Mesopotamian journal of Quran studies
Vol.2025, **pp**. 8–18
DOI: https://doi.org/10.58496/MJQS/2026/002; ISSN: 3005–9933
https://mesopotamian.press/journals/index.php/MJQS

الجرائم الإلكترونية وأحكامها في الفقه الإسلامي دراسة مقارنة

Cybercrimes and Their Rulings in Islamic Jurisprudence: A Comparative Study

يسرى محمد امين [١، *]
[١] الكلية التربوية المفتوحة فرع ابي غريب الدراسي, بغداد, العراق.

Yusra Mohammed Amin [1,*]
[1] *Open Educational College, Abu Ghraib Branch, Baghdad, Iraq.*

الخلاصة

يهدف هذا البحث إلى بيان التكييف الفقهي للجرائم الإلكترونية وأحكامها في ضوء مقاصد الشريعة الإسلامية، مع إجراء مقارنة موجزة بالقانون الوضعي. وقد تناول البحث مفهوم الجرائم الإلكترونية وخصائصها، والأسس الشرعية لتجريم الأفعال الإلكترونية، ثم بيّن التكييف الفقهي لأبرز صورها مثل الاحتيال الإلكتروني، والقذف الإلكتروني، والتجسس واختراق الأنظمة، ونشر الشائعات عبر الوسائط الرقمية. كما ناقش البحث العقوبات الشرعية المترتبة على هذه الجرائم، وبيّن أن التعزير يمثل الإطار العقابي الأوسع لها، مع إمكانية تطبيق بعض الحدود في حالات محددة عند توافر شروطها الشرعية. وتوصل البحث إلى أن قواعد الشريعة الإسلامية ومقاصدها قادرة على استيعاب الجرائم الإلكترونية ومعالجتها معالجة متكاملة تحقق حفظ الحقوق ودفع المفاسد في البيئة الرقمية المعاصرة.

ABSTRACT

This study aims to clarify the jurisprudential characterization of cybercrimes and their rulings in Islamic law, with a brief comparison to positive law. The research addresses the concept and characteristics of cybercrimes and examines the Sharia foundations for criminalizing electronic acts. It also analyzes the jurisprudential classification of major cybercrimes such as online fraud, electronic defamation, cyber espionage, system intrusion, and spreading misinformation through digital platforms. The study discusses the applicable Islamic penalties and concludes that discretionary punishment (Ta'zir) constitutes the primary legal framework for most cybercrimes, while certain fixed punishments may apply under specific conditions. The research finds that Islamic legal principles and objectives are capable of addressing cybercrimes effectively and ensuring the protection of rights in the digital environment.

Keywords
الكلمات المفتاحية
الجرائم الإلكترونية، الفقه الإسلامي، التعزير، التكييف الفقهي
Cybercrime, Islamic jurisprudence, Ta'zir, legal characterization

Received	Accepted	Published online
استلام البحث	**قبول النشر**	**النشر الالكتروني**
11/03/2026	05/04/2026	13/05/2026

١. مقدمة

الحمد لله رب العالمين، والصلاة والسلام على سيدنا محمد، وعلى آله وصحبه أجمعين.

أما بعد:

يشهد العالم المعاصر انتقالًا واسعًا إلى البيئات الرقمية في المال والأعمال والخدمات وتداول المعرفة، وهو انتقالٌ فتح آفاقًا للتنمية والابتكار، لكنه أفرز في الوقت نفسه صورًا جديدة للسلوك الإجرامي أو أعاد تشكيل صورٍ تقليدية بوسائط رقمية محضة. وتضع هذه التحوّلات المنظومتين الشرعية والقانونية أمام أسئلة ملحّة تتصل بحدود التجريم ومجالات الردع وضوابط الإثبات، وبكيفية استحضار مقاصد الشريعة وقواعدها الكلّية عند تنزيل الأحكام على وقائع لا مادية يكون محلّها بيانات وهويات رقمية وبنى معلوماتية معقّدة. ومن ثمّ تتبدّى الحاجة إلى معالجة أكاديمية رصينة تؤصّل للجرائم الإلكترونية في ضوء أصول الفقه ومقاصده، مع

*Corresponding author yousraameen8@gmail.com

قراءةٍ مقارنةٍ متوازنة لمخرجات التقنين العربي والمعايير الدولية ذات الصلة؛ بغية بناء سياسة جنائية رقمية متّسقة وقابلة للتطبيق تراعي خصوصيات الوسيط التقني ومآلاته.

تبرز أهمية الموضوع من اتساع أثر الجرائم الإلكترونية وتعدّد صورها كالاحتيال عبر القنوات المالية، والابتزاز القائم على تسريب البيانات، والاختراق غير المشروع للأنظمة، والتجسّس على الخصوصية، ونشر الأخبار الكاذبة بما يمسّ أموال الأفراد وسمعتهم وأمنهم الرقمي، ويؤثر في ثقة المجتمع بالمؤسسات. كما تبرز من فجوةٍ تأصيليةٍ نسبية بين منطق المقاصد والقواعد الفقهية من جهة، ومتطلبات الإثبات والإجراءات التقنية والقانونية من جهة أخرى؛ إذ تميل معالجاتٌ إلى التقنية الخالصة المنبتّة عن التأصيل الشرعي، وأخرى إلى فقهٍ نظري مجتزأ لا يراعي سيولة الوسيط الرقمي، وثالثة إلى عرضٍ قانوني غير مؤسّس على قراءةٍ مقاصدية تُظهر مواضع الالتقاء والافتراق وإمكانات التكامل. ويسعى هذا البحث إلى ردم هذه الفجوة عبر إطارٍ مقاصديٍّ وقواعدي يضبط مناطات الحكم وييسّر تنزيلها على الصور المستجدّة، مع الإفادة النقدية من التجارب التشريعية العربية والاتفاقيات الدولية دون الارتهان لمدرسةٍ واحدة.

تنطلق إشكالية الدراسة من سؤالٍ مركزي: كيف يمكن تقعيد أحكامٍ شرعيةٍ منضبطة للجرائم الإلكترونية تكفل صون الحقوق ودرء المفاسد وجلب المصالح، باستثمار كليات الشريعة—حفظ الضروريات، لا ضرر ولا ضرار، سدّ الذرائع، المصالح المرسلة، حفظ الحقوق—وتحديد دور وليّ الأمر في سنّ التعازير لما لا يدخل تحت حدٍّ منصوص، ثم مواءمة ذلك مع مقتضيات القوانين الوضعية وآليات الإثبات الرقمي والتعاون العابر للحدود؟ ويتفرّع عنه تحرير المفهوم التشغيلي للجريمة الإلكترونية وتمييزها عن التقليدية، وبيان خصائصها ودوافعها، والتكييفات الفقهية لأشهر صورها، وموقع الحدود الممكن إعمالها وضوابط التعزير حيث لا حدّ، على وجهٍ يوازن بين مقتضيات الردع والعدالة الإجرائية ومآلات الأحكام.

يعتمد البحث منهجية مركّبة تجمع بين الوصف والتحليل لاستقراء البيئة الرقمية وخصائصها، والمنهج الأصولي/المقاصدي لاستنباط القواعد العامة الملائمة لسيولة التقنيات، والمنهج المقارن لموازنة المخرجات الشرعية بنصوص القوانين العربية والاتفاقيات الدولية، والمنهج التطبيقي من خلال نماذج واقعية لصور الجريمة وآليات جمع الأدلة وحفظ سلاسل الحيازة وشروط سلامة الدليل الرقمي. وتُعتمد تعريفاتٌ تشغيلية تضبط محلّ الحكم وتحدّ من اللبس؛ فالجريمة الإلكترونية كل فعلٍ مُجرّم شرعًا أو قانونًا يقع بوسائط رقمية أو يردّ على محلٍّ رقمي ويؤول إلى اعتداءٍ على حقٍّ معتبرٍ أو مصلحةٍ عامةٍ راجحة، والاعتداء على الخصوصية الرقمية نفاذٌ أو اطّلاعٌ أو معالجةٌ أو نشرٌ لبياناتٍ شخصية بغير إذنٍ معتبر بما يوقع الضرر، والاختراق نفاذٌ غير مشروع أو تجاوزٌ لصلاحياتٍ مرخّصة يفضي إلى تعطيلٍ أو إتلافٍ أو سرقةٍ أو عبثٍ بالأنظمة والبيانات.

وتُراعى اعتباراتٌ أخلاقيةٌ ومعياريةٌ صارمة: أمثلةٌ تعليمية خالية من بياناتٍ شخصية مميّزة، وتحقيق الحياد العلمي في المفاضلة بين الخيارات التقنية والقانونية بما يتّسق مع المقاصد، وضبط المصطلح وتحرير محلّ النزاع في موارد الخلاف ذات الأثر العملي مع بيان الراجح ودليله ومناط رجحانه. كما تُؤخذ تحدّياتٌ متوقعة بالحسبان: سيولة الواقع التقني، وتعقيد الإثبات الرقمي، وتداخل أدوار الفاعلين، وتفاوت الاستجابات التشريعية، وتنامي ظواهر الذكاء الاصطناعي والعملات الرقمية وما تثيره من أسئلةٍ في التكييف والمسؤولية. وسيقترح البحث حلولًا منهجيةً عملية، من قبيل ترسيخ قواعد عامة مرنة قابلة للتنزيل، وتضمين دلائل إجرائية مختصرة لحفظ الأدلة الرقمية، وبناء مصفوفاتٍ معيارية لتحديد المسؤوليات، وصياغة مبادئ تشريعية إطارية تراعي الخصوصية العربية ولا تنعزل عن مقتضيات التعاون الدولي.

٢. المبحث الأول: ماهية الجرائم الإلكترونية وضوابطها الشرعية

١.٢. المطلب الأوّل: مفهومُ الجرائمِ الإلكترونيّة وأنواعُها

أوّلًا: تعريفُ الجريمةِ لغةً واصطلاحًا

تدلّ مادّة «ج ر م» في العربية على الأصل اللغوي «القَطْع»، ثم نُقلت دلالتها إلى الجناية والإثم، فقيل: «أَجْرَمَ» إذا أتى ذنبًا أو اعتداءً، و«الجُرْم» الذنبُ نفسُه، وهو استعمالٌ راسخ في المعاجم التراثيّة وشواهدها[١]. ويُعضّد هذا المعنى ما قرّره مجمع اللغة العربية في المعجم الوسيط من أنّ «الجُرْم» الذنبُ والجريرة وما يُكتسب[٢] من فعلٍ مُستنكر .

أمّا اصطلاحًا في العلوم الجنائيّة، فالجريمة هي «فعلٌ أو امتناعٌ يقرّر له الشارعُ عقوبةً أو تدبيرًا إذا ورَدَ بنصّ عامّ يجرّمه»، وهو تعريفٌ إجرائيّ يَصِلُ الفعلَ بنصّ التجريم والجزاء دون تقييدٍ بمحلّه أو وسيلته.[٣] وقد بسط عبد القادر عودة عناصر هذا الضبط في بنية التجريم والعقاب في الشريعة وبيّن نقاط المقارنة مع القانون الوضعي .

---

[١] ابن منظور، لسان العرب، بيروت: دار صادر، ط٣، ١٤١٤ه.

[٢] مجمع اللغة العربية بالقاهرة، المعجم الوسيط، القاهرة: المجمع، ط٢، ١٩٧٢م.

[٣] عبد القادر عودة، التشريع الجنائي الإسلامي مقارنًا بالقانون الوضعي، دمشق/بيروت: مؤسسة الرسالة ناشرون، ط٣، ٢٠١٣م.

ثانيًا: تعريفُ الجريمةِ الإلكترونيّة فقهيًّا وقانونيًّا

يقترح هذا البحث تعريفًا تشغيليًّا للجريمة الإلكترونية بأنها: «كلُّ فعلٍ أو امتناعٍ مُجرَّمٍ شرعًا أو قانونًا يقع بواسطة منظوماتٍ رقميةٍ أو يردّ على محلٍّ رقميّ (بيانات/أنظمة/هويات)، ويؤول إلى الاعتداء على حقٍّ معتبرٍ أو مصلحةٍ عامةٍ راجحة». يتّسق هذا الضبط مع مقاصد الشريعة في الحفظ والوقاية والردع، كما ينسجم مع الأطر المعيارية الدولية التي صنّفت أفعال الاعتداء على سريّة البيانات وسلامتها وتوافرها، والجرائم المتّصلة بالحاسوب كالاحتيال والتزوير، وجرائم المحتوى، والاعتداء على الملكيّة الفكريّة [١]وعلى الصعيد العربي، وضعت الاتفاقية العربية لمكافحة جرائم تقنيّة المعلومات إطارًا للتجريم والتعاون القضائي وتعاريف إجرائيّة موحّدة بين الدول الأعضاء [٢] ويظهر التنزيل التشريعي لهذه المفاهيم في أنظمةٍ وطنيةٍ حديثة مثل نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية [٣]

ثالثًا: أهمُّ الخصائصِ التي تميّزُ الجرائمَ الإلكترونيّة

تتّسم الجرائم الإلكترونية بخصائص نوعيّة تفارق كثيرًا نظائرها التقليدية؛ من أبرزها لامادّيةُ محلّ الاعتداء حيث تكون «المعلومة/البيانات» موضوعًا للجريمة؛ وعابريةُ الحدود بما يُحدثُ تداخُلًا قضائيًّا واسعًا؛ وانخفاضُ كلفة الأداة مقابل ارتفاع شدّة الأثر وقابليّة التكرار؛ وإمكاناتُ الإخفاء والتمويه والتشفير وتعقيدُ سلاسل الحيازة؛ فضلًا عن تسارع الانتشار بحكم قابلية النسخ الفوري للمعلومات. وقد سجّل مكتب الأمم المتحدة المعني بالمخدرات والجريمة هذه السمات في دراسةٍ شاملة دعت إلى مواءمة الأطر الوطنية وتعزيز التعاون العابر للحدود [٤]وتعرض الأدبياتُ السوسيولوجيّة الجنائيّة لهذه الخصائص وتحلّل انعكاساتها على الضحيّة والمجتمع وآليات الردع [٥].

رابعًا: أبرزُ الدوافعِ لارتكابِ الجرائمِ الإلكترونيّة

تتراوح الدوافع بين الربح المالي المباشر—كالاحتيال المعلوماتي، وسرقة بيانات الدفع، وبرامج الفدية—والدوافع الأيديولوجيّة/السياسيّة كالتأثير في الرأي العام و«الهاكتيفيزم»، ودوافع الانتقام والمنافسة الاقتصادية، إضافةً إلى الحوافز الرمزية والسوقية داخل اقتصاديات المنصّات غير المشروعة في الشبكة المظلمة. وتُظهر دراسات علم الإجرام المعلوماتي تداخلًا بين دوافع الأفراد وبُنى الأسواق السوداء ودوائر الوساطة التقنية التي تُيسّر الجريمة وتقلّل تكلفتها .[٦]

خامسًا: أشهرُ صورِ الجرائمِ الإلكترونيّة

تجري الاستفادة تنظيميًّا من تصنيفاتٍ معياريةٍ جامعة، من أهمّها ما أقرّته اتفاقية بودابست: (أ) جرائمُ الاعتداء على الأنظمة والبيانات: الدخول غير المصرّح، اعتراض الاتصالات، التدخّل في البيانات أو الأنظمة بالحذف أو التعطيل أو حجب الخدمة؛ (ب) الجرائمُ المتّصلة بالحاسوب: الاحتيال المعلوماتي والتزوير المعلوماتي والاستيلاء غير المشروع؛ (ج) جرائمُ المحتوى؛ (د) الاعتداء على الملكيّة الفكريّة (Council of Europe, ٢٠٠١). وتتجلّى تطبيقاتٌ عربية حديثة لهذه التصنيفات في بنودٍ تُجرّم الوصول غير المصرّح وإساءة استخدام الأجهزة والبرمجيات الضارّة ونشر الشائعات والمحتوى غير المشروع، كما في النظام السعودي لعام ٢٠٠٧ والمرسوم الاتحادي الإماراتي لعام ٢٠٢١ [٧]

سادسًا: أثرُ التطوّرِ التقنيّ في انتشارِ هذه الجرائم

أسهمَ تعميم الحوسبة السحابية، واتّساع إنترنت الأشياء، وتيسّر أدوات الهجوم الجاهزة (Malware-as-a-Service) ، في خفض كلفة الجريمة ورفع أثرها وتكراريّتها، مع اتساع فجوة القدرات بين فاعلي الجريمة وجهات إنفاذ القانون. وتؤكّد التقارير الأمميّة أنّ قابلية القياس والنسخ الفوري للمعلومة تُضاعف أثر الاعتداء مقارنةً بالجرائم التقليدية، بما يستوجب تحديث أدوات الإثبات والتحليل الجنائي الرقمي وتوسيع قنوات التعاون الدولي [٨]

٢.٢. المطلب الثاني: الأسس الشرعية لتجريم الأفعال الإلكترونية

أولًا: مقاصد الشريعة في حفظ الضروريات الخمس.

المقاصد الكلية–حفظ الدين والنفس والعقل والنسل/العِرض والمال–هي الإطار الأعلى الذي يضبط به الاجتهاد الجنائي في البيئة الرقمية. فكل اعتداء إلكتروني يُهدّد واحدًا أو أكثر من هذه الضروريات (كالاختراق المفضي إلى تسريب البيانات الماسة بالسمعة والعِرض، أو الاحتيال الرقمي المُهدر للأموال، أو بثّ

---

[١] Council of Europe, Convention on Cybercrime Budapest Convention, CETS No. ١٨٥, (٢٠٠١).
[٢] جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، نصّ رسمي،(٢٠١٠).
[٣] أمر ملكي رقم م/١٧ لعام ٢٠٠٧والمرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة (نصّ رسمي، ٢٠٢١).
[٤] UNODC, Comprehensive Study on Cybercrime, ٢٠١٣ .
[٥] Majid Yar & Kevin F. Steinmetz, Cybercrime and Society, ٣rd ed., SAGE, ٢٠١٩ .
[٦] Thomas J. Holt & Adam M. Bossler, Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses, Routledge, ٢٠١٦st ed., ؛ وانظر أيضًا: Yar & Steinmetz، ٢٠١٩، الطبعة الثالثة).
[٧] (المملكة العربية السعودية، نظام مكافحة الجرائم المعلوماتية، ٢٠٠٧؛ الإمارات العربية المتحدة، المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١، ٢٠٢١).
[٨] (UNODC, ٢٠١٣؛ وانظر أيضًا: Explanatory Report to the Convention on Cybercrime, Council of Europe, ٢٠٠١).

الشائعات المُقوِّضة لأمن المجتمع) يدخل في نطاق ما تُعاقِب عليه الشريعة؛ لأن مناط التجريم هو الإضرار بهذه الكليات أو ملحقاتها الحاجية والتحسينية. ويضيف بعض المقاصديين المعاصرين توكيداتٍ على مقاصد "حفظ النظام والحرية والعدالة"[1] بما يُعين على ضبط السياسات الجنائية الحديثة في الفضاء الرقمي بوصفها وسائل لحراسة المقاصد لا مزاحمة لها.

ثانيًا: قاعدة "لا ضرر ولا ضرار" وأثرُها في التجريم.

قاعدة «الضرر يُزال» المتفرعة عن الحديث النبوي «لا ضرر ولا ضرار» تُنشئ معيارًا عامًا يُجرَّم بمقتضاه كل فعلٍ إلكترونيّ مُضرٍّ ابتداءً أو مقابلةً، ويُوجب جبرَه ودفعه ومنع أسبابه؛ فتسريب البيانات الشخصية، وتعطيل الأنظمة الحيوية (المستشفيات، المرافق العامة)، والهجمات الحرمانية (Ransomware)؛ كلها أضرارٌ صِرفٌ تُمنَع ويُزال أثرُها وتُقدَّر جزاءاتُها تعزيرًا، ويُرشد فقه القواعد إلى ألا يُزال الضرر بضررٍ مماثل أو أشدّ، وألا تُتَّخذ الرخص وسيلةً للتحايل. وبذلك تكون القاعدة ميزانًا عامًّا للتكييف ومنع تغوّل المصلحة الخاصة أو العبث التقني على حساب الحق العام والخاص.

ثالثًا: قاعدة "سدّ الذرائع" وحمايتها للمجتمع الرقمي.

تُقرِّر الشريعة منع الوسائل التي يغلب على الظنّ إفضاؤها إلى المفسدة؛ وهو أصلٌ اشتهر تقريرُه في المدرستين المالكية والحنبلية. وفي المجال الرقمي تتجلّى الذرائع في بنى تقنية أو ممارسات تفتح الطريق إلى الإضرار؛ كتصميم منصات تسمح افتراضيًّا بجمعٍ مُفرِط للبيانات دون ضوابط، أو نشر أدواتٍ تكسِرُ الحماية وتُسهِّل اقتحام الأنظمة. فيُمنَع ما كان وسيلةً راجحة الإفضاء إلى العدوان أو انتهاك الخصوصية—even قبل وقوع المفسدة—ويُشرَع لوليّ الأمر تقييد المباحات التقنية إذا غلبت مفسدتُها على مصلحتها. وهذا يُوفِّر سندًا أصوليًّا لسياسات "الأمن بالتصميم" و"الخصوصية بالتصميم" ومنع أدوات الاختراق وتسويقها بلا ترخيص.

رابعًا: قاعدة "حفظ الحقوق" وأهميتها في المعاملات الإلكترونية.

تندرج تحت حفظ الحقوق جملة من القواعد الكلية: "العادة محكَّمة" و"اليقين لا يزول بالشك" و"الضرر يُزال" و"الغُنم بالغُرم"، وهي قواعد تُعين على ضبط المعاملات الإلكترونية حيث تتعاظم التعويلات التعاقدية والواجهات البرمجية وسياسات الاستخدام. فتحكيم العرف الرقمي المنضبط (كقواعد منصّات الدفع أو معايير الإثبات التقنية) معتبرٌ ما لم يُخالف نصًّا أو قاعدةً قطعية، كما أن اليقين في سلامة الدليل الرقمي لا يزول بالشك المجرد، بل يحتاج إلى بيّنةٍ فنيةٍ مقبولة تُثبت سلامة سلسلة الحيازة وتكامل البيانات. ومن ثمّ تُصان حقوق المتعاملين رقمياً بإثباتات معيارية وبعقودٍ واضحةٍ وتدابيرِ مسؤوليةٍ متوازنة بين المزوّدين والمستخدمين والوسطاء.

خامسًا: قاعدة "المصالح المرسلة" ودورها في استحداث أحكام.

سيولة الوسائط الرقمية وتحوّل صور الجريمة يستدعيان اجتهادًا يلحظ "المصلحة المرسلة"؛ أي المصالح التي لم يشهد نصٌّ خاصّ باعتبارها أو إلغائها، لكنها ملائمة لمقاصد الشرع وكلياته. وبها يمكن تسويغ بناء منظوماتٍ للإثبات الرقمي، وإقرار بدائل عقابيةٍ غير تقليدية (كالمنع من الوصول، والتدريب الإلزامي على أمن المعلومات)، وسَنّ سياسات "إدارة المخاطر السيبرانية" ما دامت تحقّقُ حفظ الضروريات وتدرأ المفاسد الراجحة. ويُفرِّق الأصوليون بين اعتبار المصلحة المرسلة بضوابطها وبين نزعة تقديم "المصلحة" بإطلاقٍ عند التعارض مع النص والإجماع—وهي أطروحةٌ نوقِشَت ونُقدِّرها نقدًا علميًّا—ليظلّ الاجتهاد المقاصدي منضبطًا بكليات الشريعة ومصادرها القطعية.

سادسًا: دور وليّ الأمر في سنّ عقوباتٍ تعزيريةٍ للجرائم الحديثة.

العقوبات التعزيرية مجالُ ولايةٍ وسياسةٍ شرعيةٍ يُناط فيها بسلطة الدولة تقديرُ النوع والمقدار بما يحقق الردع والعدل ويصون النظام العام، وهو ما يصدق على الجرائم الإلكترونية ذات الصور المتجددة. فيندرج تحت التعزير—وفق ضوابطه الشرعية—تغليظ الغرامات، والمنعُ من مزاولة بعض الأنشطة الرقمية، وإغلاق المنصّات أو تعليق تراخيصها عند الإخلال الجسيم، وربطُ الجزاءات ببرامج إصلاحٍ تقني وأخلاقي. كما تُسوِّغ السياسة الشرعية اعتمادَ إجراءاتٍ وقائية (تراخيص، معايير أمنية ملزمة، بلاغات إلزامية لحوادث الاختراق) ما دامت تحقق مصلحةً عامة راجحة وتراعي حقوق الأفراد والإجراءات العادلة.

٣.٢. المطلبُ الثالث: التكييفُ الفقهيُّ للجرائمِ الإلكترونيّة

أوّلًا: إلحاقُ جرائمِ الاحتيالِ الإلكتروني بأحكامِ السرقة

تُعرِّف المذاهبُ السرقةَ بأنها أخذُ مالٍ متقوَّمٍ مَحفوظٍ في حِرزٍ خُفيةً بغير حقّ، مع اشتراطاتٍ كالنِّصاب والحِرز وكيفيّة الأخذ. وقد قرّر الحنفيةُ أنّ "حقيقةَ السرقةِ إخراجُ المال من الحرزِ على وجهِ الخُفية"[2] وبيّن السرخسي أنّ مناطَ الحدّ يتحقّق بالأخذِ من الحرز خُفيةً مع قيامِ يدِ المالك عليه[3] وفي التطبيقات الرقمية: إن ترتّب على الاحتيال نقلٌ فعليٌّ لمالٍ متقوَّمٍ من حسابٍ ماليٍّ محفوظٍ (حِرزٍ اعتباريّ) إلى يدِ الجاني خُفيةً وبدون إذنٍ صحيح، أمكن تنزيلُ أحكامِ السرقة حدًّا

[1] https://doi.org/10.58916/jhas.v10.i4
[2] (الكسّاني، بدائع الصنائع، بيروت: دار الكتب العلمية، ط٢، ١٩٨٦م).
[3] (السرخسي، المبسوط، بيروت: دار المعرفة، ط١، ١٤٠٦هـ).

بشروطها، وإلّا فالأصلُ إلحاقه بأكلِ أموالِ الناس بالباطل والغصب والتزوير المعلوماتي والتسبُّب الضارّ، ويكون الجزاءُ تعزيريًّا مع الضمانِ وردِّ المال. وقد نصّ ابن قدامة على أنّ المالَ المتقوَّم يثبت فيه الضمانُ والغُرمُ عند الإتلاف والاستيلاء [1]كما أقرّ "مجمع الفقه الإسلامي الدولي" اعتبارَ الحقوق والمنافع والمعلومات والأعيان المعنوية أموالًا متقوّمةً تجب حمايتها وتُضمن عند الاعتداء ([2]وبذلك فاحتيالُ تحويلاتٍ مصرفيةٍ إلكترونية—متى استوفى شروط الحِرز والنَّقل الخفي—يقاربُ مفهومَ السرقة حدًّا، وإلّا فتعزيرٌ مُغلَّظٌ وضمان.

ثانيًا: إلحاقُ جرائمِ القذفِ الإلكتروني بأحكامِ القذفِ الشرعي

القذفُ حدًّا هو رميُ المُحصَنة أو المُحصَن بالزِّنا أو نفيُ النَّسب تصريحًا أو كنايةً مفهومة، وتُقامُ به العقوبةُ بثمانين جلدة مع ردِّ الشهادة والحُكم بالفسق ما لم يتُب، وفقًا لتفسير الفقهاء لآيات سورة النور. وقد فصّل ابن قدامة شروطَ إقامةِ الحدّ وأدلته ، وشرح القرطبيُّ دلالات آيات القذف وأحكام البيّنة واللِّعان [3]وعليه فكلُّ منشورٍ إلكترونيّ يتضمن اتّهامًا صريحًا بالزِّنا أو نفيَ نسبٍ يثبتُ به حدُّ القذف بشروطه (بلوغٌ، عقلٌ، تعيينُ المقذوف، انتفاءُ الشبهة، قيامُ البيّنة أو الإقرار)، أمّا السبُّ والشتْمُ والإشاعةُ الماسّة بالاعتبار دون قذفٍ صريحٍ فتندرجُ في التعزير وتقديرِه بحسبِ الجناية وسَعَة ضررِها الرقمي.

ثالثًا: التجسُّسُ واختراقُ الخصوصيّةِ وحكمُه في الفقه الإسلامي

الأصلُ الشرعيّ في حرمةِ التَّجسُّس قوله تعالى: ﴿وَلَا تَجَسَّسُوا﴾ [الحجرات: ١٢]، وما صحّ من السنّة في النهي عن الاطّلاع على بيوت الناس واستراقِ سمعِهم؛ ففي الصحيح: «مَنِ اطَّلَعَ في بيتِ قومٍ بغيرِ إذنِهم فقد حلّ لهم أن يَفْقَئوا عينَه»[4]. وقرّر ابن كثير عند تفسير النهي أنّه يشملُ كلَّ ما يفضي إلى الوقيعةِ بغير حقّ (ابن كثير، تفسير القرآن العظيم، بيروت: دار المعرفة، ط٢، ١٤٠٧هـ). والمجالُ الرقميُّ داخلٌ في هذا العموم: فاختراقُ البريد والهواتفِ وقواعدِ البيانات واعتراضُ الاتصالات تجسّسٌ محرّم، يُعاقَبُ عليه تعزيرًا وتُجبُ تبعاتُه من ضمانِ ما ترتّب من أضرارٍ ماديةٍ ومعنوية، مع استثناءاتٍ مقيّدةٍ بولايةِ القضاء والتحرّي النظاميّ في الجرائمِ وبمراعاةِ الضوابط الشرعية والقانونية (ضرورةٌ، اختصاصٌ، قدْر الحاجة).

رابعًا: حكمُ اختراقِ الأنظمةِ وسرقةِ المعلومات (الغصبُ والاعتداء)

الغصبُ هو الاستيلاءُ على حقّ الغيرِ عدوانًا، ويتعلّق بالأعيانِ والمنافعِ والحقوق، وتثبتُ به الضماناتُ عند الإتلاف والمنعِ من الانتفاع [5]وقد توسّع فقهُ المعاصِر في اعتبارِ الأعيانِ المعنويّة والبياناتِ والبرمجياتِ أموالًا وحقوقًا متقوَّمة، ومن ذلك تقريرُ المجمعِ الفقهي الدولي في الملكية الفكرية ووجوبِ صونِها ومنع الاعتداءِ عليها. وعليه فإن اختراقَ الأنظمةِ وإتلافَ البياناتِ أو حبسَها (كالحجبِ والـRansomware) أو الاستيلاءَ على أسرارٍ تجاريةٍ يُكيَّفُ غصبًا واعتداءً مُوجِبًا للضمانِ والتعزير، ويغلَّظُ بحسبِ خطورةِ المرفق المعتدى عليه ومآلات الضرر. ويُقاسُ على الإتلافِ المادّيّ ما يساويه أو أشدُّ منه من الإتلافِ المعنويّ المُفضي إلى خسائرَ مُتحقِّقة.

خامسًا: حكمُ نشرِ الفتنِ والأخبارِ الكاذبة عبر الوسائطِ الرقميّة

دلّت النصوصُ على وجوبِ التثبّتِ قبل إذاعةِ الأخبار: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَإٍ فَتَبَيَّنُوا﴾ [الحجرات: ٦]، وعلى تحريمِ الكذبِ وإشاعةِ الفاحشةِ والخوضِ في الأعراض (النور: ١١–١٩). وفي الحديث: «كَفَى بالمرءِ كَذِبًا أن يُحدِّثَ بكلِّ ما سمع»[6]. وبناءً عليه فإن ترويجَ الشائعاتِ الرقميّة وقلبَ الحقائقِ والتحريضَ المؤدّي إلى الفتنةِ والاضطرابِ جرائمُ تعزيريّة تُقدَّرُ بقدرِ ضررِها واتّساعِ أثرِها، وقد ترتقي إلى صورٍ أشدّ إذا اقترنت بقذفٍ صريحٍ أو بتهديدِ السِّلم العام، ويُستندُ في التغليظ إلى قاعدةِ صيانةِ النظام العام وتغليبِ مصلحةِ الدفع والوقاية.

سادسًا: الفرقُ بين الجريمةِ الإلكترونيّة والجريمةِ التقليديّة

الفروقُ المؤثّرةُ فقهًا وقضاءً تشملُ: أوّلًا لاماديّةُ محلِّ الاعتداء في كثيرٍ من الصور (بيانات/منافع/حقوق) مع الاعترافِ بقيمتها الماليّة وضمانِها؛ ثانيًا عابريةُ الحدود وما تُحدِثُه من تعقيدٍ في الاختصاصِ والإثبات؛ ثالثًا إمكاناتُ الإخفاءِ والتمويه والتّزوير الرقميّ وتعقيدُ سلاسلِ الحيازة؛ رابعًا سُرعةُ الانتشارِ والتضاعفُ الهائل للأثر بسبب قابليةِ النسخِ الفوريّ؛ خامسًا تحوّلُ مفهومِ الحِرزِ إلى حِرزٍ اعتباريّ (حواجزُ تقنيّة/أنظمةُ أمنٍ معلوماتي) يقابلُ الحِرزَ المادّي في الفقهِ الكلاسيكي. وقد نبّه الفقهُ المعاصرُ إلى أنّ هذه الفروق لا تُسقِط الأوصافَ الشرعيّة، بل تستدعي اجتهادَ تنزيلٍ يُحافظُ على المقاصدِ ويُطوّرُ أدواتِ الإثباتِ والحماية [7]كما قرّر المجمعُ الفقهيُّ الدولي أنّ المصلحةَ العامةَ وحمايةَ النظامِ الرقميّ تُسوّغان سياساتٍ وقائيّة وإجرائيّة خاصّة دون إخلالٍ بالضماناتِ الشرعيّة [8]

---

[1] (ابن قدامة، المغني، الرياض: دار عالم الكتب، ط٣، ١٩٩٧م).
[2] مجمع الفقه الإسلامي الدولي، قرارات وتوصيات المجمع، جدة: المجمع، ط٢، ٢٠٠٦م).
[3] (القرطبي، الجامع لأحكام القرآن، بيروت: دار الكتب العلمية، ط١، ٢٠٠٣م).
[4] (صحيح البخاري، بيروت: دار ابن كثير، ط٣، ٢٠٠٢م)
[5] (السرخسي، المبسوط، ١٤٠٦هـ؛ ابن قدامة، المغني، ١٩٩٧م).
[6] (ابن حجر، فتح الباري، بيروت: دار المعرفة، ط٢، ١٣٧٩هـ)
[7] (شبير، فقه النوازل في العبادات والمعاملات، عمّان: دار النفائس، ط٢، ٢٠٠٧م؛ القرضاوي/القَرَضاغي، فقه المعاملات المالية المعاصرة، الدوحة: دار البشائر/الرواد، ط٢، ٢٠١٠م).
[8] (مجمع الفقه الإسلامي الدولي، قرارات وتوصيات، ط٢، ٢٠٠٦م).

٣. المبحث الثاني: أحكام الجرائم الإلكترونية وعقوباتها في الفقه الإسلامي والقانون الوضعي

١.٣ .المطلب الأوّل: العقوبات الشرعية للجرائم الإلكترونية

أوّلًا: الحدود التي يمكن أن تنطبق على بعض الجرائم (كالسرقة والقذف).

الأصل في الحدود أنها عقوباتٌ مقدّرة تُدرأ بالشبهات وتُقام باجتماع شروطها وارتفاع موانعها. والقياس على صورٍ رقميةٍ يقتضي تحرير المناط بدقّة؛ فسرقةُ الأموال المنقولة رقميًا تلحقُ بأخذِ «مالٍ متقوَّمٍ» من «حرزٍ» خفيةً إذا تحقّق نقلُ يدِ المالك إلى يدِ الجاني من حرزٍ اعتباري (أنظمة الحماية والحسابات الموثّقة) وبلغ المالُ النصاب وثبتت طريقةُ الأخذ بلا شبهة؛ وإلا انصرف الحكمُ إلى التعزير مع الضمان وردّ الحقوق. وكذا القذفُ الإلكتروني: إن تضمّن اتهامًا صريحًا بالموجب حدًّا—كرمي المحصن/المحصنة بالزنى أو نفي النسب وأمكن إثباته بشروطه قامت عقوبة الحدّ، أمّا السبّ والبهتان دون قذفٍ صريح فمجاله التعزير. هذا التفريق قرّره الفقهاء عند تحرير حدّ السرقة وحدّ القذف وشروط كلٍّ منهما، وأفادته مباحثُ «الحِرز» و«النصاب» و«الصريح والكناية» في كتب الحدود. [١]

ثانيًا: التعزير وضوابطه في الجرائم التي لا حدّ فيها.

حقلُ الجرائم الإلكترونية—لحداثة وسائطه وتنوّع صُوَره—يغلب عليه التعزير، وهو عقوبةٌ غير مقدّرة تُناط بتقدير القاضي ووليّ الأمر وفق ضوابط: مراعاة المقاصد، وتناسب العقوبة مع الجناية وأثرها، واعتبار حال الجاني والعود، وتحقيق الردع مع العدالة الإجرائية. تتعدّد صُوَر التعزير بحسب المصلحة: الغرامات، الحبس التعليمي، المنع من مزاولة أنشطة رقمية،[٢] تعليق التراخيص، مصادرة الأدوات غير المشروعة، الإلزام بتدريبٍ تقنيٍّ وقائي، ونحوها مما تقرّه السياسة الشرعية.[٣]

ثالثًا: عقوبة التجسّس والاعتداء على الخصوصية.

يدخل التجسّس الرقمي—كاختراق المراسلات والهواتف وقواعد البيانات واعتراض الاتصالات—في عموم النهي القرآني عن التجسّس، وتتدرج جزاءاته في باب التعزير بحسب جسامة الاعتداء ومآلاته، مع ضمان الأضرار المادية والمعنوية. إذا اقترن التجسّس بجرائم أُخر (قذفٍ صريح، ابتزاز، سرقة بيانات مالية) لحقته أحكامُها الخاصة. ويُستثنى من المنع ما كان وفق ولايةٍ نظاميةٍ مُقيّدة بضوابط القضاء والتحرّي، وبقدر الحاجة. انظر: ابن العربي، أحكام القرآن (بيروت: دار الكتب العلمية، ط١، ٢٠٠٣م)؛ الطبري، جامع [٤]

رابعًا: عقوبة نشر الشائعات والإضرار بالمجتمع.

نشرُ الأخبار الكاذبة والتحريضُ المفضي إلى الفتنة وتقويض السِّلم الأهلي عبر الوسائط الرقمية جرائمُ تعزيرية تُغلّظ بقدر اتساع أثرها وضررها المُتحقّق. فإن اشتملت على قذفٍ صريح أُقيم حدّ القذف، وإلا فالتعزير بوسائله المعتبرة. ويؤسِّس لذلك أصلُ التثبّت واعتبارُ المآلات، ومعنى «حفظ النظام» ضمن الضروريات الملحقة بمقاصد الشريعة. [٥]

خامسًا: تقدير العقوبات من قبل وليّ الأمر.

لوليّ الأمر سلطةُ السياسة الشرعية في تقنين التعزير وتوحيد معاييره وإقرار الإجراءات الوقائية، ما دام تصرّفه «منوطًا بالمصلحة». وفي الجرائم الإلكترونية يمتدّ ذلك إلى سنّ تراخيص مزاولة بعض الأنشطة التقنية، وإلزام الجهات بمعايير أمن معلوماتي، والتبليغ الإلزامي عن حوادث الاختراق، وتحديد جداول غراماتٍ وتدابيرَ إصلاحٍ ملائمة. مع ضرورة صيانة الضمانات الإجرائية: لا عقوبة إلا بنصّ، ولا مساس بالخصوصية إلا بولايةٍ قضائية، وتناسبُ الجزاء مع الجناية. انظر: أبو يعلى، الأحكام السلطانية (١٩٨٣م)؛ ابن نجيم، الأشباه والنظائر (١٩٨٣م)؛ الطرطوشي، سراج الملوك (بيروت: دار الكتب العلمية، ط١، ١٩٩٤م).

سادسًا: الاجتهاد الفقهي في المستجدّات التقنية.

تقتضي سيولة التقنية تجديدَ النظر بضوابطه: اعتبار المصالح المرسلة الملائمة للكليات، وقياس الأشباه والنظائر، وتحقيق المناط الخاص، والتكييف الدقيق للحقوق الرقمية بوصفها «أموالًا وحقوقًا متقوَّمة»، وبناء منظومات إثباتٍ رقميةٍ عدلية تراعي سلامة سلسلة الحيازة. ويُستدلّ لذلك بمباحث المقاصد والسياسة الشرعية، وبالدراسات المعاصرة في النظام الجنائي الإسلامي التي تُبرز مرونة التعزير وإمكانات مواءمته لأدوات العصر. [٦]

---

[١] انظر: ابن رشد، بداية المجتهد ونهاية المقتصد (القاهرة: دار الحديث، ط١، ١٤٢٥هـ/٢٠٠٤م)؛ الشوكاني، نيل الأوطار (بيروت: دار الجيل، ط٢، ١٩٧٣م)؛ الزحيلي، الفقه الإسلامي وأدلته (دمشق: دار الفكر، ط٤، ١٩٩٧م).

[٢] انظر: أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي (القاهرة: دار الفكر العربي، ط١، ١٩٥٥م)؛

[٣] ابن فرحون، تبصرة الحكّام في أصول الأقضية ومناهج الأحكام (بيروت: دار الكتب العلمية، ط١، ١٩٨٦م)؛

[٤] البيان (القاهرة: دار هجر، ط١، ٢٠٠١م)؛ أبو زهرة، أصول الفقه (القاهرة: دار الفكر العربي، ط٣، ١٩٥٨م) في أساسات «الضرر» و«المصلحة».

[٥] انظر: الشاطبي، الموافقات تحقيق مشهور آل سلمان (الخبر: دار ابن عفّان، ط١، ١٤١٧هـ/١٩٩٧م)؛ ابن نجيم، الأشباه والنظائر (بيروت: دار الكتب العلمية، ط١، ١٩٨٣م) في قاعدة «الضرر يزال» وما تفرّع عنها.

[٦] انظر: الجويني، غياث الأمم في التياث الظلم (بيروت: دار المنهاج، ط١، ٢٠٠٧م)؛ الشاطبي، الموافقات (١٩٩٧م)؛ محمد سليم العوّا، في أصول النظام الجنائي الإسلامي (القاهرة: دار النهضة العربية، ط٢، ١٩٨٣م)؛ أحمد فتحي بهنسي، السياسة الجنائية في الشريعة الإسلامية (القاهرة: دار الشروق، ط٣، ١٩٨٣م).

٢.٣ .المطلبُ الثاني: موقفُ القوانينِ الوضعيّةِ من الجرائمِ الإلكترونيّة

أوّلًا: التشريعاتُ العربيةُ في مكافحةِ الجرائمِ الإلكترونيّة.

عرفت المنطقةُ العربيةُ موجةَ تقنينٍ متدرّج للجرائمِ المعلوماتيّة خلال العقدين الأخيرين، اتّخذت صورًا متقاربة في التجريم والإجراءات مع اختلافٍ في حدّةِ العقوبات واتّساعِ التعاريف. من الأمثلة الدالّة: قانونُ البحرين رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات الذي قسّم الأفعال إلى اختراقٍ، وإتلافِ بيانات، وغشٍّ إلكتروني، ونصّ على ظروفٍ مشدِّدةٍ عند المساسِ بالبيانات أو المرافق الحسّاسة، وهو منشورٌ في البوّابة الرسمية وفي السجلّ التشريعي الوطني. [١]

وفي قطر صدر قانون مكافحة الجرائم الإلكترونيّة رقم (١٤) لسنة ٢٠١٤ متضمّنًا أبوابًا للتعريفات وجرائمِ اختراق الأنظمة والبرامج والشبكات وإجراءاتِ الضبط، مع إتاحة النسخة الإنجليزية عبر هيئة تنظيم الاتصالات. [٢]

وأقرّ المغرب مبكرًا القانون ٠٧-٠٣ المكمّل لقانون العقوبات في ما يتعلّق بالجرائم المرتبطة بمعالجة المعطيات الآلية، محدِّدًا صور الدخول غير المصرّح والتخريبِ والعرقلةِ كجرائمٍ أصيلة.

كما سنّت الأردن قانون الجرائم الإلكترونيّة رقم ١٧ لسنة ٢٠٢٣ الذي وسّع نطاق الأفعال المجرّمة وشدّد العقوبات، وأعلن دخوله حيّز النفاذ في ١٣ أيلول/سبتمبر ٢٠٢٣ وفق الجريدة الرسمية.

ثانيًا: التشريعاتُ الدوليّةُ وأبرزُ الاتفاقيات.

يتصدّر المشهدَ الدولي «البروتوكول الإضافيّ الثاني لاتفاقية بودابست بشأن التعاون المُعزّز والكشف عن الأدلّة الإلكترونيّة» (٢٠٢١)، إذ اعتمدَهُ مجلسُ وزراء مجلسِ أوروبا وفتح بابَ التوقيعِ عليه لاحقًا؛ وهو ييسّر طلباتِ الكشف العاجلة والتعاونَ مع مزوّدي الخدمة عبر الحدود.

كما يمثّل «اتفاق مالابو» للاتحاد الإفريقي (٢٠١٤) إطارًا قارّيًّا لتقريب تشريعات الأمن السيبرانيّ وحماية البيانات في إفريقيا.

وفي الاتحاد الأوروبي دخل «تنظيم الأدلة الإلكترونيّة» رقم ١٥٤٣/٢٠٢٣ حيّزَ النفاذ في ١٨ آب/أغسطس ٢٠٢٣ ليُعمل به إلزامًا بعد فترةِ انتقال حتى ٢٠٢٦، مُقرّرًا أوامرَ أوروبية للإنتاج والحفظ موجّهةً مباشرةً لمزوّدي الخدمة.

ويرتبطُ بذلك تحديث إطار الثقة والهوية الرقمية عبر تنظيم (EU)٢٠٢٤/١١٨٣ eIDAS»)٢(« الذي يُعزّز الحجّية القانونية للمعرّفات والشهادات الإلكترونية العابرة للحدود.

وتوازي هذه المنظومةَ حمايةُ البيانات في «الاتفاقية ١٠٨+» المُحدَّثة (٢٢٣CETS) التي قوّت ضماناتِ الخصوصية وحوكمةَ المعالجة.

ثالثًا: المقارنةُ بين القانونِ الوضعيّ والفقهِ الإسلاميّ.

يهدف القانونُ الوضعيُّ إلى توحيد أوصاف الجريمة وإجراءاتِ ملاحقتها وضماناتِ المحاكمة، ويُدخل أدواتٍ خاصةً بالتعاونِ عبرَ الحدود وبالإثبات الرقمي، بينما ينطلقُ الفقهُ الإسلاميّ من مقاصدِ الحفظ والعدل واعتبار المصالح والذرائع، مع مرونةِ التعزير حيث لا حدّ. نقطةُ الالتقاء تظهرُ في حماية الضروريات الخمس (المال، العرض، النظام العام) واعتبارِ الضرر، بينما يختلف المسلكُ في تقدير العقوبات وضبطِ القيود على حرّية التعبير؛ لذا تُفيدُ التجربةُ الأوروبية في موازنة النفاذ إلى البيانات مع الضمانات (مثال: تحفظات سلطات حماية البيانات الأوروبية على الوصول الأمني المباشر).

والنتيجةُ المنهجيّة: إمكانُ مواءمة أدوات القانون الوضعيّ—أوامر الإنتاج والحفظ، معايير الهوية الرقمية، قواعد حماية البيانات—مع مقاصدِ الشريعة متى روعيت الضرورات والحقوق والإجرائية العادلة.

رابعًا: وسائلُ الإثباتِ القانونيةُ للجرائمِ الإلكترونيّة.

تتجه الأنظمةُ المقارنة إلى وضع قواعدَ خاصّة بالأدلّة الرقمية: ففي الولايات المتحدة أضيفت القاعدتان ٩٠٢(١٣) و٩٠٢(١٤) إلى «قواعد الإثبات الفيدرالية» عام ٢٠١٧ لإتاحة «التوثيق الذاتي» لبعض المخرجاتِ الرقمية وشهاداتِ سلامةِ النسخ دون شاهدٍ مباشر، مع بقاء عبءِ السماعِ والموثوقيّة. [٣]

وعلى مستوى المعايير الفنية تُعدّ « ISO/IEC٢٧٠٣٧:٢٠١٢» مرجعًا دوليًّا لإجراءات التعرّف والجمع والاكتساب والحفظ بما يصون سلامةَ الدليل.

وعند القاضي الأوروبيّ صدرت أدلّةٌ عملية من مجلس أوروبا (دليل الأدلّة الإلكترونيّة ٣.٠٧) تُبيّن مسالكَ الضبط والموثوقية وسلسلةَ الحيازة.

وإجرائيًّا، يقرّر تنظيمُ «الأدلة الإلكترونية» في الاتحاد الأوروبي أوامرَ إنتاجٍ وحفظٍ مباشرةً لمزوّدي الخدمة عبر الحدود، ما ينعكسُ على حجّيةِ السجلات وشهاداتِ مقدّمي الخدمة في الإثبات.

خامسًا: آليّاتُ التعاونِ الدوليّ لمكافحةِ هذه الجرائم.

يُؤطِّر «نظام نقاط الاتصال المتاحة ٧/٢٤» المنصوصُ عليه في اتفاقية بودابست تبادلَ الطلبات العاجلة بين الدول وتنسيقَ الحفظ السريع للبيانات.

---

[١] https://legalaffairs.gov.bh/

[٢] https://www.cra.gov.qa/

[٣] https://www.law.cornell.edu/

وتقوم منظومةُ الإنتربول على شبكة I-٢٤/٧ لربط أجهزةِ إنفاذ القانون وقواعدِ البيانات عالميًّا.

كما أوجد «قانون السحابة» الأمريكي (CLOUD Act) إطارًا لمعاهداتِ نفاذٍ متبادل إلى البيانات مع دولٍ كالمملكةِ المتحدة وأستراليا، لتيسير الحصول على الأدلة من مزوّدي الخدمة عبر الحدود ضمن قيودٍ وضماناتٍ محدّدة.[١]

ويُكمل «البروتوكول الإضافيّ الثاني» لبودابست هذه الآلياتَ عبر توسيعِ سُبلِ طلبِ الإفصاح المباشر ومخاطبةِ مزوّدي الخدمة الأجانب وفق ضوابطِ حمايةِ البيانات.

سادسًا: قصورُ بعضِ التشريعاتِ أمامَ التطوّرِ التقنيّ.

تُظهِر تقاريرُ حقوقيّةٌ ودراساتُ سياساتٍ إقليمية أنّ بعض قوانين «الجرائم الإلكترونيّة» في المنطقة تتّسع بألفاظٍ فضفاضةٍ تُجرّم محتوياتٍ تعبيرية وتحجب الضماناتِ الإجرائية، ما يهدّد التناسبَ ويُضعف الثقة الرقمية—ومن شواهد ذلك النقاشات حول القانون الأردنيّ لسنة ٢٠٢٣ وانتقاداتُ المنظّمات الحقوقية له عند التطبيق.

Human Rights Watch[٢]

كما نَبَّهَت تقاريرٌ متخصّصة إلى النزوع نحو توظيف قوانينٍ جنائيةٍ رقمية لكبح التعبير أو الشرعنةِ للتقييد خارج إطار الضرورة والملاءمة، داعيةً إلى معاييرَ أوضح وضماناتٍ أقوى[٣].

٣.٣. المطلبُ الثالث: التحدّياتُ المعاصرةُ في تطبيقِ الأحكامِ الشرعيّة

أوّلًا: صعوبةُ الإثباتِ والتعقّبِ الرقمي

تفرضُ طبيعةُ الدليلِ الرقمي—بصفته سريعَ الزوال وقابلًا للتغيير والنسخ—اشتراطاتٍ منهجيّةً صارمةً في الجمعِ والحفظِ والتوثيق؛ إذ يتعيّنُ ضبطُ سلسلةِ الحيازة (Chain of Custody)، وتثبيتُ سلامةِ البيانات ببصماتٍ تجزئيّة، وتقييدُ جميع الإجراءات فنّيًا وزمنيًا لئلاّ يختلّ شرطُ الموثوقيّة أمام القضاء. وقد رسّمت المعاييرُ الدوليّة (ISO/IEC ٢٧٠٣٧) الخطواتِ الأولى من التعرّفِ والجمعِ والاكتسابِ والحفظ، مؤكّدةً على أن أيَّ تغييرٍ لا مفرّ منه يجبُ توثيقُه توثيقًا كاملًا، كما حافظ "دليلُ الممارسة الرشيدة للأدلّة الرقمية" لدى الشرطة البريطانية (ACPO/NPCC) على قواعدَ عمليّةٍ متداولةٍ في الضبط الميداني. هذه المتطلباتُ تجعلُ الإثباتَ الرقميَّ أكثر حساسيةً من الإثباتِ التقليدي، وتفسّرُ جانبًا من تعسّرِ التعقّب عبر الحدود وكلفةِ الفحصِ المختبري[٤].

ثانيًا: المُستجدّاتُ مثلُ العملاتِ الرّقميّة والذّكاءِ الاصطناعي

تُحدثُ الأصولُ المشفّرةُ ووساطاتُها (VASPs) أسئلةً مُركّبةً في التكييفِ الشرعي والامتثالِ القانونيّ؛ وقد تحرّكت المعاييرُ الدوليّة لتطويقِ مخاطر غسل الأموال وتمويل الإرهاب عبر "تحديثاتٍ موجّهة" من مجموعة العمل المالي (FATF) وتوسيعِ نطاق "قاعدة السفر" وتتبّعِ التحويلاتِ ذات الصلة. وفي المقابل شيّد الاتحادُ الأوروبي إطارَ MiCA المنظّم لأسواقِ الأصول المشفّرة وضوابطَ مُصدري العملاتِ المستقرّة ومقدّمي الخدمات، بما يعالجُ فجواتِ الشفافية وحمايةَ المستهلك. أمّا الذكاءُ الاصطناعيّ، فمع انفجارِ تطبيقاته (ومنها التوليديّة) تزايدت الحاجةُ إلى أُطرِ إدارةِ مخاطرٍ مؤسسيةٍ ومعاييرَ حَوْكمة—مثل "إطار إدارة مخاطر الذكاء الاصطناعي" لدى NIST ومعيار ISO/IEC ٤٢٠٠١ لأنظمة إدارة الذكاء الاصطناعي—بما ينعكسُ مباشرةً على تقديرِ المسؤولية وحجّيةِ المخرجات التقنيّة.

ثالثًا: تعقيدُ تحديدِ المسؤوليةِ الجنائيّة

تُربكُ البيئةُ الرقميّةُ قواعدَ الإسناد (Attribution) وتوزيعَ المسؤوليات؛ فالتلاعبُ بالهُويّات، والبُنى الموزّعة، والتشغيلُ عبر سلسلة مزوّدين، تُضعفُ ربطَ الفعلِ بفاعلٍ محدّد وتفتحُ أبوابَ التنازع على الاختصاصِ القضائيّ. ويُبرز "تالين ٢.٠" (Tallinn Manual ٢.٠) تعقيداتِ الإسناد والمسؤوليّة في سياق القانون الدوليّ—وإن كان موجّهًا أساسًا إلى سلوكِ الدُّول—إلا أنّ منهجيّةَ تفكيكِ عناصرِ السلوكِ الرّقميّ والولايةِ والنتيجة تُفيدُ في البناءِ الجنائيّ الداخليّ، لاسيّما مع ازديادِ الوقائعِ التي تقعُ دون عتبةِ "القوة" وتستلزمُ أدلّةً تقنيّةً دقيقة.[٥]

---

[١] https://www.justice.gov/

[٢] هو تطبيق يوفر تحديثات يومية وأبحاثًا معمقة من منظمة حقوق الإنسان الرائدة عالميًا، ويحتوي على محتوى متنوع يشمل المدونات وتقارير البحث ومقاطع الفيديو والرسومات، مع ميزات تسمح للمستخدم بتخصيص صفحته الرئيسية، كما أن التطبيق لا يجمع أي بيانات من المستخدمين أو يشاركها وفقًا لمطور التطبيق .

[٣] https://gp-digital.org/

[٤] https://amnafzar.net/

[٥] https://www.google.com/search?q=Cambridge+University+Press+&oq=Cambridge٩٨٥IQ٩٨٥GCEJ_enIQ١C١+Assessment&rlz=٢٦%+Assessment&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzMzOGowajSoAgCwAgA&sourceid=chrome&ie٢٦%+University+Press+٨=UTF-

رابعًا: ضعفُ الوعيِ الشرعيّ والقانوني لدى الأفراد

يظلُّ الوعيُ العامُّ—بحدودِ الخصوصيّة والرضا والبياناتِ الحسّاسة ومخاطرِ النّشر—أدنى من المطلوب، ما يُفاقمُ التعرضَ للابتزاز والاحتيال ويُضعفُ مناعةَ المجتمع الرّقمي. وتؤكد تقاريرُ ENISA أنّ رفعَ الوعي عنصرٌ أساسٌ في الاستراتيجيّات الوطنيّة للأمنِ السيبرانيّ، مع التوصية بمناهجَ تدريبيّةٍ مُوجّهةٍ وشراكاتٍ مجتمعيّةٍ مستدامة، وهو ما يوازيه—في البيئات العربية—حاجةٌ إلى محتوىً تثقيفيٍّ يدمجُ أحكامَ الشريعةِ في السلوكِ الرقميّ الرشيد.

خامسًا: الحاجةُ لتأصيلٍ فقهيٍّ حديثٍ يُواكبُ التقنية

يستدعي تغيّرُ الوسائط والأعيانِ الاعتباريّة تفعيلَ أدواتِ الاجتهاد: تحقيقُ المناط في "الأموالِ والمنافع الرّقميّة"، اعتبارُ المصالحِ المرسلة بضوابطها، توسيعُ مفهوم الحِرز إلى الحِرزِ الاعتباريّ، وترتيبُ الضماناتِ على الإتلافِ غيرِ المادّي. وتظهرُ وثائقُ "المجمع الفقهي الإسلامي الدولي" مرجعيّةً تأصيليّةً مُعِينة—مع تحديثٍ متواصل لمدوّنة القرارات—في مسائل حمايةِ الحقوقِ المعنويّة والتعامُل الإلكترونيّ والعملاتِ الرقميّة، بما يُتيحُ جسورًا عمليّةً بين التأصيلِ والواقعِ التنظيميّ. IIFA

سادسًا: مقترحاتٌ فقهيّةٌ وتشريعيّةٌ لمعالجةِ الإشكالات

يمكنُ حصرُ مساراتٍ عمليّةٍ جامعة: (١) سنُّ قواعدِ إثباتٍ رقميٍّ وطنيةٍ تُحيلُ إلى معاييرَ دوليّة (ISO/IEC ٢٧٠٣٧ وما في حكمِها) وتُقرّ مبادئَ سلامةِ السلسلة والتوثيق الذاتي لبعض المخرجات؛ (٢) مواءمةُ تشريعاتِ الأصول المشفَّرة مع معايير FATF وMiCA، وربطُ الامتثالِ الماليّ بآلياتِ التحقّقِ الشرعيّ في أبوابِ الربا والغرر والمقامرة؛ (٣) اعتمادُ أطرِ حوكمةِ الذكاء الاصطناعي المؤسّسية (NIST AI RMF، ISO/IEC ٤٢٠٠١) ضمن سياسةٍ شرعيّةٍ تُحقّقُ مقاصدَ الحفظ وتُقلّلُ المفاسد؛ (٤) ترسيخُ برامجِ وعيٍ رقميٍّ شرعيٍّ مستمرّةٍ على مستوى التعليمِ العامّ والمهني؛ (٥) إنشاءُ وحداتِ خبرةٍ قضائيّةٍ رقميّةٍ متخصّصة؛ (٦) تطويرُ اتفاقاتِ تعاونٍ ثنائيّةٍ وإقليميّةٍ عاجلةٍ لتبادلِ الأدلّةِ مع ضماناتِ الخصوصيّة. بهذه الرُّزم يُؤمَنُ التكييفُ الشرعيّ وتتماسكُ أدواتُ الردع والإثبات.

٤. الخاتمة

يخلص هذا البحث—«الجرائم الإلكترونية وأحكامها في الفقه الإسلامي: دراسة مقارنة»—إلى أن الظاهرة الإجرامية الرقمية لا تُفهم بوصفها مجرد امتدادٍ تقني للجريمة التقليدية، بل باعتبارها مجالًا ذا خصائصٍ ومناطاتٍ جديدةٍ تستدعي تأصيلًا فقهيًا منضبطًا ومقاربةً تشريعيةً مرنة. وقد عالجت المباحث تعريفات الجريمة الإلكترونية وحدودها، وأقامت أسس التجريم على المقاصد والقواعد الكلية، وكيّفت أشهر صورها فقهًا، ثم قارنت أحكامها بمخرجات القانون الوضعي وآلياته الإجرائية والإثباتية، قبل أن تستعرض التحديات العملية وسبل معالجتها. وتبيّن أن باب التعزير هو الغالب في الجرائم الرقمية مع بقاء إمكان إعمال بعض الحدود بشروطها، وأن الاعتراف بالقيمة المالية للبيانات والحقوق المعنوية ركنٌ لازم لضبط الضمان والعقوبة. كما ظهر أن مواءمة أدوات القانون الوضعي—خاصة قواعد الإثبات والتعاون العابر للحدود—ممكنةٌ متى روعيت المقاصد والضمانات الإجرائية. وانتهى البحث إلى توصيةٍ بمدوّنة وطنية للأدلة الرقمية، وسياسات «الأمن/الخصوصية بالتصميم»، وبرامج توعيةٍ مستمرة، ومراجعةٍ تشريعيةٍ دورية تراعي تحولات الذكاء الاصطناعي والأصول المشفرة؛ بما يحقق مقصد الشريعة في صيانة الضروريات وإقامة العدل في الفضاء الرقمي.

أولًا: النتائج:

١. توصّل البحث إلى تعريفٍ تشغيليّ للجريمة الإلكترونية يضبط محلّ الحكم: «كلُّ فعلٍ أو امتناعٍ مُجرَّمٍ شرعًا أو قانونًا يقع بواسطة منظوماتٍ رقمية أو يَرِدُ على محلٍّ رقمي (بيانات/أنظمة/هويات) ويؤول إلى الاعتداء على حقّ معتبر أو مصلحةٍ عامةٍ راجحة». وقد ثبت أن الاعتراف بالأموال والحقوق المعنوية (البيانات، البرمجيات، الأسرار التجارية) ضروريّ لحماية المصالح وقياس الضمان.

٢. ترتكز الشرعيةُ الكلية للتجريم في البيئة الرقمية على مقاصد حفظ الضروريات الخمس، وتتفرع عنها قواعد «لا ضرر ولا ضرار»، و«سدّ الذرائع»، و«حفظ الحقوق»، و«المصالح المرسلة»، بما يوفّر إطارًا مرنًا يوازن بين الوقاية والردع والعدالة الإجرائية، ويُجيز لوليّ الأمر سنَّ تدابيرٍ تنظيمية وتعزيريةٍ تواكب المستجدات.

٣. في التكييف الفقهي: يُلحق الاحتيال الإلكتروني—إن استوفى شروط الحِرز والنقل الخفي والنصاب—بأحكام السرقة حدًّا، وإلا فتعزيرٌ مُغلّظ مع الضمان؛ ويُجرى حدّ القذف على الاتهامات الرقمية الصريحة بالموجب، وتُعزر صور السبّ والبهتان؛ ويُعدّ التجسّسُ الرقمي واختراقُ الخصوصية محرّمين تعزيرًا مع ضمان الضرر؛ ويُكيّف اختراقُ الأنظمة وإتلافُ البيانات أو حبسُها (كالفدية) غصبًا واعتداءً موجبًا للضمان؛ أمّا نشرُ الشائعات المفضية إلى الفتنة فيُغلّظ تعزيرُه بقدر اتّساع أثره ومآلاته.

٤. الحدود الشرعية قابلةٌ للانطباق على بعض الوقائع الرقمية بشروطها وضوابطها، غير أن الغالب في الجرائم الإلكترونية هو بابُ التعزير لاتساع صوره وتنوّع وسائطه، وهو ما يفتح مجالًا واسعًا لملاءمة العقوبة مع طبيعة الفعل وضرره.

٥. أظهرت المقارنة مع القانون الوضعي نقاطَ التقاءٍ واسعة في حماية الأموال والعِرض والنظام العام، وفي إقرار قواعدٍ خاصة للإثبات الرقمي والتعاون العابر للحدود. كما كشفت عن فجواتٍ تشريعيةٍ في بعض البيئات—خاصةً في ضبط التعريفات ومنع العموميات المُجرِّمة للمحتوى—وتفاوتٍ في آليات الإثبات وحجّية السجلات الرقمية وسلسلة الحيازة.

٦. أبرز التحديات التطبيقية: حساسية الإثبات الرقمي ومتطلبات سلامته، وصعوبة الإسناد وتحديد المسؤولية في البيئات الموزّعة وعبر الحدود، والتطور السريع في العملات المشفرة والذكاء الاصطناعي وما يستتبعه من أسئلةٍ في الضمان والمسؤولية، وضعف الوعي الشرعي والقانوني لدى الجمهور والفاعلين التقنيين.

ثانيًا: التوصيات العملية

١. تشريعٌ مُحكم: سنّ نصوصٍ واضحة تُعرّف الجريمة الإلكترونية تعريفًا دقيقًا وتتجنب العبارات الفضفاضة، مع إيراد «حِرزٍ اعتباري» ومعاييرَ تقنيةٍ تُوازي الحِرز المادي، وتجريمٍ صريح للاعتداء على البيانات والأنظمة والهوية الرقمية، وربط الجزاءات بضررٍ مُتحقق ومآلاتٍ معتبرة.

٢. تقنينُ الإثبات الرقمي: اعتماد مدونة وطنية لأساليب جمع الأدلة وحفظها وفحصها تُحيل إلى المعايير الدولية (سلسلة الحيازة، البصمات التجزئية، سجلاتُ التدقيق)، وتقرّ التوثيق الذاتي لبعض المخرجات الرقمية بشروطٍ فنيةٍ وقضائية، مع إنشاء مختبراتٍ رقميةٍ قضائية معتمدة.

٣. تعزيرٌ مُغاير للوسيط: تفعيل بدائلَ عقابيةٍ متدرجة (الغرامة المتناسبة، المنع المؤقّت من مزاولة النشاط الرقمي، تعليق التراخيص، برامج الإصلاح والتدريب الإلزامي، تدقيقٌ أمنيّ دوريّ) بما يحقق الردع ويُصلح السلوك، مع تغليظ العقوبة عند مساس الأفعال بالمرافق الحيوية أو السلامة العامة.

٤. مواءمةٌ مقاصديةٌ مع الأطر الوضعية: الإفادة من أدوات التعاون الدولي (نقاط اتصال ٧/٢٤، أوامر الحفظ والإنتاج عبر الحدود) مع تضمين ضمانات الخصوصية والإجرائية العادلة، ومواءمة تنظيمات الأصول المشفرة والذكاء الاصطناعي مع مقاصد الشريعة في منع الضرر والغرر والربا والمقامرة.

٥. بناءُ قدراتٍ مؤسسية: إنشاء وحداتٍ متخصصة بالادعاء والقضاء للتحقيقات الرقمية، وتأهيل القضاة وأعضاء الضبط القضائي تدريبًا مستمرًا على التقنيات الحديثة، ووضع أدلةٍ عمليةٍ معيارية للاشتغال الرقمي على مستوى الجهات الحكومية والقطاع الخاص.

٦. حوكمةُ المنصّات وسياسات «الخصوصية/الأمن بالتصميم»: إلزام مزوّدي الخدمة بمعايير أمنٍ معلوماتي وواجهاتٍ تُقلل جمع البيانات وتحدّ من إساءة الاستخدام، واشتراط الإفصاح المسؤول عن الحوادث والالتزام بمهلٍ للحفظ والإبلاغ، وتضمين عقود الاستخدام بنودًا واضحة للحقوق والضمانات.

٧. تمكينٌ مجتمعي وتوعية: إطلاق برامج تثقيفيةٍ مستمرةٍ تُدمج فيها مفاهيم السلوك الرقمي الرشيد والأحكام الشرعية ذات الصلة، واستهداف الفئات الأكثر عُرضة (الناشئة، أصحاب الأعمال الصغيرة، موظفو الجهات الحساسة) بمحتوى عمليّ قابل للتطبيق.

٨. مراجعةٌ دورية قائمة على تقييم الأثر: إنشاء آلية وطنية لمراجعة التشريعات واللوائح الرقمية كل سنتين على الأقل، تقيس التناسب والفعالية والأثر الحقوقي، وتُحدّث النصوص وفق المستجدات التقنية والتجارب القضائية.

إنَّ الجمع بين التأصيل المقاصدي والقواعدي وبين أدوات القانون الوضعي والإثبات الرقمي يفتحُ طريقًا عمليًا لبناء سياسةٍ جنائيةٍ رقميةٍ عادلة ونافذة. فالمنظور الشرعي يُزوّدُ صانع القرار بمعاييرَ واضحة لضرورات الحفظ ومنع الضرر وتحقيق العدل، فيما تمنحُ المنظوماتُ الوضعيةُ آلياتِ التنفيذ العابرة للحدود ومعاييرَ الإثبات والحوكمة. ولئن كان الوسيطُ الرقمي سريعَ التحول، فإنّ اعتماد قواعد عامةٍ محكمةٍ وآلياتِ مراجعةٍ دوريةٍ وتعاونٍ مؤسسيٍّ رصين، كفيلٌ بأن يحفظ الحقوق ويُعلي مناعَة المجتمع، ويقود إلى منظومة جزائيةٍ معاصرة تُحقّق مقصد الشريعة في صيانة الضروريات وإقامة العدل.

١. يُعدّ الشرط الجزائي من الوسائل الحديثة التي تهدف إلى حفظ الالتزامات التعاقدية، وقد نال قبولًا في الفقه الإسلامي ضمن أطر وضوابط معينة.

٢. الغاية الرئيسة من الشرط الجزائي هي حماية مصالح المتعاقدين وردع الإخلال، مع ضمان تعويض الطرف المتضرر.

٣. المجامع الفقهية المعاصرة أجمعت في معظمها على جواز الشرط الجزائي، بشرط ألا يُفرض على الالتزامات المالية النقدية.

٤. الفقه الإسلامي يشترط تناسب مبلغ الشرط مع حجم الضرر، بما يحقق قاعدة: "الجزاء من جنس العمل" ويمنع التعسف في استعمال الحق.

٥. التطبيق القضائي في العالم الإسلامي يميل إلى مراعاة الضوابط الفقهية، ويُخضع تقدير الشرط الجزائي للسلطة القضائية بما يحقق العدالة.

.

Conflicts Of Interest

The author declares no conflict of interest in relation to the research presented in the paper.

Funding

No grant or sponsorship is mentioned in the paper, suggesting that the author received no financial assistance.

Acknowledgment

The author extends gratitude to the institution for fostering a collaborative atmosphere that enhanced the quality of this research.

References

[1] Ibn Manzur, Muhammad ibn Mukarram, Lisan al-'Arab, Beirut: Dar Sadir, 3rd ed., 1414 AH. Link
[2] Ibn Qudamah, Abdullah ibn Ahmad, Al-Mughni, Riyadh: Dar 'Alam al-Kutub, 3rd ed., 1997. Link
[3] Al-Sarakhsi, Muhammad ibn Ahmad, Al-Mabsut, Beirut: Dar al-Ma'rifah, 1st ed., 1406 AH. Link
[4] Al-Kasani, 'Ala' al-Din, Bada'i' al-Sana'i' fi Tartib al-Shara'i', Beirut: Dar al-Kutub al-'Ilmiyyah, 2nd ed., 1986. Link
[5] Al-Qurtubi, Muhammad ibn Ahmad, Al-Jami' li Ahkam al-Qur'an, Beirut: Dar al-Kutub al-'Ilmiyyah, 1st ed., 2003.Link
[6] Ibn Kathir, Isma'il ibn 'Umar, Tafsir al-Qur'an al-'Azim, Beirut: Dar al-Ma'rifah, 2nd ed., 1407 AH/1987. Link
[7] Al-Tabari, Muhammad ibn Jarir, Jami' al-Bayan 'an Ta'wil Ay al-Qur'an, Cairo: Dar Hajar, 2001. Link
[8] Al-Shatibi, Ibrahim ibn Musa, Al-Muwafaqat fi Usul al-Shari'ah, Al-Khobar: Dar Ibn 'Affan, 1417 AH/1997. Link
[9] Al-Zuhayli, Wahbah, Al-Fiqh al-Islami wa Adillatuh, Damascus: Dar al-Fikr, 1997. Link
[10] Abu Zahrah, Muhammad, Al-Jarimah wa al-'Uqubah fi al-Fiqh al-Islami, Cairo: Dar al-Fikr al-'Arabi, 1955. Link
[11] 'Awdah, 'Abd al-Qadir, Al-Tashri' al-Jina'i al-Islami Muqaranan bi al-Qanun al-Wad'i, Beirut: Mu'assasat al-Risalah, 2013. Link
[12] International Islamic Fiqh Academy, Resolutions and Recommendations of the Academy, Jeddah: The Academy, 2006. Link
[13] Arabic Language Academy, Al-Mu'jam al-Wasit, Cairo, 1972. Link
[14] Saudi Anti-Cyber Crime Law, 2007. Link
[15] UAE Cybercrime Law, 2021. Link
[16] Council of Europe, Convention on Cybercrime (Budapest Convention), 2001. Link
[17] League of Arab States, Arab Convention on Combating Information Technology Offences, 2010. Link
[18] UNODC, Comprehensive Study on Cybercrime, 2013. Link
[19] Yar, Majid & Steinmetz, Kevin F., Cybercrime and Society, 2019.
[20] Holt, Thomas J. & Bossler, Adam M., Cybercrime in Progress, 2016. Link
[21] African Union, African Union Convention on Cyber Security, 2014. Link
[22] ARTICLE 19, Analysis of the UN Cybercrime Convention, 2024.
[23] European Union, Regulation (EU) 2023/1543, 2023. Link
[24] European Union, Regulation (EU) 2024/1183, 2024. Link
[25] ISO/IEC 27037:2012, Digital Evidence Guidelines, 2012. Link
[26] NIST, Artificial Intelligence Risk Management Framework, 2023. Link
[27] FATF, Virtual Assets Update, 2023. Link