Wisdom Journal For Studies And Research Volume 06 Issue 05/ 31-08-2026
ISSN print/ 2769-1926 ISSN online/ 2769-1934

Digital Social Transformations and Their Impact on Cybercrime

Dr. Mohammad Hussein Hussein Abu Zneid
Al-Istiqlal University – Jericho, Palestine
Mohammad.znaid@pass.ps

Received:14/07/2026 Accepted : 18/08/2026

Abstract:

This paper examines a fundamental issue arising from the accelerating transformations experienced by contemporary societies: the impact of digital social transformations on the evolution of cybercrime, and the adequacy of criminal legislation in confronting it. The study proceeds from the hypothesis that the rapid evolution of digital society has produced new patterns of criminal behavior that traditional legal rules are unable to adequately absorb. Relying on the descriptive-analytical method and the comparative method, the researcher examines selected models drawn from relevant Arab and Western legislation, tracing points of similarity and difference in mechanisms of criminalization and judicial prosecution, and paying particular attention to the legislative void that still characterizes the Palestinian legal system in this field. The paper is organized around three main axes: the conceptual framework of digital social transformations and the characteristics of digital society; the impact of these transformations on the emergence and evolution of cybercrime, including newly emerging forms such as deepfake crimes, advanced ransomware, and crypto fraud; and the legislative response at the international, Western, Arab, and Palestinian levels, together with the fundamental technical and legal challenges facing criminal justice systems. The research concludes with a number of findings, most notably that digital transformations have contributed to shaping an unprecedented criminal environment characterized by cross-border reach and difficulty of criminal attribution, and that many criminal laws still lack adequate mechanisms for confronting newly emerging forms of cybercrime. The study further finds that international cooperation is an essential condition for the effectiveness of the criminal response, and that a preventive strategy grounded in digital awareness and education is no less important than the legislative and judicial response. The paper closes with a set of legislative, institutional,

international, and preventive recommendations, with particular emphasis on the urgent need for Palestine to enact dedicated cybercrime legislation.
Keywords: Cybercrime; Digital Transformation; Social Variables; Criminal Legislation; Digital Criminal Protection.

التحولات الاجتماعية الرقمية وأثرها على الجريمة الإلكترونية

د. محمد حسين حسين (أبو زنيد)
جامعة الاستقلال – أريحا، فلسطين
Mohammad.znaid@pass.ps

ملخص:

يتناول هذا البحث إشكالية جوهرية في ظل المتغيرات المتسارعة التي تشهدها المجتمعات المعاصرة، وهي: أثر التحولات الاجتماعية الرقمية على تطور الجريمة الإلكترونية ومدى كفاية التشريعات الجنائية في مواجهتها. وتنطلق الدراسة من فرضية مفادها أن التطور المتسارع للمجتمع الرقمي قد أفرز أنماطاً جديدة من السلوك الإجرامي تعجز القواعد القانونية التقليدية عن استيعابها بصورة كافية. وقد اعتمد الباحث على المنهج الوصفي التحليلي والمنهج المقارن، عبر دراسة نماذج مختارة من التشريعات العربية والغربية ذات الصلة، مع إيلاء عناية خاصة للفراغ التشريعي الذي لا يزال يسم المنظومة القانونية الفلسطينية في هذا المجال. ويتوزع البحث على ثلاثة محاور رئيسية: الإطار المفاهيمي للتحولات الاجتماعية الرقمية وخصائص المجتمع الرقمي؛ وأثر هذه التحولات على نشأة الجريمة الإلكترونية وتطورها، بما في ذلك الأشكال المستحدثة كجرائم التزييف العميق وبرمجيات الفدية المتطورة واحتيال العملات الرقمية؛ والاستجابة التشريعية على المستويات الدولية والغربية والعربية والفلسطينية، إلى جانب التحديات التقنية والقانونية الجوهرية التي تواجه أجهزة العدالة الجنائية. وقد خلص البحث إلى جملة من النتائج، أبرزها: أن التحولات الرقمية أسهمت في تشكيل بيئة إجرامية غير مسبوقة تتسم بالعابرية الحدودية وصعوبة الإسناد الجنائي، وأن كثيراً من التشريعات الجنائية لا تزال تفتقر إلى الآليات الكافية لمواجهة الأشكال المستحدثة من الجريمة الإلكترونية. كما توصّل البحث إلى أن التعاون الدولي يُعدّ شرطاً جوهرياً لفاعلية الاستجابة الجنائية، وأن الاستراتيجية الوقائية القائمة على التوعية والتعليم الرقمي لا تقلّ أهمية عن الاستجابة التشريعية والقضائية. ويختتم البحث بجملة من التوصيات التشريعية والمؤسسية والدولية والوقائية، مع التشديد بوجه خاص على الحاجة الملحّة لإقرار فلسطين تشريعاً خاصاً بالجرائم الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية، التحول الرقمي، المتغيرات الاجتماعية، التشريعات الجنائية، الحماية الجنائية الرقمية.

Wisdom Journal For Studies And Research Volume 06 Issue 05/ 31-08-2026
ISSN print/ 2769-1926 ISSN online/ 2769-1934

The Research

Introduction

The world today is living through a genuine digital revolution that has reshaped the nature of social, economic, and cultural relationships, giving rise to what has come to be known as the "digital society," in which real and virtual life are increasingly intertwined. Since the spread of the internet in the 1990s, through the smartphone revolution of the first decade of the third millennium, to the current era of artificial intelligence and the Internet of Things, successive waves of digital transformation have continued and deepened, redrawing the map of human and institutional interaction on an unprecedented scale.

Yet this radical transformation has not been free of risks, as it has been accompanied by the emergence of new and evolving forms of crime known as electronic or cyber crimes. These crimes possess characteristics that fundamentally distinguish them from traditional crime, most notably: cross-border reach, extreme speed of execution, and difficulty of tracing and criminal attribution, in addition to the intangible nature of the perpetrator, the victim, and the instrument of the crime all at once. The criminal legislative system has found itself facing an unprecedented challenge, since classical legal rules were formulated in a physical context entirely different from the current digital environment.

This paper studies the dialectical relationship between digital social transformations and the evolution of cybercrime, by analyzing the concept of these transformations and their criminal effects, assessing the extent to which criminal legislation has absorbed the requirements of effective confrontation, and envisioning prospects for developing digital criminal policy. The research problem centers on the following question: what is the impact of digital social transformations on the evolution of cybercrime, and to what extent is criminal legislation adequate to confront it? The study proceeds from the hypotheses that (1) the deeper digital social transformations become, the more cybercrime develops in quantity and quality; (2) criminal legislation in most Arab states does not adequately keep pace with this development; (3) the absence of effective international cooperation weakens the criminal response to cross-border cybercrime; and (4) a preventive strategy based on digital awareness and education is no less important than the legislative response. The researcher relies on the descriptive-analytical method, through the analysis of relevant concepts

and legal texts, and the comparative method, through the study of Arab legislation (Jordanian, Emirati, Saudi, Egyptian, and Palestinian) alongside Western legislation (American and European), reinforced by a method of legal critique aimed at uncovering gaps and proposing reform.

I. The Conceptual Framework of Digital Social Transformations

Subtitle 1: The Concept and Dimensions of Digital Social Transformations

Digital social transformations refer to the totality of structural and functional changes that occur in society as a result of the adoption of digital technologies across various fields of human life, encompassing transformations in patterns of social interaction, economic structures, political institutions, and cultural values (Castells, 2010). These transformations are not confined to the use of new technical tools; they extend to restructuring social relations and shaping new identities and behavioral patterns. Digital transformation differs from mere technical modernization: modernization uses technology to perform existing tasks more efficiently, whereas digital transformation radically rethinks the very nature of these tasks on the basis of a different digital logic.

The Author Argues: Digital social transformations cannot be properly understood except as a comprehensive civilizational transformation rather than a mere technical change — which is what makes studying them within criminal law a scientific necessity, since cybercrime cannot be understood without grasping the socio-digital environment that produced it.

Three main technical axes have driven and accelerated these transformations: the internet, which connected societies in a shared digital space; social media platforms, which revolutionized patterns of expression and interaction and produced "digital identity"; and big-data and artificial-intelligence technologies, which added an unprecedented analytical and predictive capacity. More recently, the Internet of Things (IoT) and blockchain technology — the foundation of cryptocurrencies — have deepened this transformation further, each generating accompanying social change and new criminal opportunity at once.

On the quantitative level, the International Telecommunication Union (ITU, 2023) reports that the number of internet users worldwide has exceeded five billion — about 66% of the global population — with the fifth billion added in only a few years after the first billion took seventeen years, signaling a tremendous acceleration. Qualitatively, social media platforms have become a new model of friendship, social influence, and collective identity, while the digital economy has reshaped labor markets, displacing traditional jobs even as it creates new ones, generating significant social tension.

Subtitle 2: The Digital Society and Its Characteristics

Digital society is defined as a society that relies fundamentally on digital technologies to organize its economic, social, political, and cultural relations, treating cyberspace as a space parallel to — not a substitute for — material life (van Dijk, 2020). It is characterized by network interconnectedness across time and place, extreme speed of information flow, multiple identity that allows individuals to adopt diverse personas online, and the democratization of access to information, accompanied by risks of misuse and misinformation.

Despite the wide spread of digital technologies, the world still suffers from a digital divide — disparity in access to and use of digital technology, between states and within societies — which deepens existing inequalities and widens the vulnerability of particular groups to digital risk. The Global Internet Governance Report (2022) notes that this divide extends beyond infrastructure to a gap in digital knowledge and risk awareness, making technologically disadvantaged communities more vulnerable to digital threats; the untrained, security-unaware user is an easy target for cybercriminals.

The Author Argues: The digital divide is not merely a developmental-economic problem but a criminal problem in its own right: technologically disadvantaged societies become exposed to criminal exploitation while remaining unable to employ digital tools to counter cybercrime — making the closing of the digital divide a policy objective with explicit criminal dimensions.

II. The Impact of Digital Transformations on Cybercrime

Subtitle 1: The Concept, Characteristics, and Classification of Cybercrime

Cybercrime can be comprehensively defined as any act or omission criminalized by law, committed by a person with criminal intent, making use of a computer, an electronic network, or other digital technology, whether that means constitutes the instrument of the crime, its subject matter, or both (Najm, 2014). While some jurists prefer the term “computer crime,” the prevailing trend favors “cybercrime” as more comprehensive in describing the diverse crimes of cyberspace (Wall, 2007).

Cybercrime is distinguished from traditional crime by several characteristics: cross-border reach, which complicates jurisdiction and undermines the principle of territoriality; intangibility, which makes proof and damage assessment more difficult; extreme speed, allowing a single piece of malicious software to infect millions of devices within moments; difficulty of proof, since digital evidence can be easily altered and requires specialized expertise to collect and verify; and continuous evolution that outpaces legislative capacity to keep up.

Cybercrimes can be classified by subject matter into four categories: crimes against systems and data (illegal intrusion, sabotage, denial-of-service attacks, ransomware); digital economic crimes (electronic fraud, digital money laundering via cryptocurrencies, infringement of intellectual property, market manipulation); crimes against persons committed digitally (extortion, harassment, cyberbullying, invasion of privacy, non-consensual distribution of intimate content); and digital national-security crimes (attacks on critical infrastructure, digital espionage, online recruitment of extremists, dissemination of terrorist content).

Subtitle 2: Quantitative and Qualitative Development, and Social Drivers

Digital transformations have driven an almost continuous expansion in cybercrime. The American Internet Crime Complaint Center (IC3, 2023) reports losses from cybercrime in the United States alone exceeding ten billion dollars in 2022, in an uninterrupted rise over two decades, while Cybersecurity Ventures (2023) estimates global economic costs at more than eight trillion dollars annually. This increase is driven by the growing number of internet users, the accumulation of digital wealth, the spread of e-commerce and digital banking, and — since the COVID-19 pandemic of 2020–2021 — the sudden acceleration of digital transformation that created security vulnerabilities exploited by cybercriminals.

The Author Argues: The quantitative growth of cybercrime exceeds, in scale and pace, any other criminal phenomenon in human history — evidence not merely of the spread of technology but of the criminal justice system's failure to achieve adequate deterrence, demanding urgent legislative, judicial, and institutional response.

Beyond quantitative growth, artificial intelligence and machine learning have produced a new generation of "smart crimes": deepfake crimes, which use AI to forge audio and video content for disinformation, extortion, and defamation, and are now accessible through free online tools; advanced ransomware, which has evolved from encrypting individual data to targeting hospitals and critical infrastructure, at times directly threatening human life; and crypto fraud, exploiting weak legal regulation of cryptocurrencies in most countries. Social media platforms have further given rise to crimes of the digital social space — harassment, cyberbullying, invasion of privacy, non-consensual distribution of intimate content, digital hate speech, online recruitment of extremists, and fake news — which frequently leave severe psychological effects on victims given the difficulty of erasing digital traces.

The Author Argues: Confronting social-media crimes requires a dual approach: a legislative approach that criminalizes these acts through clear, precise provisions that do not infringe legitimate freedom of expression, and an institutional approach holding social media companies to broader responsibility for harmful content — since the near-absolute immunity these companies enjoy leaves the effectiveness of combating such crimes incomplete.

Social variables also drive cybercrime: studies link social and economic exclusion to a greater likelihood of sliding into cybercrime, particularly among unemployed youth who find in digital space an outlet or a source of rapid income. The weakening of traditional social bonds and the declining role of family and community institutions have further created an environment conducive to digital criminal behavior — reinforced by anonymity online, which weakens the social-moral deterrent. This is captured in psychologist John Suler's concept of the "online disinhibition effect" (Suler, 2004), describing the tendency of individuals to behave less restrainedly online than in material reality, partly explaining elevated rates of hate speech, harassment, and fraud.

The Author Argues: Anonymity online is a dual-edged challenge: it facilitates crime while obstructing the pursuit of the criminal. The solution is not the abolition of digital privacy — which would violate fundamental rights — but balanced legal and technical mechanisms that lift immunity from criminals while preserving the privacy of law-abiding users.

II. Results and Discussion: The Legislative Response and Prospects for Digital Criminal Policy

International and National Legislation

The Council of Europe's Convention on Cybercrime (the Budapest Convention, 2001) remains the most prominent international instrument, having laid down an integrated framework for criminalization and international cooperation, acceded to by more than 66 states. It distinguishes four categories of offenses — against confidentiality, integrity, and availability of data; computer-related offenses such as forgery and fraud; content-related offenses such as child pornography; and intellectual-property offenses — and establishes rules for judicial cooperation and evidence exchange.

The Author Argues: The Budapest Convention, despite its importance, remains deficient in confronting the current reality; drafted more than two decades ago, it does not accommodate newly emerging forms such as AI attacks, deepfake crimes, and cryptocurrency fraud. The anticipated United Nations instrument on cybercrime should address these gaps and provide a framework more attuned to current developments.

At the American level, the Computer Fraud and Abuse Act (CFAA) of 1986 remains the primary legislative pillar, though criticized for broad, ambiguous provisions that have at times been used excessively against security researchers. The European Union has adopted an integrated system comprising the General Data Protection Regulation (GDPR, 2018), the NIS2 Directive on network and information security, and the EU Artificial Intelligence Act (ratified 2024), the first comprehensive global AI legislation.

Arab states have shown tangible legislative movement: Saudi Arabia's Anti-Cyber Crime Law (2007), the UAE's Cybercrime Law No. 5 of 2012, Jordan's Cybercrime Law of 2023, and Egypt's Anti-Cyber and Information Technology Crimes Law No. 175 of 2018. This legislation contains explicit criminalization of a wide range of cybercrimes and deterrent penalties, but was largely enacted reactively rather than as systematic anticipation of technical development, and frequently contains vague provisions raising concerns for freedom of expression.

The Author Argues: Arab cybercrime legislation suffers from three interlinked structural problems: a drafting problem (elastic provisions open to expansive interpretation), an updating problem (legislation lagging technical development), and a safeguards problem (deficient guarantees for the accused and fair-trial

rights in the digital context) — requiring comprehensive review that balances digital security with freedom of expression and privacy.

Palestine still lacks specialized, comprehensive cybercrime legislation; no Palestinian Cybercrime Law has been enacted despite drafts prepared over more than a decade, forcing the judiciary to rely on the amended Jordanian Penal Code No. 16 of 1960, formulated in an entirely different societal context. This gap leaves many harmful digital acts uncriminalized and pushes prosecutors to apply general criminal provisions to digital acts that do not precisely correspond to them, raising concerns under the principle of criminal legality.

The Author Argues: Palestine is in urgent need of dedicated cybercrime legislation addressing this legal void, drawing on comparative experience while accounting for Palestinian particularities, and giving special attention to digital criminal evidence — the gap most frequently encountered in cases before the courts. The delay in enacting this law harms victims of cybercrime and weakens public confidence in the criminal justice system.

Fundamental Challenges

Criminal justice agencies face fundamental technical challenges: technical development outpacing the capacity of security and judicial agencies; the difficulty of collecting and preserving digital evidence to strict legal standards; jurisdictional problems in cross-border crimes; and criminals' use of VPNs, encryption, and the Tor network to conceal identity. Related to this is the “going dark” dilemma, in which governments seek encryption backdoors to facilitate monitoring while security experts warn that any backdoor weakens digital security for everyone.

Legally and procedurally, digital evidence raises problems of credibility, integrity, and admissibility given the ease of tampering, and the necessity of establishing a reliable chain of custody. Jurisdiction in cross-border crimes raises the question of whether the state of the perpetrator, the victim, the harm, or the server should govern. On criminal liability, digital service providers and social media companies have persistently invoked the immunity of Section 230 of the U.S. Communications Act of 1996, a provision now subject to wide controversy given the severe harms of content spread on these platforms.

The Author Argues: The liability of digital platforms is among the most pressing legal issues of our time: it is unreasonable for the state alone to bear the burden of combating digital crimes committed through platforms that profit enormously from amplifying content without responsibility. The European

Digital Services Act (DSA), establishing graduated platform accountability, is a reform model worth adapting in Arab legislation.

Prospects for Development

Confronting cybercrime effectively requires: enacting or periodically updating specialized legislation with precise drafting that prevents arbitrary judicial expansion; developing rules of criminal evidence to accommodate digital evidence under an objective methodology; reviewing jurisdictional rules to align with cybercrime's cross-border nature; extending criminal liability to digital entities such as platforms and service providers; and establishing incentive-based measures such as Responsible Disclosure Programs that encourage security researchers to report vulnerabilities without exposure to prosecution.

International cooperation — intelligence, judicial, technical, and legislative — is indispensable given cybercrime's cross-border nature. The League of Arab States is well placed to lead the drafting of a unified Arab convention against cybercrime, building on the relative homogeneity of Arab legal systems and shared values.

A preventive strategy is equally essential: early digital education in schools, continuous specialized training for security and judicial personnel, and public-private cooperation on digital security. Finland's model — incorporating digital education from the primary level, establishing specialized investigation-training centers, and fostering close public-private cooperation — offers a case worth studying.

The Author Argues: Investment in digital awareness and education yields the highest return in confronting cybercrime, since the aware victim is the first line of defense before any legislation or security apparatus. In the Palestinian context specifically, a subject on “Digital Security and the Ethics of Cyberspace” should be incorporated into curricula at all educational stages, alongside community awareness programs targeting the groups most exposed to digital risk, such as women, children, and the elderly.

Conclusion

This study set out to examine the impact of digital social transformations on the evolution of cybercrime and the adequacy of criminal legislation in confronting it. It reached the following findings:

1. Digital social transformations have radically reshaped social structure, creating an open digital environment conducive to newly emerging forms of cybercrime characterized by cross-border reach and difficulty of criminal attribution, clearly confirming the first hypothesis.
2. Cybercrime has undergone rapid quantitative and qualitative development unparalleled in the history of the criminal phenomenon, now inflicting severe economic, security, and social losses.
3. A wide gap exists between the rapid technical development of cybercrime and the response of criminal legislative systems, particularly in Arab states, confirming the second hypothesis.
4. The absence of effective international coordination among criminal justice systems constitutes a strategic gap in confronting cross-border cybercrime, confirming the third hypothesis.
5. Social, psychological, and technical factors combine to drive and sustain cybercrime, making the criminal response alone insufficient absent a comprehensive preventive strategy, confirming the fourth hypothesis.
6. Palestinian legislation suffers from an acute legal void in the field of cybercrime, requiring urgent enactment of dedicated legislation balancing digital security with rights and freedoms.

On this basis, the study recommends: (1) at the legislative level, periodically reviewing and updating cybercrime legislation with precise drafting, and urging the Palestinian Authority to expedite a cybercrime law covering digital evidence, service-provider liability, and international cooperation; (2) at the institutional level, establishing specialized investigation units, continuous training, adequate budgets, and digital forensic laboratories meeting international standards; (3) at the international level, acceding to relevant conventions, expanding judicial cooperation, and working through the League of Arab States toward a unified Arab convention; (4) at the level of digital responsibility, developing a legal framework for platform and service-provider liability drawing on the EU's Digital Services Act; (5) at the preventive level, incorporating digital security and cyberspace ethics into curricula at all educational stages and developing sustained community awareness programs; and (6) at the research level,

supporting specialized scientific research and establishing research centers that supply legislators, judges, and practitioners with reliable, continuously updated data.

Bibliography List.

Books

1. Castells, M. (2010). The information age: Economy, society and culture: Vol. 1. The rise of the network society (2nd ed.). Wiley-Blackwell, United States.
2. Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press, United Kingdom.
3. Lusthaus, J. (2018). Industry of anonymity: Inside the business of cybercrime. Harvard University Press, United States.
4. van Dijk, J. (2020). The digital divide. Polity Press, United Kingdom.
5. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press, United Kingdom.
6. Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). SAGE Publications, United Kingdom.
7. Ibrahim, A. H. (2020). Cybercrime: A comparative study [in Arabic]. Dar Al-Nahda Al-Arabiya, Egypt.
8. Al-Halabi, M. A. (2018). Computer and internet crimes: Provisions of information-technology crime [in Arabic]. Dar Al-Thaqafa, Jordan.
9. Abdel Moaty, H. E. (2019). The law on combating information-technology crimes: An analytical study [in Arabic]. Dar Al-Jamea Al-Jadida, Egypt.
10. Awad, M. M. (2020). Criminal policy in confronting information-technology crime [in Arabic]. Dar Al-Nahda Al-Arabiya, Egypt.
11. Mustafa, M. F. (2022). Digital criminal evidence: Its rules and problems [in Arabic]. The Arab Center for Legal Studies.
12. Najm, M. S. (2014). Computer and internet crimes [in Arabic]. Dar Al-Thaqafa for Publishing and Distribution, Jordan.
13. Hilali, A. (2022). Cybercrime: Legal, social, and technical dimensions [in Arabic]. Al-Wafa Legal Library, Egypt.

Journal Articles

1. Al-Khater, N. M. (2019). Information-technology crimes and their impact on Arab criminal legislation [in Arabic]. Journal of Law and Political Science, 12(2), 45–78.
2. Al-Zoubi, S. (2021). Digital transformations and their impact on social structure: A sociological study [in Arabic]. Arab Journal of Social Sciences, 18(3), 112–140.
3. Al-Sayed, R. (2022). Criminal liability in cyberspace crimes: A comparative analytical study [in Arabic]. Journal of Law and Economics, 92(1), 1–55.
4. Al-Sharif, M. I. (2021). Artificial intelligence crimes: Problems of criminalization and liability [in Arabic]. University of Sharjah Journal for Legal Sciences, 18(2), 87–130.
5. Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, United States, 7(3), 321–326.

Internet Websites

1. Council of Europe. (2001). Convention on cybercrime (ETS No. 185). Budapest. https://www.coe.int
2. Cybersecurity Ventures. (2023). Cybercrime to cost the world $8 trillion annually in 2023. https://cybersecurityventures.com
3. Internet Crime Complaint Center (IC3). (2023). 2022 internet crime report. Federal Bureau of Investigation. https://www.ic3.gov
4. International Telecommunication Union (ITU). (2023). Measuring digital development: Facts and figures 2023. https://www.itu.int

Laws and Legislation

1. Jordanian Cybercrime Law No. (27) of 2023.
2. Jordanian Penal Code No. (16) of 1960, as amended.
3. Egyptian Law No. (175) of 2018 on Combating Information Technology Crimes.
4. Saudi Anti-Cyber Crime Law of 1428 AH / 2007 CE, as amended.
5. UAE Federal Law No. (5) of 2012 on Combating Information Technology Crimes, as amended.
6. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (1986, as amended), United States.
7. Directive (EU) 2022/2555 (NIS2 Directive).
8. Regulation (EU) 2016/679 (GDPR).
9. Regulation (EU) 2022/2065 (Digital Services Act – DSA).
10. Regulation (EU) 2024/1689 (EU AI Act).