضمن الإطار التقليدي للقانون الجنائي الذي تشكّل في بيئة مادية مستقرة، بل أصبح من الضروري الانتقال نحو نموذج قانوني–تقني جديد يعيد صياغة العلاقة بين القانون والتكنولوجيا بوصفها علاقة تكامل لا علاقة تبعية. هذا النموذج يقوم على فكرة أساسية مفادها أن الفضاء الرقمي ليس مجرد "مجال لتطبيق القانون"، بل هو بيئة تنتج قواعدها الخاصة وتعيد تشكيل مفاهيم المسؤولية والفاعل والدليل (متولي،٢٠٢١). ومن ثمّ، فإن تطوير استجابة قانونية فعّالة للجريمة السيبرانية يتطلب إعادة بناء المفاهيم القانونية، ودمج الأدوات التكنولوجية في العمل القانوني، وتطوير حوكمة رقمية عالمية أكثر شمولًا ومرونة(Brenner, 2010,p.158; Wall, 2007,p.177) .

إعادة بناء المفاهيم القانونية

إن أولى خطوات التحول نحو نموذج قانوني–تقني جديد تتمثل في إعادة بناء المفاهيم الأساسية التي يقوم عليها القانون الجنائي، وعلى رأسها مفهوم المسؤولية الجنائية. فالمسؤولية في التصور التقليدي ترتبط بفاعل بشري يتمتع بالإرادة والوعي، إلا أن تطور الأنظمة الذكية والخوارزميات التكيفية فرض إعادة النظر في هذا الافتراض(علي،٢٠٢٢، ص.٥١) ففي البيئة الرقمية المعاصرة، لم يعد الفعل الإجرامي دائمًا نتيجة مباشرة لإرادة بشرية فردية، بل قد يكون نتاج تفاعل معقد بين الإنسان والنظام الخوارزمي. لذلك، أصبح من الضروري توسيع مفهوم المسؤولية ليشمل أشكالًا متعددة من الإسناد القانوني، قد تتوزع بين المطور، والمستخدم، والمشغل، وأحيانًا النظام نفسه من حيث تأثيره الفعلي في إنتاج السلوك الإجرامي (Goodman, 2015,p.185) .

وفي هذا السياق، يبرز مفهوم "الفاعل الخوارزمي" بوصفه أحد أكثر التحولات إشكالية في الفكر القانوني الحديث. فمع تطور أنظمة الذكاء الاصطناعي القادرة على التعلم واتخاذ القرار(حسني،٢٠٢١)، لم يعد بالإمكان تجاهل دور هذه الأنظمة في تشكيل الفعل الإجرامي. وقد طرح بعض الباحثين فكرة أن الخوارزمية قد تُعامل بوصفها "فاعلًا وظيفيًا" في نطاق محدد من المسؤولية، ليس بمعنى الاعتراف بشخصيتها القانونية، بل باعتبارها عنصرًا منتجًا للسلوك يجب أخذه في الاعتبار عند تحديد المسؤولية الجنائية(Hilgendorf, 2019,p.933) .

دمج القانون بالتكنولوجيا

يمثل دمج القانون بالتكنولوجيا أحد أهم التحولات البنيوية في النظام القانوني المعاصر، حيث لم يعد القانون يعمل بمعزل عن الأدوات التقنية، بل أصبح يعتمد عليها بشكل متزايد في مجالات متعددة، بدءًا من تحليل البيانات القانونية وصولًا إلى التحقيق في الجرائم المعقدة.

يُعرف هذا المجال، إلى استخدام التكنولوجيا، وخاصة الذكاء الاصطناعي وتحليل البيانات الضخمة، في دعم العمليات القانونية. ففي سياق الجرائم السيبرانية (تيسير،٢٠٢٠)، يمكن استخدام هذه التقنيات لتحليل أنماط الهجمات، وتتبع الأنشطة المشبوهة، وربط الأدلة الرقمية ببعضها البعض بشكل أسرع وأكثر دقة من الطرق التقليدية (Casey, 2011,p.51).

كما أصبح الذكاء الاصطناعي أداة مهمة في التحقيقات الجنائية، حيث يُستخدم في تحليل كميات ضخمة من البيانات الرقمية، واكتشاف الأنماط غير الطبيعية، والتنبؤ بالهجمات السيبرانية قبل وقوعها(هادي، ٢٠٢٣) إلا أن هذا التطور يطرح في الوقت ذاته إشكاليات قانونية تتعلق بالشفافية، وحجية النتائج، ومدى إمكانية الاعتماد على القرارات الآلية في الإجراءات القضائية(Goodman, 2015,p.188) .

ومن ثمّ، فإن دمج القانون بالتكنولوجيا لا يعني استبدال الإنسان بالآلة، بل يعني إعادة تشكيل العلاقة بينهما بحيث تصبح التكنولوجيا أداة داعمة للقرار القانوني، وليس بديلاً عنه.

الحوكمة الرقمية العالمية

تُعد الجريمة السيبرانية بطبيعتها جريمة عابرة للحدود، وهو ما يجعل مواجهتها خارج نطاق قدرة الدولة الواحدة. لذلك، أصبح من الضروري الانتقال نحو نموذج حوكمة رقمية عالمية يقوم على التعاون الدولي وتوحيد المعايير القانونية والتقنية.

إن غياب إطار دولي موحد يؤدي إلى تباين كبير في كيفية تعريف الجريمة السيبرانية ومعالجتها بين الدول، مما يخلق بيئة خصبة للإفلات من العقاب واستغلال الثغرات القانونية (ثامر،٢٠٢٢،ص.١٦). لذلك، تبرز الحاجة إلى تطوير نظام حوكمة رقمية عالمي يحدد المبادئ الأساسية للسلوك في الفضاء السيبراني، ويعزز آليات التعاون القضائي والأمني بين الدول(Wall, 2007,p.177) .

وقد لعبت (United Nations) دورًا متزايدًا في هذا المجال من خلال مبادراتها المتعلقة بالأمن السيبراني، إلا أن غياب إلزامية هذه المبادرات يحد من فعاليتها. كما أن بعض الاتفاقيات الدولية، مثل اتفاقية (Budapest Convention on Cybercrime)، تمثل خطوة مهمة نحو توحيد الجهود، لكنها لا تزال محدودة من حيث الانتشار العالمي والقبول الدولي (Yar, 2013,p.45).

وبالتالي، فإن الحوكمة الرقمية العالمية لا تعني فقط وضع قواعد قانونية مشتركة، بل تتطلب أيضًا بناء منظومة تعاون تقني وقضائي مستدامة، تأخذ في الاعتبار الطبيعة الديناميكية للفضاء السيبراني، وتوازن بين حماية الأمن الرقمي وصون الحقوق والحريات.

٨. النموذج التحليلي المقارن

يُعدّ التحليل المقارن أحد أهم المناهج في دراسة الجريمة السيبرانية، لأنه يكشف عن التباينات البنيوية بين النظم القانونية المختلفة في فهمها للجريمة الرقمية وآليات مكافحتها. فالجريمة السيبرانية بطبيعتها العابرة للحدود لا يمكن فهمها ضمن إطار وطني ضيق، بل تتطلب مقاربة مقارنة تُبرز الفروق بين النماذج التشريعية الكبرى: النموذج الأوروبي، والنموذج الأنجلوسكسوني، والنموذج العربي. ويهدف هذا التحليل إلى تقييم مدى الفعالية والتحديات التي يواجهها كل نموذج في التعامل مع التحولات الرقمية المتسارعة (Wall, 2007,p.179; Brenner, 2010,p.161).

النموذج الأوروبي

يمتاز النموذج الأوروبي بنزعة تنظيمية موحدة نسبيًا تعتمد على التعاون الإقليمي والتنسيق التشريعي بين الدول، وقد تجسّد ذلك بشكل واضح في اتفاقية (Budapest Convention on Cybercrime) التي تُعد الإطار الدولي الأبرز في مجال مكافحة الجرائم السيبرانية(عبد الله، ٢٠٢٣،ص.١٢١). هذا النموذج يركز على توحيد تعريفات الجرائم، وتنسيق إجراءات التحقيق، وتعزيز تبادل الأدلة بين الدول الأعضاء.

كما تلعب مؤسسات مثل المجلس الأوربي دورًا محوريًا في تطوير المعايير القانونية المتعلقة بالأمن السيبراني، مما يمنح هذا النموذج درجة عالية من الاتساق التشريعي. غير أن من أبرز تحدياته محدودية الانتشار العالمي، إذ لا تزال العديد من الدول خارج نطاق الالتزام الكامل بهذه الاتفاقيات، مما يضعف من فاعليتها في معالجة الجرائم العابرة للحدود على نطاق عالمي(Yar, 2013,p.45) .

النموذج الأنجلوسكسوني

يعتمد النموذج الأنجلوسكسوني، خاصة في الولايات المتحدة والمملكة المتحدة، على نهج مرن يقوم على التوسع في التفسير القضائي للقوانين القائمة بدلًا من الاعتماد الكلي على تشريعات متخصصة. هذا النموذج يتميز بقدرة عالية على التكيف مع التطورات التقنية، حيث تلعب المحاكم دورًا مهمًا في تطوير القواعد القانونية من خلال السوابق القضائية.

غير أن هذا النهج يواجه تحديًا يتمثل في التشتت التشريعي وعدم وجود إطار موحد شامل للجريمة السيبرانية، مما قد يؤدي إلى تباين في التطبيق القضائي وصعوبة في تحقيق الاتساق القانوني (هادي، ٢٠٢٣). كما أن التركيز على الحلول القضائية أكثر من التشريعية قد يؤدي إلى تأخر في الاستجابة لبعض التهديدات السيبرانية المستجدة.

. (Kerr, 2003,p.365)

النموذج العربي

أما النموذج العربي، فيتسم بالتنوع وعدم التجانس، حيث تختلف التشريعات من دولة إلى أخرى بشكل كبير من حيث التعريفات والعقوبات وآليات التنفيذ (مجيد،٢٠٢٤). بعض الدول العربية أصدرت قوانين متقدمة نسبيًا في مجال مكافحة الجرائم المعلوماتية، بينما لا تزال دول أخرى تعتمد على تشريعات تقليدية لا تستوعب التعقيدات التقنية الحديثة.

ويعاني هذا النموذج من عدة تحديات، أبرزها ضعف التنسيق الإقليمي، وغياب إطار قانوني عربي موحد للجريمة السيبرانية، بالإضافة إلى محدودية البنية التحتية التقنية في بعض الدول، مما يؤثر على فعالية تطبيق القوانين. كما أن نقص الخبرات المتخصصة في القانون الرقمي يزيد من صعوبة التعامل مع القضايا السيبرانية المعقدة.

. (Brenner, 2010,p.172)

تحليل الفعالية والتحديات المقارنة

عند مقارنة النماذج الثلاثة، يمكن ملاحظة أن النموذج الأوروبي يتميز بالاتساق التنظيمي لكنه محدود جغرافيًا، بينما يتميز النموذج الأنجلوسكسوني بالمرونة القضائية لكنه يعاني من التشتت، في حين أن النموذج العربي يواجه تحديات هيكلية تتعلق بالتشريع والتنفيذ والبنية التحتية.

ومن منظور الفعالية، يمكن القول إن أي نموذج منفرد غير كافٍ لمواجهة الطبيعة المعقدة للجريمة السيبرانية، التي تتطلب تكاملًا بين المرونة القانونية، والتنسيق الدولي، والتطور التقني. كما أن الطبيعة العابر للحدود للجريمة السيبرانية تجعل من الضروري تعزيز التعاون بين هذه النماذج بدلًا من عزلها، من خلال بناء إطار عالمي أكثر شمولًا وتوازنًا.

. (Wall, 2007,p.179; Goodman, 2015,p.221)

٩. النتائج

تكشف الدراسة التحليلية للجريمة السيبرانية في أبعادها المفاهيمية والتقنية والقانونية عن مجموعة من النتائج الجوهرية التي تتجاوز الوصف السطحي للظاهرة، لتصل إلى مستوى إعادة تفسير البنية العميقة للعلاقة بين القانون

والتكنولوجيا. ويمكن القول إن الجريمة السيبرانية لم تعد مجرد "نمط جديد من الجرائم"، بل أصبحت مؤشرًا على تحول بنيوي في النظام القانوني ذاته، حيث لم يعد القانون هو الإطار الوحيد المنظم للسلوك، بل أصبح يتقاسم هذا الدور مع البنية الخوارزمية التي تنتج الفعل وتوجهه وتعيد تشكيله (Lessig, 2006,p.6; Wall, 2007,p.180).

أولًا: أظهرت الدراسة أن هناك انفصالًا متزايدًا بين المفاهيم القانونية التقليدية وطبيعة الفعل السيبراني .فالمفاهيم الأساسية في القانون الجنائي مثل الفعل، والنية، والفاعل، لم تعد قادرة على استيعاب الأفعال التي تُنتج داخل بيئات رقمية تعتمد على الأتمتة والذكاء الاصطناعي (حسني،٢٠٢١). هذا الانفصال لا يعني مجرد قصور تطبيقي، بل يعكس أزمة مفاهيمية أعمق تتعلق بقدرة النظرية الجنائية التقليدية على تفسير الواقع الرقمي المعاصر(Brenner, 2010,p.183) .

ثانيًا: تبين أن البنية التقنية أصبحت عنصرًا منتجًا للسلوك الإجرامي وليس مجرد وسيط له . فالخوارزميات وأنظمة الذكاء الاصطناعي لا تنقل الفعل الإجرامي فقط ، بل تسهم في تشكيله وإعادة صياغته، بل وقد تنتجه بشكل مستقل نسبيًا عن الإرادة البشرية المباشرة (عايد،٢٠٢١، ص.٢١٣). وهذا ما يؤدي إلى إعادة توزيع المسؤولية القانونية بين الإنسان والنظام التقني، مما يضعف من مركزية الفاعل البشري في التحليل الجنائي التقليدي(Goodman, 2015,p.233)).

ثالثًا: أظهرت النتائج وجود فجوة جوهرية بين سرعة التطور التقني وبطء الاستجابة القانونية .فبينما تتطور تقنيات الهجوم والدفاع السيبراني بوتيرة متسارعة، تبقى النصوص القانونية محكومة بإجراءات تشريعية بطيئة، مما يؤدي إلى حالة من "التأخر التشريعي المزمن". هذا التأخر لا يؤثر فقط على فعالية الردع، بل يخلق أيضًا مساحات قانونية رمادية يستغلها الفاعلون الإجراميون(Kerr, 2003,p.369) .

رابعًا: كشفت الدراسة أن الدليل الرقمي يعاني من هشاشة بنيوية تؤثر على استقراره وحجيته القانونية .فإمكانية التعديل أو النسخ أو الإخفاء دون أثر واضح تجعل من الصعب تحقيق اليقين القضائي الكامل، مما يؤدي إلى إعادة تعريف مفهوم الإثبات الجنائي في البيئة الرقمية، والانتقال من اليقين المطلق إلى اليقين الاحتمالي المدعوم تقنيًا (Casey, 2011,p.135).

خامسًا: توصلت الدراسة إلى أن الطبيعة العابرة للحدود للجريمة السيبرانية تُضعف فعالية السيادة القانونية التقليدية، حيث لم تعد الدولة قادرة على ممارسة سلطتها القضائية بشكل منفرد داخل الفضاء الرقمي (هادي، ٢٠٢٣). هذا الواقع يعزز الحاجة إلى نماذج حوكمة دولية أكثر مرونة وتكاملًا، قادرة على تجاوز حدود الاختصاص الوطني.

. (Wall, 2007,p.180)

وأخيرًا، فإن النتيجة الأهم التي توصلت إليها الدراسة تتمثل في أن الفجوة بين القانون والتقنية ليست فجوة ظرفية، بل فجوة بنيوية معرفية .فهي لا تتعلق فقط ببطء التشريع أو ضعف التطبيق، بل بوجود اختلاف جذري في منطق كل من النظامين: فالقانون يعمل بمنطق معياري ثابت نسبيًا، بينما تعمل التكنولوجيا بمنطق ديناميكي متغير باستمرار. هذا الاختلاف الجذري هو ما يجعل عملية التوفيق بينهما تحديًا مستمرًا وليس حالة يمكن حلها بشكل نهائي.

. (Yar, 2013,p.183)

وبناءً على ذلك، يمكن القول إن الجريمة السيبرانية تمثل نقطة التقاء حرجة بين نظامين معرفيين مختلفين، وأن مستقبل القانون الجنائي سيتحدد بقدرته على التكيف مع هذا التداخل البنيوي بين القانون والتكنولوجيا.

١٠. المناقشة

يشهد العالم المعاصر تحولًا جذريًا في طبيعة الجريمة بفعل التقدم المتسارع في تقنيات الذكاء الاصطناعي، الأمر الذي لم يعد يقتصر على تغيير أدوات ارتكاب الجريمة، بل امتد ليعيد تشكيل بنيتها المفاهيمية ذاتها. فالجريمة لم تعد فعلًا بشريًا بسيطًا يمكن ضبطه ضمن إطار قانوني تقليدي، بل أصبحت ظاهرة ديناميكية تتداخل فيها الخوارزميات، والبيانات الضخمة، والأنظمة الذاتية التعلم، مما يثير تساؤلات عميقة حول مستقبل المفهوم الجنائي وحدود صلاحيته في العصر الرقمي (Goodman, 2015,p.239; Wall, 2007,p.187) .

هل نحن أمام جيل جديد من الجرائم؟

إن تطور الذكاء الاصطناعي، وخاصة الأنظمة القادرة على التعلم الذاتي واتخاذ القرار المستقل، أدى إلى ظهور أنماط جديدة من السلوك الإجرامي لا يمكن تصنيفها بسهولة ضمن الأطر التقليدية للجريمة. فاليوم لم يعد الفعل الإجرامي مقتصرًا على الإنسان، بل أصبح من الممكن أن تنشأ أفعال ضارة نتيجة تفاعل خوارزميات معقدة دون تدخل بشري مباشر في كل مرحلة من مراحل التنفيذ.

هذا الواقع دفع العديد من الباحثين إلى القول إننا أمام "جيل جديد من الجرائم"، يتميز بخصائص مختلفة جذريًا عن الجرائم التقليدية، أبرزها: غياب الفاعل البشري المباشر، وتعدد مستويات المسؤولية، وصعوبة التنبؤ بالسلوك الإجرامي أو التحكم فيه. ففي هذا السياق، قد يقوم النظام الذكي بتنفيذ سلوك ضار نتيجة تدريب خاطئ أو بيانات منحازة أو تفاعل غير متوقع مع بيئة رقمية معقدة، مما يخلق نوعًا من الإجرام غير المقصود أو الإجرام الخوارزمي (Brenner, 2010,p.188) .

كما أن الجريمة في هذا الإطار لم تعد حدثًا منفصلًا، بل أصبحت عملية مستمرة تتطور مع تطور النظام نفسه، وهو ما يعزز فكرة أن الجريمة السيبرانية لم تعد ظاهرة ثابتة، بل حالة ديناميكية تتغير باستمرار وفق تطور التكنولوجيا.

هل يجب إعادة تعريف الجريمة بالكامل؟

إن التساؤل حول ضرورة إعادة تعريف الجريمة لا يتعلق فقط بتحديث النصوص القانونية، بل يمس جوهر النظرية الجنائية ذاتها. فالتعريف التقليدي للجريمة باعتبارها فعلًا غير مشروع صادر عن إرادة إجرامية يترتب عليه ضرر لم يعد كافيًا لاستيعاب الواقع الجديد الذي تفرضه الأنظمة الذكية.

في ظل الذكاء الاصطناعي، أصبح من الضروري إعادة النظر في عناصر الجريمة الأساسية:

١. الفاعل :لم يعد بالضرورة إنسانًا، بل قد يكون نظامًا خوارزميًا أو مزيجًا بين الإنسان والآلة .
٢. النية الجنائية :لم تعد واضحة أو قابلة للإثبات دائمًا، خاصة في حالات التعلم الآلي التي تنتج نتائج غير متوقعة .
٣. الضرر :أصبح أكثر تعقيدًا، إذ قد يكون غير مباشر أو مؤجل أو موزعًا عبر شبكات رقمية واسعة .

وقد أشار (Lawrence Lessig) إلى أن "الكود هو القانون"، بمعنى أن البنية البرمجية أصبحت تحدد السلوك الممكن والممنوع داخل الفضاء الرقمي، وهو ما يعني أن الجريمة لم تعد فقط انتهاكًا للقانون، بل قد تكون نتيجة تصميم تقني بحد ذاته (Lessig, 2006,p.8) .

كما أن تطور الأنظمة الذكية يفرض إعادة التفكير في مفهوم المسؤولية القانونية، حيث لم يعد من الممكن حصرها في فرد واحد، بل قد تمتد إلى المطورين، والمستخدمين، ومصممي الخوارزميات، وحتى المؤسسات التي تدير هذه الأنظمة. وهذا

ما يجعل القانون الجنائي التقليدي بحاجة إلى تحول جذري نحو نموذج أكثر مرونة وتعددية في الإسناد القانوني (Hilgendorf, 2019,p.941).

من جهة أخرى، فإن استمرار الاعتماد على التعريفات التقليدية للجريمة قد يؤدي إلى فجوة متزايدة بين الواقع التقني والنص القانوني، مما يضعف من قدرة القانون على تحقيق الردع والعدالة. لذلك، فإن إعادة تعريف الجريمة في عصر الذكاء الاصطناعي لا تُعد خيارًا نظريًا فحسب، بل ضرورة عملية لضمان فعالية النظام القانوني في مواجهة التهديدات المستقبلية (Yar, 2013,p.185).

١١. التوصيات

في ضوء التحليل النظري والمقارن الذي تناولته الدراسة، يتضح أن مواجهة الجريمة السيبرانية لا يمكن أن تتحقق من خلال الأدوات التقليدية وحدها، بل تتطلب إعادة بناء شاملة لمنظومة التشريع والتطبيق والتعاون المؤسسي. فطبيعة الجريمة السيبرانية بوصفها ظاهرة ديناميكية عابرة للحدود وتتحرك ضمن بيئة خوارزمية متغيرة، تفرض تبني مقاربات مرنة وتكاملية تجمع بين القانون والتكنولوجيا والمعرفة المتخصصة (Brenner, 2010,p.189; Wall, 2007,p.189).

تطوير تشريعات مرنة وقابلة للتكيف

توصي الدراسة بضرورة الانتقال من النموذج التشريعي التقليدي القائم على الثبات النسبي للنصوص القانونية إلى نموذج تشريعي مرن قادر على مواكبة التطور السريع للتكنولوجيا. فالقوانين الحالية غالبًا ما تعاني من "تأخر تشريعي" يجعلها غير قادرة على استيعاب الجرائم المستحدثة في الوقت المناسب. ويقتضي ذلك اعتماد صياغات قانونية مرنة تعتمد على المبادئ العامة بدلًا من التفصيلات التقنية الضيقة، بما يسمح بتفسير النصوص القانونية بشكل يتكيف مع التطورات المستقبلية. كما يُوصى بتضمين آليات مراجعة دورية للتشريعات المتعلقة بالجرائم السيبرانية، لضمان تحديثها المستمر بما يتناسب مع التطور التقني(Kerr, 2003,p.371) . إضافة إلى ذلك، يجب تعزيز التعاون الدولي في صياغة التشريعات، بما يضمن تقاربًا أكبر بين الأنظمة القانونية المختلفة، خاصة في ظل الطبيعة العابرة للحدود للجريمة السيبرانية، وهو ما يتطلب تطوير أطر دولية أكثر شمولًا وفعالية.

بناء شراكات بين القانونيين والتقنيين

تؤكد الدراسة على أن أحد أبرز أسباب الفجوة بين القانون والتكنولوجيا يتمثل في ضعف التكامل بين الخبرة القانونية والمعرفة التقنية. لذلك، توصي بضرورة بناء شراكات مؤسسية مستدامة بين القانونيين وخبراء التكنولوجيا، سواء على مستوى التشريع أو التحقيق أو القضاء. فصياغة قوانين فعالة لمكافحة الجريمة السيبرانية تتطلب فهمًا دقيقًا لبنية الأنظمة الرقمية والخوارزميات وآليات الهجوم والدفاع السيبراني. كما أن تفسير الأدلة الرقمية أمام القضاء يتطلب تعاونًا وثيقًا بين القاضي والخبير التقني، لضمان فهم دقيق للوقائع التقنية المعقدة(Casey, 2011,p.141) . وفي هذا السياق، يمكن إنشاء لجان مشتركة دائمة تضم قانونيين ومهندسين وخبراء أمن سيبراني، تكون مهمتها تقديم استشارات تقنية للمشرّع، والمساهمة في تطوير السياسات العامة المتعلقة بالأمن الرقمي.

إنشاء وحدات تحقيق رقمية متخصصة

توصي الدراسة بضرورة إنشاء وحدات تحقيق رقمية متخصصة داخل أجهزة إنفاذ القانون، تكون مزودة بالخبرات التقنية والأدوات التحليلية اللازمة للتعامل مع الجرائم السيبرانية المعقدة (عبد الله، ٢٠٢٣،ص.١٢٤) فالتعامل مع هذا النوع

من الجرائم لم يعد ممكنًا باستخدام الأساليب التقليدية للتحقيق الجنائي، بل يتطلب قدرات متقدمة في تحليل البيانات الرقمية، وتتبع الأنشطة الإلكترونية، وفحص الأدلة التقنية. وتتمثل أهمية هذه الوحدات في قدرتها على سد الفجوة التطبيقية بين النص القانوني والواقع الرقمي، من خلال تحسين جودة جمع الأدلة الرقمية وضمان سلامتها، بالإضافة إلى تعزيز سرعة الاستجابة للجرائم السيبرانية. كما يمكن لهذه الوحدات أن تلعب دورًا محوريًا في التعاون الدولي، نظرًا للطبيعة العابرة للحدود لهذه الجرائم(Goodman, 2015,p.240) . ومن المهم أن تكون هذه الوحدات مرتبطة بشبكات تعاون دولية، بما يتيح تبادل المعلومات والخبرات، ويعزز من فعالية مكافحة الجريمة السيبرانية على المستوى العالمي.

بشكل عام، تؤكد الدراسة أن مواجهة الجريمة السيبرانية تتطلب تحولًا جذريًا في الفكر القانوني والمؤسسي، يقوم على ثلاثة محاور رئيسية: تشريعات مرنة، تكامل معرفي بين القانون والتكنولوجيا، وبنية تحقيقية متخصصة. وبدون هذا التحول، سيظل القانون متأخرًا عن الواقع التقني، مما يضعف من قدرته على تحقيق العدالة والردع في العصر الرقمي.

المصادر

أبو العطا، عزة تيسير .(2020) .المسؤولية المدنية الناشئة عن استخدام تقنيات الذكاء الاصطناعي: دراسة تحليلية مقارنة .دار النهضة العربية.

البشر، محمد بن عبد الله .(2023) .الجرائم السيبرانية الموجهة ضد الأنظمة الذكية: التحديات التقنية والتشريعية .المجلة العربية للدراسات الأمنية، ٣٩(2)، ١١٥–١٣٨.

الجندي، أحمد حسني .(2021) .جرائم الذكاء الاصطناعي والروبوتات: دراسة في القانون الجنائي المقارن .دار الفكر الجامعي.

الحمامي، فهد نايف .(2022) .التنظيم القانوني للأمن السيبراني: آليات حماية البنية التحتية المعلوماتية الحيوية .مكتبة القانون والاقتصاد.

الخلايلة، محمد علي .(2022) .المسؤولية الجنائية عن جرائم أنظمة الذكاء الاصطناعي والتزييف العميق .مجلة الحقوق والعلوم السياسية، ١٤(1)، ٤٥–٧٨.

السامرائي، عمر مجيد .(2024) .الحماية الجنائية للفضاء السيبراني في ظل التشريعات العربية الحديثة .دار المناهج للنشر والتوزيع.

الشمري، خالد بن عايد .(2021) .التحديات القانونية المترتبة على استخدام خوارزميات الذكاء الاصطناعي في الاستدلال الجنائي .مجلة العلوم الأمنية والتحقيق الجنائي، ٣(2)، ٢٠١–٢٣٥.

العبيدي، علي هادي .(2023) .التطبيقات القانونية للذكاء الاصطناعي والويب الدلالي: صياغة العقود والأحكام القضائية .دار الثقافة للنشر والتوزيع.

العنزي، مشعل ثامر .(2022) .أطر الحوكمة القانونية للأمن السيبراني في الاستراتيجيات الوطنية العربية .المجلة الدولية للقانون والتكنولوجيا، ٥(1)، ١٢–٤٠.

القاضي، رامي متولي .(2021) .المسؤولية الجنائية عن أخطاء المركبات ذاتية القيادة والأنظمة المستقلة .دار النهضة العربية.

المحيميد، عبد العزيز بن محمد .(2023) .نظام مكافحة الجرائم المعلوماتية ومدى استيعابه للمخاطر السيبرانية الناشئة عن الذكاء الاصطناعي التوليدي .مجلة الشريعة والقانون، ٣٧(4)، ٣١٠–٣٥٥.

سيد، محمود محمد .(2023) .المسؤولية المدنية والجنائية لمبرمجي ومصنعي أنظمة الذكاء الاصطناعي في الفضاء الرقمي .مجلة البحوث القانونية والاقتصادية، ١٣(2)، ٨٥–١٢٤.

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

Breuker, J., Boer, A., Hoekstra, R., & Winkels, R. (2009). Legal ontologies in knowledge engineering and information processing. In J. Breuker, P. Casanovas, M. A. Klein, & C. Francesconi (Eds.), Law, ontologies and the semantic web: Channelling the legal information flood (Vol. 188, pp. 5–34). IOS Press.

Breuker, J., Valente, A., & Winkels, R. (2005). Use and reuse of legal ontologies in knowledge engineering and information management. In R. Benjamins, P. Casanovas, J. Breuker, & A. Gangemi (Eds.), Law and the semantic web: Legal ontologies, methodologies, legal information retrieval, and applications (pp. 36–64). Springer.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Council of Europe. (2001). Convention on cybercrime (European Treaty Series - No. 185). Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Doubleday.

Hilgendorf, E. (2019). Robot law. In E. Hilgendorf, J. Joerden, & T. Petrillo (Eds.), Robot law (pp. 1–22). Edward Elgar Publishing.

Kerr, O. S. (2003). The problem of perspective in internet law. Georgetown Law Journal, 91(2), 357–379.

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

Moor, J. H. (1985). What is computer ethics? Metaphilosophy, 16(4), 266–275.

Pagallo, U. (2013). The laws of robots: Crimes, contracts, and torts. Springer.

Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.

Susskind, R. (2019). Online courts and the future of justice. Oxford University Press.

United Nations. (2021). Developments in the field of information and telecommunications in the context of international security (A/75/816). United Nations General Assembly Reports.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Yar, M. (2013). Cybercrime and society (2nd ed.). SAGE Publications.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. Regulation & Governance, 12(4), 505–523.