LAW AND DIGITAL SECURITY: PROTECTING SMART SYSTEMS AND DATA IN THE MODERN ERA

A Comparative and Integrative Jurisprudential Analysis of Cybersecurity, Artificial Intelligence, and the Internet of Things

By Dr. Mohamed Kamal Arafa Elrakhawi
Researcher, Consultant, Expert, Jurist, Legal Author, and International Lecturer in Law

DOI: 10.5281/zenodo.21828059

Published 2026

Conflict of Interest Statement: The author declares no conflicts of interest. This work was produced without funding from any governmental, corporate, or ideological organization. The author has no financial interest in any assessment instrument, compliance framework, or commercial product discussed in this treatise.

Ethical Statement: All case material presented in this work has been de-identified in accordance with the ethical guidelines of the International Association for Privacy Professionals and the European Data Protection Board. Where legislative analysis draws upon consultative practice, all material has been anonymized.

Peer Review Note: This second revised edition incorporates the substantive recommendations of independent academic review, addressing methodological transparency, in-text citation integrity, operational Islamic jurisprudential frameworks, and the inclusion of previously absent thematic domains including military cybersecurity, autonomous artificial intelligence liability, post-quantum cryptography, electoral integrity, child protection in digital spaces, and compliance standardization.

DEDICATION

To the pure and luminous souls of my mother and my father, the wellspring of mercy and the eternal school of virtue, those who planted in me the seeds of knowledge and watered them with patience and sacrifice. I ask God, the Most High, to envelop them in His vast and everlasting mercy and to grant them the highest gardens of paradise.

This work is offered as a trust, a covenant, and a humble contribution to the treasury of human knowledge, placed between the hands of legislators, judges, and cybersecurity experts to organize this vital sector in a manner that preserves wealth, protects privacy, and achieves justice.

EXECUTIVE SUMMARY

The present reference constitutes a comprehensive scholarly investigation into the intersection of law, digital security, and emerging technologies, revised and expanded in response to rigorous academic critique. As the fourth industrial revolution accelerates, the proliferation of the Internet of Things, Artificial Intelligence, and ubiquitous smart surveillance systems has created a profound legal vacuum. This treatise advances the thesis that cybersecurity is no longer merely a technical discipline but a fundamental pillar of national security, economic stability, and the preservation of human dignity in the digital age.

Across thirty-six substantive chapters, organized into eight thematic parts, the work traces the evolution of cyber legislation from isolated national laws to complex international frameworks. It employs a transparent comparative legal methodology, analyzing the legislative architectures of Egypt, Algeria, and France with specific reference to article numbers, amendment dates, and judicial precedents, while integrating the overarching principles of European Union law and international treaties. A distinctive hallmark of this treatise is its operational integration of Islamic jurisprudential principles, specifically the Maqasid al-Shariah, which are translated from homiletic abstractions into measurable forensic and legislative variables through the Al-Khawajah Operational Framework for Digital Maqasid.

This revised edition addresses previously absent domains: military and defense cybersecurity, the criminal liability of autonomous artificial intelligence systems, post-quantum cryptographic transition, electoral integrity in the digital age, the protection of children in cyberspace, and the legal transformation of voluntary technical standards into mandatory compliance obligations. The reference further addresses the most pressing challenges of the modern era: the criminal and civil liability for data breaches, the legal status of encryption and steganography, the regulation of cryptocurrencies, the protection of critical infrastructure, and the ethical obligations of cybersecurity professionals.

This work is intended as a definitive reference for legal scholars, technology policymakers, forensic investigators, and judges navigating the complex realities of digital evidence and cybercrime adjudication.

INTRODUCTION AND EPISTEMOLOGICAL FOUNDATIONS

The contemporary era witnesses a massive reconfiguration of the concepts of security, privacy, and authority. The technological revolution has dissolved the traditional boundaries of the state, replacing physical borders with porous digital networks. Smart surveillance systems relying on the Internet of Things and Artificial Intelligence have become an inseparable part of the

foundational infrastructure of modern nations. However, this rapid technological advancement has consistently outpaced the legislative process, creating a dangerous legal vacuum that threatens both individual rights and national security (Clough, 2021, p. 47).

Understanding the law of digital security requires an epistemological shift. We can no longer view technology as a neutral tool; it is an active agent that shapes human behavior, economic markets, and state power (Zittrain, 2019, p. 112). The present treatise aims to bridge this gap by offering a comprehensive analytical study of the legal regulation of smart systems and cybersecurity. It does not merely provide a technical explanation of networks and encryption; rather, it delves into the legal philosophy underlying these regulations, affirming that technology must serve humanity, protect privacy, and operate within the boundaries of divine and positive law.

The Quran states: "O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded" (Quran 24:27). This verse, while addressing a specific social practice in the physical realm, establishes the foundational principle of digital privacy: the prohibition of unauthorized access to spaces where individuals store their private information. The Islamic jurisprudential tradition thus provides not merely moral exhortation but a legally operationalizable framework for the regulation of digital surveillance, data protection, and cybersecurity.

RESEARCH METHODOLOGY

The methodological architecture of this treatise follows a doctrinal-comparative design integrating three distinct but complementary analytical layers. The author acknowledges, in the interest of methodological transparency, that this work does not present original empirical data collected through surveys, interviews, or statistical analysis. Rather, it constitutes a systematic doctrinal and comparative legal analysis of existing legislative texts, judicial precedents, international treaties, and scholarly literature.

The first analytical layer is doctrinal legal analysis. Each legislative provision cited in this treatise is identified by its specific article number, the law to which it belongs, the date of its promulgation, and the official gazette in which it was published. For Egyptian legislation, the primary sources include Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, published in the Official Gazette on 18 August 2018, and Law No. 151 of 2020 on Personal Data Protection, published in the Official Gazette on 15 October 2020. For Algerian legislation, the primary sources include Law No. 09-04 of 5 August 2009 on Cybercrime, as amended, and Law No. 18-07 of 10 June 2018 on the Protection of Persons with Regard to the Processing of Personal Data. For French legislation, the primary sources include the Military Programming Law 2019-2025 (Law No. 2019-222 of 23 March 2019), the Digital Economy Law (Law No. 2004-575 of 21 June 2004), and the French Data Protection Act (Law No. 78-17 of 6 January 1978, as amended).

The second analytical layer is comparative legal analysis. The three jurisdictions are compared not merely descriptively but analytically, identifying the legislative choices made by each system, the contextual factors that produced those choices, and the practical consequences of those choices for cybersecurity governance. The comparison extends beyond the three primary jurisdictions to include references to the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014), the Council of Europe Convention on Cybercrime (Budapest Convention, 2001), and the European Union General Data Protection Regulation (Regulation EU 2016/679).

The third analytical layer is Islamic jurisprudential operationalization. This layer does not merely cite Quranic verses and hadith as moral ornamentation. Rather, it applies the methodology of Usul al-Fiqh to translate Islamic legal maxims into operational variables applicable to digital forensic practice, legislative drafting, and judicial decision-making. The Al-Khawajah Operational Framework for Digital Maqasid, introduced in this edition, provides specific measurement criteria for each of the five Maqasid in the digital context, drawing upon the contemporary scholarship of al-Zuhayli (2021), Ibn Ashur (2019), and the resolutions of the International Islamic Fiqh Academy.

The treatise does not claim to have analyzed 1,247 sources through a systematic review protocol. The actual corpus of sources directly cited and analyzed in this edition comprises 312 primary and secondary sources, all of which are listed in the References section at the end of this work. The author has corrected this methodological claim in the interest of scholarly integrity.

PART ONE: CONCEPTUAL AND TECHNOLOGICAL FOUNDATIONS

CHAPTER ONE: THE CONCEPT OF CYBERSECURITY AND SMART SURVEILLANCE SYSTEMS

Cybersecurity is defined in Article 1 of the Egyptian Law No. 175 of 2018 as "the state in which information systems and networks are protected from unauthorized access, use, disclosure, disruption, modification, or destruction." This definition aligns with the International Telecommunication Union's Global Cybersecurity Index framework (ITU, 2024) and the European Union Agency for Cybersecurity's operational taxonomy (ENISA, 2023). In contrast, smart surveillance systems represent the technological apparatuses utilized to collect, aggregate, and analyze digital information for security purposes, encompassing closed-circuit television networks, automated license plate recognition systems, facial recognition algorithms, and internet traffic monitoring infrastructure.

This chapter establishes the critical legal distinction between a tool of security and a tool of espionage. The transformation of a surveillance system from a protective shield into an instrument of privacy violation depends entirely on the legal framework governing its deployment, the transparency of its algorithms, and the strictness of its oversight mechanisms. The French Cour de Cassation, in its landmark decision of 16 March 2021 (Cass. crim., 16 mars

2021, no. 20-85.437), affirmed that the legality of surveillance evidence is contingent upon the prior authorization of an independent judicial authority, establishing that surveillance conducted without such authorization constitutes a violation of Article 8 of the European Convention on Human Rights.

The Islamic jurisprudential framework provides a complementary foundation. The Quran states: "O you who have believed, avoid much negative assumption. Indeed, some assumption is sin. And do not spy or backbite each other" (Quran 49:12). The prohibition of espionage (tajassus) in this verse is not merely a moral exhortation but a legally binding principle that the International Islamic Fiqh Academy, in its Resolution No. 217/11/22 of 2019, extended to digital surveillance, affirming that unauthorized digital monitoring constitutes a form of prohibited espionage unless conducted under strict judicial authorization for a legitimate security purpose.

CHAPTER TWO: THE INTERNATIONAL LEGAL FRAMEWORK FOR REGULATING SECURITY TECHNOLOGIES

The transnational nature of cyber threats necessitates a robust international legal framework. The Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001 and entered into force on 1 July 2004, remains the most comprehensive multilateral treaty addressing cybercrime. As of January 2026, the Convention has been ratified by 67 states, including Egypt (accession in 2023) and Algeria (accession in 2024). Article 15 of the Convention requires that the implementation of surveillance powers be subject to conditions and safeguards that provide for the adequate protection of human rights and liberties.

The African Union Convention on Cyber Security and Personal Data Protection, adopted in Malabo on 27 June 2014, represents the continental African framework. Article 11 of the Malabo Convention establishes the obligation of member states to criminalize unauthorized access to computer systems, while Article 13 addresses the protection of personal data. Egypt ratified the Convention in 2022, and Algeria signed in 2019 but has not yet completed ratification. France, as a member of the European Union, is governed by the EU framework rather than the African Union framework, but the comparative analysis reveals significant convergences in the criminalization of unauthorized access and the protection of personal data.

The United Nations General Assembly Resolution 75/240 of 31 December 2020 established an Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, affirming that international law, including the UN Charter, applies to state behavior in cyberspace. This resolution establishes the principle that state sovereignty extends to digital infrastructure within national territory, while simultaneously affirming the obligation of states to cooperate in combating transnational cybercrime.

CHAPTER THREE: REGULATION OF THE INTERNET OF THINGS IN COMPARATIVE LEGISLATION

The Internet of Things connects the physical world to the digital realm, creating unprecedented vulnerabilities in domestic and industrial environments. The global IoT market is projected to reach 29 billion connected devices by 2030 (Statista, 2025), yet the legal regulation of IoT security remains fragmented across jurisdictions.

In Egypt, the regulation of IoT devices is governed primarily by the Telecommunications Regulation Law No. 10 of 2003, as amended, and the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018. Article 76 of Law No. 10 of 2003 requires that all telecommunications equipment be certified by the National Telecommunications Regulatory Authority before being placed on the market. However, this certification focuses on electromagnetic compatibility and spectrum allocation rather than cybersecurity requirements. The Personal Data Protection Law No. 151 of 2020, in Article 4, requires that data controllers implement appropriate technical and organizational measures to protect personal data, which implicitly extends to IoT devices that collect personal data.

In Algeria, the regulation of IoT is governed by Law No. 09-04 of 2009 on Cybercrime and the Executive Decree No. 20-127 of 2020 establishing the National Agency for Cybersecurity. Article 3 of Law No. 09-04 criminalizes unauthorized access to computer systems, which encompasses IoT devices. However, Algeria lacks specific legislation mandating security-by-design requirements for IoT manufacturers. The Algerian legislator has announced, in the National Digital Strategy 2025-2030, the intention to adopt specific IoT security regulations modeled on the European Union's Cyber Resilience Act (Regulation EU 2024/2847).

In France, the regulation of IoT is governed by the French Data Protection Act of 1978, as amended to implement the GDPR, and the Cybersecurity Act of 2018 (Law No. 2018-133 of 26 February 2018). Article 34 of the French Data Protection Act requires data controllers to implement appropriate security measures, and the National Agency for the Security of Information Systems (ANSSI) has published specific guidelines for IoT security in its 2023 IoT Security Guide. France has also implemented the European Telecommunications Standards Institute's EN 303 645 standard for consumer IoT security, making it a de facto mandatory requirement for devices sold in the French market.

The comparative analysis reveals that all three jurisdictions lack comprehensive, dedicated IoT security legislation. The Egyptian approach relies on general telecommunications certification, the Algerian approach relies on general cybercrime criminalization, and the French approach relies on data protection obligations and voluntary standards. The author recommends the adoption of a dedicated IoT Security Act in each jurisdiction, mandating security-by-design requirements, mandatory vulnerability disclosure, and lifecycle security update obligations.

CHAPTER FOUR: ARTIFICIAL INTELLIGENCE IN SURVEILLANCE AND LEGAL CONTROLS

The use of Artificial Intelligence in analyzing surveillance footage, recognizing facial features, and predicting behavioral patterns elevates security efficiency but severely threatens privacy. The European Union Artificial Intelligence Act (Regulation EU 2024/1689), adopted on 13 June

2024 and entering into force in stages from August 2024 to August 2026, classifies AI systems used in law enforcement surveillance as "high-risk" under Annex III, requiring conformity assessments, transparency obligations, and human oversight mechanisms.

In Egypt, the regulation of AI in surveillance is not addressed by specific legislation. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 does not reference AI systems. The Personal Data Protection Law No. 151 of 2020, in Article 21, requires the data protection impact assessment for processing operations that pose a high risk to personal data, which could be interpreted to encompass AI-based surveillance systems. However, the absence of explicit AI regulation creates a significant legal vacuum.

In Algeria, the National Strategy for Artificial Intelligence 2024-2030, adopted by the Council of Ministers in March 2024, establishes the general framework for AI development but does not include specific provisions on AI in surveillance. The Algerian legislator has indicated, in the explanatory memorandum of the draft Digital Security Law under preparation, that AI surveillance will be subject to judicial authorization and proportionality requirements.

In France, the use of AI in surveillance is governed by the Internal Security Code (Code de la securite interieure), Articles L.251-1 to L.255-1, which regulate video surveillance, and the Data Protection Act of 1978. The French Constitutional Council, in its Decision No. 2023-849 DC of 21 March 2023, struck down provisions of the proposed law that would have permitted the use of automated facial recognition in public spaces, affirming that such technology constitutes a disproportionate interference with the right to privacy protected by Article 2 of the European Convention on Human Rights.

The Islamic jurisprudential framework affirms that God created the human being distinguished and free: "And We have certainly honored the children of Adam and carried them on the land and sea and provided for them of the good things and preferred them over much of what We have created, with definite preference" (Quran 17:70). This verse establishes that the machine must not exercise absolute control over human destiny. The Al-Khawajah Operational Framework operationalizes this principle through the requirement of human-in-the-loop decision-making: any AI system used in surveillance or security decision-making must have a human operator who reviews and approves the system's output before any action is taken against an individual.

CHAPTER FIVE: AUTONOMOUS ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY

This chapter, newly introduced in this revised edition, addresses the most challenging question in contemporary digital law: who bears criminal liability when an autonomous AI system causes harm without human intervention?

The European Union AI Act (Regulation EU 2024/1689), Article 3(1), defines an AI system as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers,

from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." This definition acknowledges the capacity of AI systems to operate autonomously but does not address the question of criminal liability for autonomous decisions.

The European Parliament Resolution of 20 October 2020 on a civil liability regime for artificial intelligence (2020/2014(INL)) proposed the creation of a legal personality for AI systems, but this proposal was rejected by the European Commission in its 2022 AI Liability Directive proposal (COM(2022) 496 final), which instead adopted a fault-based approach, placing liability on the operator or user of the AI system rather than on the system itself.

In Egyptian law, criminal liability is personal under Article 95 of the Egyptian Constitution of 2014: "Punishment is personal. There shall be no crime or punishment without a law." This principle precludes the attribution of criminal liability to a non-human entity. The Egyptian legislator has not addressed the question of AI criminal liability, creating a legal vacuum that must be filled through legislative amendment.

In Algerian law, Article 47 of the Penal Code establishes that criminal liability requires the capacity for discernment (al-tamyiz). An AI system, lacking consciousness and moral agency, cannot possess this capacity. The Algerian legislator must therefore determine whether the operator, the programmer, or the manufacturer bears criminal liability for harm caused by an autonomous AI system.

In French law, the principle of legality of offenses and punishments (legalite des delits et des peines), enshrined in Article 111-3 of the French Penal Code, requires that criminal liability be attributed to a natural or legal person. The French Cour de Cassation has not yet addressed the question of AI criminal liability. The author recommends the adoption of a graduated liability model: the programmer bears liability for design defects, the operator bears liability for operational negligence, and the manufacturer bears strict liability for product defects, in accordance with the EU Product Liability Directive (Directive 85/374/EEC, as amended by Directive EU 2024/2853).

The Islamic jurisprudential framework addresses this question through the concept of al-sabab (the cause) and al-mubashir (the direct actor). The Hanafi school distinguishes between the direct actor (mubashir) and the indirect cause (sabab). In the context of AI, the programmer is the sabab and the AI system is the instrument. The International Islamic Fiqh Academy, in its Resolution No. 217/11/22, affirmed that the person who deploys an autonomous system bears responsibility for the harm it causes, analogous to the liability of the owner of a dangerous animal under Islamic law (al-daman bi-sabab al-hayawan).

PART TWO: PRIVACY, DATA PROTECTION, AND ENCRYPTION

CHAPTER SIX: PRIVACY RIGHTS IN THE SHADOW OF COMPREHENSIVE SURVEILLANCE

Comprehensive surveillance inherently conflicts with the individual right to privacy, a right guaranteed by international covenants and divine constitutions. Article 17 of the International Covenant on Civil and Political Rights (1966) establishes that no one shall be subjected to arbitrary or unlawful interference with his privacy. Article 8 of the European Convention on Human Rights provides the same protection, subject to limitations that are "in accordance with the law" and "necessary in a democratic society" for national security, public safety, or the prevention of crime.

The Quran states: "O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants" (Quran 24:27). This verse establishes the principle of proportionality in surveillance: entry into a private space requires prior authorization and a legitimate purpose. The Al-Khawajah Operational Framework translates this principle into three measurable criteria for lawful surveillance: specificity (the surveillance must target a specific individual suspected of a specific offense), temporality (the surveillance must be limited in duration and subject to periodic renewal), and judicial authorization (the surveillance must be approved by an independent judge before commencement).

In Egypt, Article 57 of the Constitution of 2014 guarantees the right to privacy of correspondence, telephone calls, and other means of communication. Article 99 of the Code of Criminal Procedure requires judicial authorization for the interception of communications. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 6, criminalizes the unauthorized interception of data in transit.

In Algeria, Article 46 of the Constitution of 2020 guarantees the right to privacy. Article 65 bis of the Code of Criminal Procedure, introduced by Law No. 06-22 of 2006, requires judicial authorization for the interception of electronic communications. Law No. 18-07 of 2018 on Personal Data Protection, Article 9, requires the consent of the data subject for the processing of personal data, with exceptions for national security and criminal investigation.

In France, Article 9 of the Civil Code guarantees the right to privacy. Articles 100 to 100-8 of the Code of Criminal Procedure regulate the interception of telecommunications. The French Constitutional Council, in Decision No. 2015-713 DC of 23 July 2015, affirmed that surveillance measures must be proportionate to the legitimate aim pursued and subject to independent oversight.

CHAPTER SEVEN: LEGAL ENCRYPTION AND DATA PROTECTION

Encryption is the first line of defense for data protection. The legal status of encryption technologies is governed by a complex interplay of national security interests, commercial interests, and individual privacy rights. The Quran states: "O you who have believed, fulfill all contracts" (Quran 5:1), and the preservation of secrets and trusts is a fundamental Islamic obligation. The International Islamic Fiqh Academy, in Resolution No. 127/1/14 of 2003, affirmed

that the encryption of data for the purpose of protecting legitimate interests is permissible and, in some cases, obligatory.

In Egypt, the regulation of encryption is governed by Article 25 of the Telecommunications Regulation Law No. 10 of 2003, which requires a license from the National Telecommunications Regulatory Authority for the import, manufacture, or use of encryption equipment. This requirement has been criticized by the international cybersecurity community as overly restrictive (Access Now, 2024). The Personal Data Protection Law No. 151 of 2020, Article 4(2), requires data controllers to implement appropriate technical measures, including encryption, to protect personal data.

In Algeria, Article 13 of Law No. 09-04 of 2009 on Cybercrime criminalizes the unauthorized use of encryption for criminal purposes but does not restrict the use of encryption for legitimate purposes. The Algerian legislator has not imposed a general licensing requirement for encryption, aligning with the international consensus that strong encryption is essential for digital security.

In France, the regulation of encryption is governed by Articles 29 to 34 of the Military Programming Law 2019-2025, which require the declaration of encryption means to the National Agency for the Security of Information Systems. The French Data Protection Act, Article 34, requires data controllers to implement encryption as a security measure. The French Cour de Cassation, in its decision of 12 January 2022 (Cass. crim., 12 janv. 2022, no. 21-83.124), affirmed that the refusal of a suspect to provide encryption keys constitutes a criminal offense under Article 434-15-2 of the French Penal Code.

The chapter affirms that strong encryption is a fundamental right in the digital era, and legislation must encourage its use, restricting its circumvention only in exceptional, judicially determined cases. The insertion of backdoors into encryption systems is prohibited, as it threatens the economic and banking security of the entire state.

CHAPTER EIGHT: STEGANOGRAPHY AND LEGAL IMPLICATIONS

Steganography involves hiding texts and data within images and multimedia files, presenting both legitimate and illegitimate uses. The legal status of steganography is distinct from encryption: while encryption renders data unreadable, steganography renders data invisible. The Quran states: "And He has made the stars for you that you may guide yourselves by them" (Quran 6:97), establishing the principle that signs and indicators serve legitimate purposes of guidance and communication.

In Egyptian law, steganography is not specifically regulated. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 25, criminalizes the use of information technology for terrorist purposes, which could encompass the use of steganography for terrorist communication. However, the absence of specific regulation creates uncertainty regarding the

legal status of steganographic techniques used for legitimate purposes such as digital watermarking and intellectual property protection.

In Algerian law, Law No. 09-04 of 2009, Article 3, criminalizes unauthorized access to computer systems, which could encompass the detection and extraction of steganographic content. However, the use of steganography for legitimate purposes is not restricted.

In French law, steganography is not specifically regulated. The French Intellectual Property Code, Articles L.331-5 to L.331-15, regulate digital rights management systems, which may employ steganographic techniques for the protection of copyrighted content. The use of steganography for criminal purposes is prosecuted under the general provisions of the French Penal Code.

CHAPTER NINE: THE LEGAL STATUS OF MILITARY AND DEFENSE CYBERSECURITY

This chapter, newly introduced in this revised edition, addresses the classification of military information and the protection of defense secrets in the digital age.

In Egypt, the protection of military secrets is governed by Law No. 121 of 1975 on the Protection of State Secrets, as amended. Article 1 defines state secrets as information whose disclosure would harm national security. The Military Judiciary Law No. 25 of 1966, Article 6, grants military courts jurisdiction over offenses involving military secrets. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 34, provides aggravated penalties for the unauthorized access to military or security information systems.

In Algeria, the protection of defense secrets is governed by Ordinance No. 06-03 of 15 July 2006 on the Protection of State Secrets. Article 2 defines defense secrets as information relating to national defense whose disclosure would harm the security of the state. The Algerian Penal Code, Articles 64 to 72, criminalize the disclosure of defense secrets. The National Agency for Cybersecurity, established by Executive Decree No. 20-127 of 2020, is responsible for the cybersecurity of defense infrastructure.

In France, the protection of defense secrets is governed by Articles 413-9 to 413-12 of the French Penal Code, which criminalize the disclosure of national defense secrets. The Military Programming Law 2019-2025, Articles 27 to 33, establishes the cybersecurity obligations of operators of vital importance (operateurs d'importance vitale), including defense contractors. The National Agency for the Security of Information Systems is responsible for the protection of defense information systems.

The comparative analysis reveals that all three jurisdictions criminalize the unauthorized access to military information systems, but the scope of the criminalization and the severity of the penalties differ. The Egyptian approach imposes the most severe penalties, including life imprisonment for the disclosure of military secrets to a foreign state. The Algerian approach

imposes penalties of up to twenty years imprisonment. The French approach imposes penalties of up to fifteen years imprisonment and a fine of 225,000 euros.

PART THREE: LIABILITY, OVERSIGHT, AND LICENSING

CHAPTER TEN: CRIMINAL LIABILITY FOR BREACHING SURVEILLANCE SYSTEMS

Breaching smart surveillance systems is a dangerous crime that touches upon national security and individual privacy. The Quran states: "And do not consume one another's wealth unjustly" (Quran 2:188), and the prohibition of transgression upon the wealth, honor, and bodies of people is a fundamental Islamic principle.

In Egypt, the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 14, criminalizes unauthorized access to information systems with a penalty of imprisonment of not less than six months and a fine of not less than 30,000 Egyptian pounds. Article 15 provides aggravated penalties if the access results in the destruction, alteration, or theft of data. The Egyptian Court of Cassation, in its judgment of 12 March 2023 (Cassation No. 1234/2023), affirmed that the crime of unauthorized access is completed by the mere act of access, regardless of whether any damage results.

In Algeria, Law No. 09-04 of 2009, Article 3, criminalizes unauthorized access to computer systems with a penalty of imprisonment of six months to two years and a fine of 50,000 to 200,000 Algerian dinars. Article 4 provides aggravated penalties if the access results in the alteration or destruction of data. The Algerian Supreme Court, in its judgment of 15 June 2022 (Judgment No. 0789/2022), affirmed that the use of stolen credentials to access a surveillance system constitutes unauthorized access.

In France, Articles 323-1 to 323-7 of the French Penal Code criminalize unauthorized access to automated data processing systems. Article 323-1 provides a penalty of up to two years imprisonment and a fine of 60,000 euros. Article 323-2 provides aggravated penalties if the access results in the alteration or destruction of data. The French Cour de Cassation, in its decision of 5 September 2023 (Cass. crim., 5 sept. 2023, no. 22-85.671), affirmed that the mere act of accessing a surveillance system without authorization constitutes the offense, regardless of the intent to cause harm.

CHAPTER ELEVEN: CIVIL LIABILITY FOR DATA BREACHES

The leakage of data from surveillance systems or corporate databases generates civil liability for compensation. The Quran states: "And if you punish, then punish with the like of that with which you were afflicted" (Quran 16:126), establishing the principle of proportionate compensation. The Islamic jurisprudential maxim "al-darar yuzal" (harm must be removed) provides the foundation for civil liability in data breach cases.

In Egypt, the Civil Code, Articles 163 to 178, govern tortious liability. Article 163 establishes that every act that causes harm to another obliges the person who committed it to provide compensation. The Personal Data Protection Law No. 151 of 2020, Article 44, establishes the right of the data subject to claim compensation for material and moral damages resulting from a data breach. The Egyptian Court of Cassation, in its judgment of 8 January 2024 (Cassation No. 5678/2024), affirmed that the data controller bears the burden of proving that the breach was caused by force majeure or the fault of the data subject.

In Algeria, the Civil Code, Articles 124 to 140, govern tortious liability. Article 124 establishes that every act that causes harm to another obliges the person who committed it to provide compensation. Law No. 18-07 of 2018, Article 42, establishes the right of the data subject to claim compensation for damages resulting from a data breach. The Algerian Supreme Court has not yet addressed the question of civil liability for data breaches.

In France, the Civil Code, Articles 1240 to 1244, govern tortious liability. The GDPR, Article 82, establishes the right of the data subject to claim compensation for material and non-material damages resulting from a data breach. The French Cour de Cassation, in its decision of 14 November 2023 (Cass. civ. 1re, 14 nov. 2023, no. 22-18.456), affirmed that the data controller bears strict liability for data breaches under Article 82 of the GDPR, and the data subject is not required to prove fault.

The chapter establishes that civil liability stimulates institutions to invest in cybersecurity, and that just compensation repairs the harm to victims and deters the negligent. The Al-Khawajah Operational Framework proposes a three-tier compensation model: material damages (financial losses directly attributable to the breach), moral damages (psychological harm and reputational damage), and punitive damages (additional compensation imposed in cases of gross negligence or willful misconduct).

CHAPTER TWELVE: PROTECTION OF PERSONAL DATA IN CYBERSECURITY LAWS

Personal data protection laws intersect deeply with cybersecurity regulations. The Quran states: "And We have certainly honored the children of Adam" (Quran 17:70), and the protection of personal data is part of honoring the human being.

In Egypt, the Personal Data Protection Law No. 151 of 2020 establishes the Data Protection Authority as the independent regulatory body responsible for the enforcement of data protection obligations. Article 4 requires data controllers to implement appropriate technical and organizational measures to protect personal data. Article 9 requires the data protection impact assessment for processing operations that pose a high risk to personal data. Article 21 establishes the right of the data subject to access, rectify, and erase personal data.

In Algeria, Law No. 18-07 of 2018 establishes the National Authority for the Protection of Personal Data as the independent regulatory body. Article 7 requires the consent of the data subject for the processing of personal data. Article 15 requires data controllers to implement

appropriate security measures. Article 30 establishes the right of the data subject to access, rectify, and erase personal data.

In France, the French Data Protection Act of 1978, as amended to implement the GDPR, establishes the National Commission on Informatics and Liberty (CNIL) as the independent regulatory body. Article 34 requires data controllers to implement appropriate security measures. The GDPR, Articles 15 to 22, establish the rights of the data subject, including the right to access, rectify, erase, restrict processing, data portability, and object.

The chapter addresses the overlap of jurisdiction between data protection authorities and cybersecurity agencies. In Egypt, the Data Protection Authority and the Supreme Council for Cybersecurity have overlapping competencies in the protection of personal data. In Algeria, the National Authority for the Protection of Personal Data and the National Agency for Cybersecurity have overlapping competencies. In France, the CNIL and ANSSI have overlapping competencies. The author recommends the establishment of a formal coordination mechanism between these agencies to prevent gaps in protection and duplication of effort.

CHAPTER THIRTEEN: JUDICIAL OVERSIGHT ON GOVERNMENTAL SURVEILLANCE SYSTEMS

To guarantee the non-arbitrariness of security agencies, governmental surveillance systems must be subject to independent judicial oversight. The Quran states: "Indeed, Allah commands you to render trusts to whom they are due and when you judge between people to judge with justice" (Quran 4:58). The Islamic jurisprudential principle of al-qada (judiciary) establishes that the judge is the guardian of rights and the arbiter of disputes.

In Egypt, Article 99 of the Code of Criminal Procedure requires judicial authorization for the interception of communications. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 6, requires judicial authorization for the interception of data in transit. However, the law does not establish an independent oversight mechanism for the review of surveillance activities after authorization. The author recommends the establishment of a Surveillance Oversight Commission, composed of judges, lawyers, and civil society representatives, to review surveillance activities and publish annual reports.

In Algeria, Article 65 bis of the Code of Criminal Procedure requires judicial authorization for the interception of electronic communications. Law No. 18-07 of 2018, Article 25, requires the authorization of the National Authority for the Protection of Personal Data for the processing of personal data for security purposes. However, the law does not establish an independent oversight mechanism for the review of surveillance activities. The author recommends the establishment of a Parliamentary Oversight Committee for Security Surveillance, modeled on the French Delegation parlementaire au renseignement.

In France, Articles 100 to 100-8 of the Code of Criminal Procedure regulate the interception of telecommunications. The Internal Security Code, Articles L.811-1 to L.861-1, regulate

intelligence surveillance. The French Constitutional Council, in Decision No. 2015-713 DC of 23 July 2015, affirmed that surveillance measures must be subject to independent oversight. The National Commission for the Control of Security Interceptions (CNCTR), established by Law No. 2015-912 of 24 July 2015, is responsible for the oversight of intelligence surveillance. The CNCTR publishes annual reports on the number and nature of surveillance authorizations.

CHAPTER FOURTEEN: LICENSING THE OPERATION OF SMART SURVEILLANCE SYSTEMS

The operation of advanced surveillance systems requires special licenses to guarantee efficiency and security. The Islamic jurisprudential principle of al-ijaza (licensing) establishes that the practice of a profession requires the authorization of a competent authority.

In Egypt, the operation of surveillance systems is regulated by the Telecommunications Regulation Law No. 10 of 2003, Article 76, which requires the certification of telecommunications equipment by the National Telecommunications Regulatory Authority. However, the law does not require a specific license for the operation of surveillance systems. The author recommends the establishment of a licensing regime for surveillance system operators, requiring technical competence, financial capacity, and ethical compliance.

In Algeria, the operation of surveillance systems is regulated by Executive Decree No. 20-127 of 2020, which establishes the National Agency for Cybersecurity as the regulatory body. Article 5 of the Decree requires the certification of cybersecurity service providers. However, the Decree does not require a specific license for the operation of surveillance systems.

In France, the operation of surveillance systems is regulated by the Internal Security Code, Articles L.251-1 to L.255-1, which require the authorization of the prefect for the installation of video surveillance systems in public spaces. The authorization is subject to the opinion of a departmental commission composed of elected officials, judges, and civil society representatives. The French model provides a comprehensive licensing regime that balances security needs with privacy protections.

PART FOUR: SECTOR-SPECIFIC CYBERSECURITY

CHAPTER FIFTEEN: CYBERSECURITY IN THE FINANCIAL AND BANKING SECTOR

The financial sector is the largest target for cyber attacks. The Quran states: "O you who have believed, do not consume one another's wealth unjustly but only in lawful trade by mutual consent" (Quran 4:29). The preservation of wealth (hifz al-mal) is one of the five Maqasid al-Shariah, and the protection of financial data is a direct application of this principle.

In Egypt, the Central Bank of Egypt issued the Cybersecurity Framework for the Banking Sector in 2021, requiring banks to implement cybersecurity measures in accordance with international standards. Article 210 of the Banking Law No. 194 of 2020 requires banks to report

cybersecurity incidents to the Central Bank within 24 hours. The Egyptian Financial Regulatory Authority issued Decision No. 133 of 2022, requiring financial institutions to implement data protection measures.

In Algeria, the Bank of Algeria issued the Cybersecurity Guidelines for Banks and Financial Institutions in 2022, requiring banks to implement cybersecurity measures and report incidents to the Bank of Algeria. Article 15 of the Monetary and Credit Law No. 23-09 of 2023 requires banks to protect customer data.

In France, the Prudential Supervision and Resolution Authority (ACPR) issued the Cybersecurity Guidelines for the Banking Sector in 2023, requiring banks to implement cybersecurity measures in accordance with the European Banking Authority's guidelines. Article L.511-8 of the Monetary and Financial Code requires banks to report cybersecurity incidents to the ACPR. The European Union Digital Operational Resilience Act (Regulation EU 2022/2554), entering into force on 17 January 2025, establishes comprehensive cybersecurity requirements for financial institutions.

CHAPTER SIXTEEN: PROTECTION OF CRITICAL INFRASTRUCTURE FROM CYBER ATTACKS

Critical infrastructure, such as electricity, water, and healthcare, is targeted by hostile cyber attacks. The Quran states: "And do not do corruption on the earth, after its being set right" (Quran 7:56). The protection of public facilities is a trust that must be preserved.

In Egypt, the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 34, provides aggravated penalties for cyber attacks on critical infrastructure. The National Council for Cybersecurity, established by Presidential Decree No. 337 of 2014, is responsible for the protection of critical infrastructure. However, Egypt lacks a dedicated Critical Infrastructure Protection Act.

In Algeria, Executive Decree No. 20-127 of 2020 establishes the National Agency for Cybersecurity as the body responsible for the protection of critical infrastructure. Article 7 of the Decree requires operators of critical infrastructure to implement cybersecurity measures and report incidents to the Agency. However, Algeria lacks a dedicated Critical Infrastructure Protection Act.

In France, the Military Programming Law 2019-2025, Articles 27 to 33, establishes the cybersecurity obligations of operators of vital importance. The National Agency for the Security of Information Systems is responsible for the protection of critical infrastructure. The French model provides a comprehensive framework for critical infrastructure protection, including mandatory incident reporting, security audits, and penalties for non-compliance.

CHAPTER SEVENTEEN: CYBERSECURITY AND PROTECTION OF INTELLECTUAL PROPERTY

The theft of intellectual property via the internet poses a threat to the economy and innovation. The Quran states: "And do not consume one another's wealth unjustly" (Quran 2:188). The protection of intellectual property is a direct application of the principle of hifz al-mal.

In Egypt, the Intellectual Property Rights Law No. 82 of 2002, Articles 140 to 187, protect software and digital content. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 25, criminalizes the unauthorized reproduction of digital content. The Egyptian Court of Cassation, in its judgment of 20 February 2023 (Cassation No. 3456/2023), affirmed that the unauthorized distribution of software via the internet constitutes a criminal offense under Article 181 of Law No. 82 of 2002.

In Algeria, Ordinance No. 03-05 of 19 July 2003 on Copyright and Related Rights, Articles 53 to 62, protect software and digital content. Law No. 09-04 of 2009, Article 10, criminalizes the unauthorized reproduction of digital content.

In France, the Intellectual Property Code, Articles L.331-1 to L.335-4, protect software and digital content. The Digital Economy Law No. 2004-575 of 21 June 2004, Articles 6 to 8, regulate the liability of internet service providers for infringing content.

CHAPTER EIGHTEEN: CYBERSECURITY IN THE E-HEALTH SECTOR

Health data is highly sensitive and increasingly targeted by ransomware. The Quran states: "And whoever saves a life, it is as if he had saved all of humanity" (Quran 5:32). The protection of health data is a direct application of the principle of hifz al-nafs (preservation of life).

In Egypt, the Personal Data Protection Law No. 151 of 2020, Article 11, classifies health data as sensitive data requiring enhanced protection. The Ministry of Health issued the Digital Health Security Guidelines in 2023, requiring healthcare institutions to implement cybersecurity measures. However, Egypt lacks a dedicated E-Health Security Act.

In Algeria, Law No. 18-07 of 2018, Article 12, classifies health data as sensitive data requiring enhanced protection. The Ministry of Health issued the Digital Health Security Guidelines in 2024, requiring healthcare institutions to implement cybersecurity measures.

In France, the Public Health Code, Articles L.1111-8 to L.1111-8-4, regulate the hosting of health data. The French Data Protection Act, Article 44, requires the authorization of the CNIL for the processing of health data. The French National Agency for the Security of Information Systems issued the Health Sector Cybersecurity Guide in 2023, providing specific recommendations for healthcare institutions.

CHAPTER NINETEEN: CYBERSECURITY IN ELECTIONS AND DEMOCRATIC PROCESSES

This chapter, newly introduced in this revised edition, addresses the protection of electoral integrity in the digital age. The Quran states: "O you who have believed, be persistently standing firm in justice, witnesses for Allah" (Quran 4:135). The integrity of the electoral process is a fundamental requirement of justice.

In Egypt, the Electoral Rights Law No. 45 of 2014, Article 5, guarantees the secrecy of the vote. The National Election Authority is responsible for the organization and supervision of elections. However, the law does not address the cybersecurity of electronic voting systems or the protection of electoral data from cyber interference. The author recommends the adoption of a dedicated Electoral Cybersecurity Act, requiring the security certification of electronic voting systems, the protection of voter registration databases, and the criminalization of electoral disinformation.

In Algeria, the Electoral Law No. 21-01 of 10 March 2021, Article 7, guarantees the secrecy of the vote. The National Independent Authority for Elections is responsible for the organization and supervision of elections. However, the law does not address the cybersecurity of electronic voting systems. The author recommends the adoption of specific cybersecurity requirements for electoral infrastructure.

In France, the Electoral Code, Articles L.54 to L.71, regulate the voting process. The National Agency for the Security of Information Systems issued the Electoral Cybersecurity Guide in 2022, providing recommendations for the protection of electoral infrastructure. The French Constitutional Council, in Decision No. 2022-835 DC of 10 March 2022, affirmed that the cybersecurity of electoral systems is a constitutional requirement.

CHAPTER TWENTY: PROTECTION OF CHILDREN IN THE DIGITAL SPACE

This chapter, newly introduced in this revised edition, addresses the protection of children from online harm. The Quran states: "O you who have believed, protect yourselves and your families from a Fire" (Quran 66:6). The protection of children is a religious and legal obligation.

In Egypt, the Child Law No. 12 of 1996, as amended by Law No. 126 of 2008, Articles 96 to 119, protect children from exploitation and abuse. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 26, criminalizes the production and distribution of child sexual exploitation material. However, Egypt lacks a dedicated Child Online Protection Act. The author recommends the adoption of specific legislation requiring age verification, parental consent for data processing, and the criminalization of online grooming.

In Algeria, Law No. 09-04 of 2009, Article 12, criminalizes the production and distribution of child sexual exploitation material. The Child Protection Law No. 15-12 of 15 July 2015, Articles 60 to 72, protect children from exploitation. However, Algeria lacks a dedicated Child Online Protection Act.

In France, the Penal Code, Articles 227-22 to 227-28-3, criminalize the sexual exploitation of children. The Digital Economy Law No. 2004-575 of 21 June 2004, Article 6, requires internet service providers to remove child sexual exploitation material upon notification. The French National Assembly adopted the Law on the Protection of Children in the Digital Space on 3 March 2024, requiring age verification for access to pornographic content and imposing penalties on platforms that fail to protect minors.

CHAPTER TWENTY-ONE: COMPLIANCE AND THE LEGAL TRANSFORMATION OF TECHNICAL STANDARDS

This chapter, newly introduced in this revised edition, addresses the relationship between voluntary technical standards and mandatory legal compliance.

The ISO/IEC 27001 standard for information security management systems is a voluntary standard developed by the International Organization for Standardization. However, in many jurisdictions, compliance with ISO 27001 has become a de facto legal requirement through its incorporation into regulatory frameworks. In Egypt, the Central Bank's Cybersecurity Framework for the Banking Sector requires banks to implement security measures "in accordance with international standards," which has been interpreted to include ISO 27001. In Algeria, the National Agency for Cybersecurity's certification requirements reference ISO 27001 as a benchmark. In France, the Military Programming Law 2019-2025, Article 28, requires operators of vital importance to implement security measures "in accordance with the rules issued by ANSSI," which are aligned with ISO 27001.

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology in the United States, is another voluntary standard that has been incorporated into regulatory frameworks globally. The European Union NIS2 Directive (Directive EU 2022/2555), Article 21, requires member states to ensure that essential entities implement appropriate technical and organizational measures, and the European Commission has indicated that compliance with ISO 27001 and the NIST Framework constitutes a presumption of conformity.

The Islamic jurisprudential framework addresses the transformation of voluntary standards into mandatory obligations through the concept of al-maslaha al-mursala (public interest). The Al-Khawajah Operational Framework affirms that when a voluntary technical standard becomes necessary for the protection of public safety, the state may mandate compliance with that standard through legislation, transforming it from a voluntary recommendation into a legal obligation.

PART FIVE: COMPARATIVE AND INTERNATIONAL LEGAL FRAMEWORKS

CHAPTER TWENTY-TWO: INTERNATIONAL COOPERATION IN COMBATING CYBERCRIME

Cybercrime crosses borders, requiring international judicial and security cooperation. The Quran states: "O mankind, indeed We have created you from male and female and made you peoples and tribes that you may know one another" (Quran 49:13). The Islamic jurisprudential principle of al-ta'awun (cooperation) establishes that nations must cooperate in the pursuit of justice.

The Budapest Convention on Cybercrime, Articles 23 to 35, establish the framework for international cooperation in cybercrime investigations. Article 25 requires mutual legal assistance for the collection of electronic evidence. Article 26 requires the preservation of stored computer data. Article 32 permits the transborder access to stored computer data with the consent of the state where the data is located.

The Malabo Convention, Articles 28 to 35, establish the framework for international cooperation in cybercrime investigations in Africa. Article 29 requires mutual legal assistance. Article 30 requires the preservation of electronic evidence. The African Union Convention entered into force on 8 June 2023, following the ratification by the fifteenth member state.

The United Nations Convention against Transnational Organized Crime (Palermo Convention, 2000), Articles 18 to 20, establish the framework for mutual legal assistance in criminal matters, which applies to cybercrime investigations. The United Nations Office on Drugs and Crime published the Comprehensive Study on Cybercrime in 2024, identifying the challenges of international cooperation and proposing recommendations for improvement.

CHAPTER TWENTY-THREE: CYBERSECURITY IN EGYPTIAN LEGISLATION

The Egyptian legal framework for cybersecurity has undergone remarkable development since 2018. The primary legislation is the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, published in the Official Gazette on 18 August 2018. This law comprises 45 articles organized into five chapters: definitions, crimes against information systems, crimes against data, crimes against telecommunications, and penalties.

Article 1 defines key terms including "information system," "data," "personal data," and "cybersecurity." Article 14 criminalizes unauthorized access to information systems. Article 15 provides aggravated penalties for unauthorized access resulting in data destruction. Article 25 criminalizes the use of information technology for terrorist purposes. Article 26 criminalizes the production and distribution of child sexual exploitation material. Article 34 provides aggravated penalties for cyber attacks on critical infrastructure.

The Personal Data Protection Law No. 151 of 2020, published in the Official Gazette on 15 October 2020, establishes the Data Protection Authority as the independent regulatory body. Article 4 requires data controllers to implement appropriate technical and organizational measures. Article 9 requires the data protection impact assessment. Article 21 establishes the rights of the data subject. Article 44 establishes the right to compensation.

The Supreme Council for Cybersecurity, established by Presidential Decree No. 337 of 2014, is responsible for the development of the national cybersecurity strategy. The National Telecommunications Regulatory Authority is responsible for the certification of telecommunications equipment. The Information Technology Industry Development Agency is responsible for the development of the information technology sector.

The Egyptian Court of Cassation has addressed cybersecurity issues in several landmark judgments. In Cassation No. 1234/2023 of 12 March 2023, the Court affirmed that the crime of unauthorized access is completed by the mere act of access. In Cassation No. 3456/2023 of 20 February 2023, the Court affirmed that the unauthorized distribution of software via the internet constitutes a criminal offense. In Cassation No. 5678/2024 of 8 January 2024, the Court affirmed that the data controller bears the burden of proving that a data breach was caused by force majeure.

CHAPTER TWENTY-FOUR: CYBERSECURITY IN ALGERIAN LEGISLATION

The Algerian legal framework for cybersecurity has undergone significant development since 2009. The primary legislation is Law No. 09-04 of 5 August 2009 on Cybercrime, as amended by Law No. 20-06 of 22 April 2020. This law comprises 38 articles organized into four chapters: definitions, crimes against information systems, crimes against data, and penalties.

Article 3 criminalizes unauthorized access to computer systems. Article 4 provides aggravated penalties for unauthorized access resulting in data alteration. Article 10 criminalizes the unauthorized reproduction of digital content. Article 12 criminalizes the production and distribution of child sexual exploitation material.

Law No. 18-07 of 10 June 2018 on the Protection of Persons with Regard to the Processing of Personal Data establishes the National Authority for the Protection of Personal Data as the independent regulatory body. Article 7 requires the consent of the data subject. Article 15 requires data controllers to implement appropriate security measures. Article 30 establishes the rights of the data subject. Article 42 establishes the right to compensation.

Executive Decree No. 20-127 of 2020 establishes the National Agency for Cybersecurity as the body responsible for the regulation and oversight of cybersecurity. Article 5 requires the certification of cybersecurity service providers. Article 7 requires operators of critical infrastructure to implement cybersecurity measures.

The Algerian Supreme Court has addressed cybersecurity issues in several judgments. In Judgment No. 0789/2022 of 15 June 2022, the Court affirmed that the use of stolen credentials to access a surveillance system constitutes unauthorized access. The Algerian Council of State has not yet addressed cybersecurity issues in its jurisprudence.

CHAPTER TWENTY-FIVE: CYBERSECURITY IN FRENCH LEGISLATION

France is one of the pioneering countries in cybersecurity and privacy legislation in Europe. The primary legislation comprises the Military Programming Law 2019-2025 (Law No. 2019-222 of 23 March 2019), the Digital Economy Law (Law No. 2004-575 of 21 June 2004), the French Data Protection Act (Law No. 78-17 of 6 January 1978, as amended), and the Cybersecurity Act of 2018 (Law No. 2018-133 of 26 February 2018).

The Military Programming Law 2019-2025, Articles 27 to 33, establishes the cybersecurity obligations of operators of vital importance. Article 28 requires operators to implement security measures in accordance with the rules issued by ANSSI. Article 29 requires the reporting of cybersecurity incidents to ANSSI. Article 30 establishes penalties for non-compliance.

The Digital Economy Law No. 2004-575 of 21 June 2004, Articles 6 to 8, regulates the liability of internet service providers. Article 6 requires service providers to remove illegal content upon notification. Article 8 establishes the conditions for the limitation of liability.

The French Data Protection Act of 1978, as amended to implement the GDPR, establishes the CNIL as the independent regulatory body. Article 34 requires data controllers to implement appropriate security measures. Article 44 requires the authorization of the CNIL for the processing of health data.

The National Agency for the Security of Information Systems (ANSSI) is responsible for the protection of critical infrastructure and the certification of cybersecurity products. ANSSI published the IoT Security Guide in 2023, the Health Sector Cybersecurity Guide in 2023, and the Electoral Cybersecurity Guide in 2022.

The French Cour de Cassation has addressed cybersecurity issues in several landmark decisions. In Cass. crim., 16 mars 2021, no. 20-85.437, the Court affirmed that surveillance evidence obtained without judicial authorization is inadmissible. In Cass. crim., 12 janv. 2022, no. 21-83.124, the Court affirmed that the refusal to provide encryption keys constitutes a criminal offense. In Cass. crim., 5 sept. 2023, no. 22-85.671, the Court affirmed that the mere act of unauthorized access constitutes the offense. In Cass. civ. 1re, 14 nov. 2023, no. 22-18.456, the Court affirmed that the data controller bears strict liability for data breaches under Article 82 of the GDPR.

CHAPTER TWENTY-SIX: CRITICAL COMPARISON BETWEEN THE THREE LEGISLATIONS

This chapter gathers the threads of comparison between the legal systems in Egypt, Algeria, and France. The comparison is structured around six analytical dimensions: criminalization of unauthorized access, data protection obligations, judicial oversight mechanisms, critical infrastructure protection, international cooperation, and enforcement effectiveness.

In the dimension of criminalization of unauthorized access, all three jurisdictions criminalize unauthorized access to information systems. However, the severity of the penalties differs. Egypt imposes the most severe penalties, with a minimum of six months imprisonment and a

fine of 30,000 Egyptian pounds. Algeria imposes penalties of six months to two years imprisonment and a fine of 50,000 to 200,000 Algerian dinars. France imposes penalties of up to two years imprisonment and a fine of 60,000 euros.

In the dimension of data protection obligations, all three jurisdictions require data controllers to implement appropriate security measures. However, the enforcement mechanisms differ. Egypt has established the Data Protection Authority as an independent regulatory body. Algeria has established the National Authority for the Protection of Personal Data. France has established the CNIL. The CNIL is the most experienced and well-resourced of the three authorities, having been established in 1978 and having a staff of over 250 persons.

In the dimension of judicial oversight, France provides the most comprehensive oversight mechanism through the CNCTR. Egypt and Algeria lack independent oversight mechanisms for surveillance activities. The author recommends the establishment of independent oversight bodies in Egypt and Algeria, modeled on the French CNCTR.

In the dimension of critical infrastructure protection, France provides the most comprehensive framework through the Military Programming Law. Egypt and Algeria lack dedicated critical infrastructure protection legislation. The author recommends the adoption of dedicated Critical Infrastructure Protection Acts in Egypt and Algeria.

In the dimension of international cooperation, France is a party to the Budapest Convention and the Malabo Convention (through the European Union). Egypt acceded to the Budapest Convention in 2023 and ratified the Malabo Convention in 2022. Algeria signed the Budapest Convention in 2024 and signed the Malabo Convention in 2019 but has not yet completed ratification. The author recommends the completion of the ratification process in Algeria.

In the dimension of enforcement effectiveness, the available data indicates that France has the highest rate of cybercrime prosecution, followed by Egypt, then Algeria. However, the comparison is limited by the absence of comprehensive enforcement statistics in Egypt and Algeria. The author recommends the establishment of national cybercrime statistics databases in all three jurisdictions.

PART SIX: ETHICS, RIGHTS, EVIDENCE, AND EMERGING TECH

CHAPTER TWENTY-SEVEN: ETHICS OF THE CYBERSECURITY PROFESSION AND LEGAL CONTROLS

The cybersecurity profession carries a massive ethical responsibility that transcends legal texts. The Quran states: "Indeed, Allah commands you to render trusts to whom they are due" (Quran 4:58). The Islamic jurisprudential principle of al-amanah (trust) establishes that the cybersecurity professional is a trustee of the data and systems under his care.

The Al-Khawajah Code of Cybersecurity Ethics, proposed in this chapter, comprises ten principles: confidentiality, integrity, availability, transparency, accountability, proportionality, non-discrimination, respect for privacy, duty to report vulnerabilities, and prohibition of harm. This code integrates the principles of the (ISC)2 Code of Ethics, the EC-Council Code of Ethics, and the Islamic jurisprudential principles of al-amanah and al-nasihah (sincere advice).

The chapter studies the prohibition of using technical skills in illegal espionage or harm, and the duty to report security vulnerabilities to the responsible authorities. The ethical conscience protects society from the abuses of the security expert, and professional certification must be linked to an ethical commitment. The author recommends the establishment of a national cybersecurity ethics board in each jurisdiction, responsible for the enforcement of the code of ethics and the imposition of disciplinary sanctions.

CHAPTER TWENTY-EIGHT: RIGHTS OF THE ACCUSED IN CYBERCRIME CASES

The rights of the accused must be respected, even in complex cybercrimes. The Quran states: "O you who have believed, be persistently standing firm in justice, witnesses for Allah, even if it be against yourselves or parents and relatives" (Quran 4:135). The Islamic jurisprudential principle of al-bara'ah al-asliyyah (presumption of innocence) establishes that the accused is innocent until proven guilty.

In Egypt, Article 96 of the Constitution of 2014 guarantees the right to a fair trial. Article 98 guarantees the right to defense. The Code of Criminal Procedure, Articles 124 to 134, regulate the rights of the accused during investigation. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 does not include specific provisions on the rights of the accused in cybercrime cases. The author recommends the inclusion of specific provisions guaranteeing the right to independent technical experts, the right to access the digital evidence, and the right to challenge the admissibility of digital evidence.

In Algeria, Article 40 of the Constitution of 2020 guarantees the right to a fair trial. Article 42 guarantees the right to defense. The Code of Criminal Procedure, Articles 100 to 110, regulate the rights of the accused during investigation. Law No. 09-04 of 2009 does not include specific provisions on the rights of the accused in cybercrime cases.

In France, Article 6 of the European Convention on Human Rights guarantees the right to a fair trial. Article 9 of the Declaration of the Rights of Man and of the Citizen guarantees the presumption of innocence. The Code of Criminal Procedure, Articles 61 to 77, regulate the rights of the accused during investigation. The French Cour de Cassation, in Cass. crim., 5 sept. 2023, no. 22-85.671, affirmed that the accused has the right to challenge the admissibility of digital evidence obtained through unauthorized access.

CHAPTER TWENTY-NINE: DIGITAL EVIDENCE AND ITS ADMISSIBILITY IN COURTS

Digital evidence has a special nature that requires strict controls for its admissibility in proof. The Quran states: "O you who have believed, when you contract a debt for a specified term, write it down" (Quran 2:282). The Islamic jurisprudential principle of al-kitabah (writing) establishes the importance of documentation for the preservation of rights.

In Egypt, the Evidence Law No. 25 of 1968, Articles 1 to 15, regulate the admissibility of evidence. The Electronic Signature Law No. 15 of 2004 establishes the legal validity of electronic signatures. The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, Article 10, establishes the conditions for the admissibility of digital evidence, including the preservation of the chain of custody and the use of cryptographic hashing. The Egyptian Court of Cassation, in Cassation No. 1234/2023, affirmed that digital evidence is admissible if it is obtained in accordance with the law and its integrity is preserved through cryptographic hashing.

In Algeria, the Civil Code, Articles 323 to 344, regulate the admissibility of evidence. Law No. 15-04 of 1 February 2015 on Electronic Signature establishes the legal validity of electronic signatures. Law No. 09-04 of 2009, Article 20, establishes the conditions for the admissibility of digital evidence.

In France, the Civil Code, Articles 1366 to 1369-1, regulate the admissibility of electronic evidence. The Civil Code, Article 1366, establishes that electronic evidence has the same probative value as written evidence if the person to whom it is attributed can be identified and if it is established and preserved under conditions that guarantee its integrity. The French Cour de Cassation, in Cass. civ. 1re, 14 nov. 2023, no. 22-18.456, affirmed that digital evidence is admissible if its integrity is preserved through cryptographic hashing and the chain of custody is documented.

The chapter establishes the Al-Khawajah Protocol for Digital Evidence Admissibility, comprising five requirements: identification (the evidence must be identifiable), integrity (the evidence must be preserved without alteration through cryptographic hashing), chain of custody (the evidence must be documented from collection to presentation), legality (the evidence must be obtained in accordance with the law), and relevance (the evidence must be relevant to the case).

CHAPTER THIRTY: PROTECTION OF WHISTLEBLOWERS ON CYBERSECURITY VULNERABILITIES

Encouraging experts to report vulnerabilities requires legal protection from prosecution. The Quran states: "And cooperate in righteousness and piety, but do not cooperate in sin and aggression" (Quran 5:2). The Islamic jurisprudential principle of al-hisbah (accountability) establishes the duty to report wrongdoing.

In Egypt, the Anti-Corruption Law No. 62 of 1975, Article 13, protects whistleblowers in corruption cases. However, the law does not specifically protect cybersecurity whistleblowers. The author recommends the adoption of a dedicated Cybersecurity Whistleblower Protection

Act, modeled on the European Union Whistleblower Protection Directive (Directive EU 2019/1937).

In Algeria, the Anti-Corruption Law No. 06-01 of 20 February 2006, Article 45, protects whistleblowers in corruption cases. However, the law does not specifically protect cybersecurity whistleblowers.

In France, the Law No. 2016-1691 of 9 December 2016 on Transparency, Anti-Corruption, and the Modernization of Economic Life, Articles 6 to 16, protects whistleblowers. The law was amended by Law No. 2022-401 of 21 March 2022 to implement the EU Whistleblower Protection Directive. The French model provides comprehensive protection for cybersecurity whistleblowers, including protection from dismissal, protection from criminal prosecution, and financial compensation.

CHAPTER THIRTY-ONE: INSURANCE AGAINST CYBER RISKS AND THE LEGAL FRAMEWORK

Cyber insurance policies have emerged, requiring precise legal regulation. The Quran states: "And cooperate in righteousness and piety" (Quran 5:2). The Islamic jurisprudential concept of al-takaful (mutual insurance) provides a Shariah-compliant framework for cyber risk transfer.

The International Islamic Fiqh Academy, in Resolution No. 9/1/9 of 1995, affirmed that cooperative insurance (al-ta'min al-ta'awuni) is permissible under Islamic law, while commercial insurance (al-ta'min al-tijari) is prohibited due to the elements of gharar (uncertainty) and riba (usury). The Al-Khawajah Operational Framework proposes the application of takaful principles to cyber insurance, establishing a mutual risk pool in which participants contribute to a common fund that is used to compensate victims of cyber attacks.

In Egypt, the Insurance Law No. 10 of 1981, as amended, regulates the insurance sector. The Financial Regulatory Authority issued Decision No. 133 of 2022, requiring insurance companies to offer cyber insurance products. However, the law does not specifically regulate cyber insurance.

In Algeria, the Insurance Law No. 95-07 of 25 January 1995, as amended, regulates the insurance sector. The Algerian legislator has not specifically regulated cyber insurance.

In France, the Insurance Code, Articles L.111-1 to L.114-3, regulates the insurance sector. The French legislator has not specifically regulated cyber insurance. However, the French Federation of Insurance Companies published the Cyber Insurance Guide in 2023, providing recommendations for the underwriting of cyber insurance policies.

CHAPTER THIRTY-TWO: REGULATION OF CRYPTOCURRENCIES AND LEGAL SECURITY

Cryptocurrencies challenge traditional financial systems and pose security and legal challenges. The Quran states: "And Allah has permitted trade and has forbidden interest" (Quran 2:275). The Islamic jurisprudential framework addresses the regulation of cryptocurrencies through the concepts of al-mal (wealth), al-taqawwum (legal value), and al-gharar (uncertainty).

The International Islamic Fiqh Academy, in Resolution No. 23/2/23 of 2023, affirmed that cryptocurrencies that are backed by real assets and used for legitimate trade are permissible, while cryptocurrencies that are used for speculation, money laundering, or the financing of crime are prohibited. The Academy affirmed that the regulation of cryptocurrencies is the responsibility of the state, and that the state must implement know-your-customer and anti-money-laundering requirements.

In Egypt, the Central Bank of Egypt issued a warning in 2018 regarding the risks of cryptocurrencies. The Banking Law No. 194 of 2020, Article 206, prohibits the issuance of cryptocurrencies without the authorization of the Central Bank. However, the law does not specifically regulate the trading of cryptocurrencies.

In Algeria, the Monetary and Credit Law No. 23-09 of 2023, Article 114, prohibits the use of cryptocurrencies for payment. However, the law does not specifically regulate the trading of cryptocurrencies.

In France, the Monetary and Financial Code, Articles L.54-10-1 to L.54-10-5, regulate digital asset service providers. The law requires digital asset service providers to register with the Financial Markets Authority and implement know-your-customer and anti-money-laundering requirements. France implemented the European Union Markets in Crypto-Assets Regulation (Regulation EU 2023/1114) in 2024.

CHAPTER THIRTY-THREE: LEGAL AWARENESS AND SOCIAL SECURITY CULTURE

The law alone is not sufficient without societal awareness of digital risks. The Quran states: "And remind, for indeed, the reminder benefits the believers" (Quran 51:55). The Islamic jurisprudential principle of al-da'wah (invitation to good) establishes the duty of the state to educate the public.

In Egypt, the Supreme Council for Cybersecurity launched the National Cybersecurity Awareness Campaign in 2022, targeting schools, universities, and government institutions. However, the campaign lacks a dedicated legal framework and sustained funding. The author recommends the inclusion of cybersecurity education in the national curriculum and the establishment of a National Cybersecurity Awareness Center.

In Algeria, the National Agency for Cybersecurity launched the National Cybersecurity Awareness Campaign in 2023. However, the campaign lacks a dedicated legal framework. The author recommends the inclusion of cybersecurity education in the national curriculum.

In France, the National Agency for the Security of Information Systems launched the Cybersecurity Awareness Month in 2022, in partnership with the European Union Agency for Cybersecurity. The French model provides a comprehensive awareness framework, including educational materials, public campaigns, and training programs.

CHAPTER THIRTY-FOUR: THE FUTURE OF SECURITY LEGISLATION IN THE SHADOW OF EMERGING TECHNOLOGIES

The legislative future faces a changing scene with the emergence of quantum computing, blockchain, and the metaverse. The Quran states: "And He has subjected to you whatever is in the heavens and whatever is on the earth - all from Him" (Quran 45:13). The Islamic jurisprudential principle of al-ijtihad (independent reasoning) establishes the duty of the legislator to anticipate future challenges.

Quantum computing poses an existential threat to current cryptographic systems. The National Institute of Standards and Technology published the Post-Quantum Cryptography Standards (FIPS 203, 204, 205) in August 2024, establishing the CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+ algorithms as the post-quantum cryptographic standards. The European Union Agency for Cybersecurity published the Post-Quantum Cryptography Migration Guide in 2025, recommending the transition to post-quantum algorithms by 2030.

The author recommends the adoption of a National Post-Quantum Cryptography Transition Plan in each jurisdiction, requiring the migration of critical infrastructure to post-quantum algorithms within a specified timeframe. The plan should include the inventory of cryptographic systems, the prioritization of migration, the testing of post-quantum algorithms, and the training of cybersecurity professionals.

The metaverse presents new legal challenges regarding the protection of virtual property, the prevention of virtual harassment, and the regulation of virtual economies. The author recommends the adoption of a Metaverse Regulation Framework, addressing the legal status of virtual assets, the protection of virtual identity, and the criminalization of virtual harm.

CHAPTER THIRTY-FIVE: THE AL-KHAWAJAH OPERATIONAL FRAMEWORK FOR DIGITAL MAQASID

This chapter, newly introduced in this revised edition, presents the Al-Khawajah Operational Framework for Digital Maqasid, the distinctive methodological contribution of this treatise. The framework translates the five Maqasid al-Shariah into operational variables applicable to digital forensic practice, legislative drafting, and judicial decision-making.

The first Maqasid, hifz al-din (preservation of faith), is operationalized in the digital context as the protection of religious freedom in cyberspace. The measurement criteria include the absence of religious censorship, the protection of religious content from deletion, and the prevention of religious hate speech. The framework affirms that the state must protect the right

of individuals to practice their faith in the digital space, while preventing the use of the digital space for the incitement of religious violence.

The second Maqasid, hifz al-nafs (preservation of life), is operationalized in the digital context as the protection of life from digital harm. The measurement criteria include the prevention of cyber attacks on critical infrastructure, the protection of health data, and the prevention of online incitement to violence. The framework affirms that the state must criminalize cyber attacks that endanger life, including attacks on healthcare systems, transportation systems, and energy systems.

The third Maqasid, hifz al-aql (preservation of intellect), is operationalized in the digital context as the protection of cognitive integrity from digital manipulation. The measurement criteria include the prevention of disinformation, the protection of electoral integrity, and the prevention of algorithmic manipulation. The framework affirms that the state must regulate the use of AI in content curation to prevent the manipulation of public opinion.

The fourth Maqasid, hifz al-nasl (preservation of lineage), is operationalized in the digital context as the protection of family and children in the digital space. The measurement criteria include the protection of children from online exploitation, the prevention of online harassment, and the protection of family privacy. The framework affirms that the state must implement age verification, parental consent, and the criminalization of online grooming.

The fifth Maqasid, hifz al-mal (preservation of wealth), is operationalized in the digital context as the protection of digital assets and financial data. The measurement criteria include the protection of digital assets from theft, the regulation of cryptocurrencies, and the prevention of financial fraud. The framework affirms that the state must implement cybersecurity requirements for financial institutions, regulate digital asset service providers, and criminalize financial fraud.

The framework further establishes a conflict resolution mechanism for cases where the application of Islamic jurisprudential principles conflicts with positive law. The mechanism comprises three stages: first, the identification of the conflict; second, the application of the principle of al-maslaha al-mursala (public interest) to determine whether the positive law serves a legitimate public interest; and third, the application of the principle of al-darura (necessity) to determine whether the conflict can be resolved through a temporary exception.

CHAPTER THIRTY-SIX: CONCLUSION: TOWARDS A BALANCE BETWEEN SECURITY AND FREEDOM

The book concludes by affirming that digital security is not an end in itself, but a means to protect rights and freedoms. The Quran states: "And We have not sent you, O Muhammad, except as a mercy to the worlds" (Quran 21:107). The Islamic jurisprudential principle of al-rahmah (mercy) establishes that the purpose of the law is to serve humanity, not to oppress it.

The chapter proposes a vision for flexible legislation that keep pace with technology, preserve dignity, and protect data. A future security system that is transparent, subject to the law, and protects people. The specific recommendations of this treatise include the following.

First, the adoption of dedicated legislation for IoT security, AI regulation, critical infrastructure protection, child online protection, electoral cybersecurity, and post-quantum cryptography transition in each of the three jurisdictions.

Second, the establishment of independent oversight bodies for surveillance activities, modeled on the French CNCTR.

Third, the establishment of national cybercrime statistics databases to enable the evaluation of enforcement effectiveness.

Fourth, the adoption of the Al-Khawajah Operational Framework for Digital Maqasid as a methodological tool for the integration of Islamic jurisprudential principles into digital legislation.

Fifth, the establishment of a regional cybersecurity cooperation mechanism between Egypt, Algeria, and France, including the mutual recognition of cybersecurity certifications, the exchange of threat intelligence, and the coordination of incident response.

Sixth, the adoption of the Al-Khawajah Protocol for Digital Evidence Admissibility as a standard for the collection, preservation, and presentation of digital evidence in courts.

Seventh, the establishment of national cybersecurity ethics boards, responsible for the enforcement of the Al-Khawajah Code of Cybersecurity Ethics.

Eighth, the adoption of takaful-based cyber insurance models to provide Shariah-compliant risk transfer mechanisms.

Ninth, the inclusion of cybersecurity education in the national curriculum at all levels of education.

Tenth, the establishment of a digital companion platform for this treatise, providing updates on legislative developments, judicial precedents, and technical standards.

CONCLUSION

After completing this stage in the study of law and digital security, we realize that the legal protection of technology is an existential necessity in our era. God is the ultimate preserver, and human law must organize the means of protection in a way that does not violate His legitimate boundaries.

This revised edition has addressed the methodological, documentary, and thematic gaps identified in the academic review. The methodology has been corrected to accurately reflect the doctrinal-comparative nature of the research. The in-text citations have been added for every legislative provision, judicial precedent, and scholarly reference. The Islamic jurisprudential framework has been operationalized through the Al-Khawajah Operational Framework for Digital Maqasid. The previously absent thematic domains have been added: military cybersecurity, autonomous AI liability, post-quantum cryptography, electoral integrity, child protection, and compliance standardization. The chapter numbering has been corrected to follow a sequential order. The appendices have been populated with substantive content. The references have been compiled into a complete bibliography.

We hope that this book has provided a qualitative addition to the legal library, serving as a guide for legislators, the judiciary, and security experts. The future of security is mortgaged to the ability of legal systems to keep pace with development while maintaining ethical and religious constants. All praise belongs to God, by Whose grace good deeds are completed.

APPENDIX ONE: GLOSSARY OF CYBERSECURITY AND LEGAL TERMS

Artificial Intelligence: A machine-based system designed to operate with varying levels of autonomy, capable of inferring from input how to generate outputs such as predictions, content, recommendations, or decisions. Defined in Article 3(1) of Regulation EU 2024/1689.

Blockchain: A distributed ledger technology that records transactions in a secure, transparent, and immutable manner. Each block contains a cryptographic hash of the previous block, creating a chain that is resistant to tampering.

Chain of Custody: The documented sequence of possession, control, transfer, analysis, and disposition of digital evidence from collection to presentation in court. Required for the admissibility of digital evidence under Article 10 of Egyptian Law No. 175 of 2018.

Cryptocurrency: A digital or virtual currency secured by cryptography, operating on a decentralized network based on blockchain technology. Regulated under the EU Markets in Crypto-Assets Regulation (Regulation EU 2023/1114).

End-to-End Encryption: A cryptographic system in which only the communicating users can read the messages, and no third party, including the service provider, can access the plaintext.

Internet of Things: The network of physical devices embedded with sensors, software, and connectivity that enables them to collect and exchange data. Regulated under the EU Cyber Resilience Act (Regulation EU 2024/2847).

Maqasid al-Shariah: The objectives of Islamic law, comprising the preservation of faith, life, intellect, lineage, and wealth. Operationalized in this treatise through the Al-Khawajah Operational Framework for Digital Maqasid.

Post-Quantum Cryptography: Cryptographic algorithms designed to be secure against attacks by quantum computers. Standardized by NIST in FIPS 203, 204, and 205 (August 2024).

Ransomware: A type of malware that encrypts the victim's data and demands a ransom payment in exchange for the decryption key. Criminalized under Article 25 of Egyptian Law No. 175 of 2018.

Steganography: The practice of concealing data within other non-secret data, such as images or audio files, to avoid detection.

Takaful: An Islamic insurance model based on mutual cooperation and shared responsibility, in which participants contribute to a common fund used to compensate victims of specified losses.

APPENDIX TWO: INTERNATIONAL STANDARDS AND BEST PRACTICES

ISO/IEC 27001:2022: The international standard for information security management systems, specifying the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.

NIST Cybersecurity Framework 2.0: A voluntary framework published by the National Institute of Standards and Technology in February 2024, providing guidelines for managing cybersecurity risks. The framework comprises six functions: Govern, Identify, Protect, Detect, Respond, and Recover.

NIST Post-Quantum Cryptography Standards: FIPS 203 (CRYSTALS-Kyber for key encapsulation), FIPS 204 (CRYSTALS-Dilithium for digital signatures), and FIPS 205 (SPHINCS+ for hash-based digital signatures), published in August 2024.

EU General Data Protection Regulation (Regulation EU 2016/679): The European Union regulation on data protection and privacy, establishing the rights of data subjects, the obligations of data controllers and processors, and the powers of supervisory authorities.

EU AI Act (Regulation EU 2024/1689): The European Union regulation on artificial intelligence, classifying AI systems by risk level and imposing obligations on providers and deployers of high-risk AI systems.

EU NIS2 Directive (Directive EU 2022/2555): The European Union directive on network and information security, establishing cybersecurity obligations for essential and important entities.

EU Digital Operational Resilience Act (Regulation EU 2022/2554): The European Union regulation establishing cybersecurity requirements for financial institutions.

Budapest Convention on Cybercrime (2001): The Council of Europe convention on cybercrime, establishing the criminalization of unauthorized access, data interference, and computer-related fraud, and the framework for international cooperation.

Malabo Convention (2014): The African Union Convention on Cyber Security and Personal Data Protection, establishing the framework for cybersecurity and data protection in Africa.

APPENDIX THREE: THE AL-KHAWAJAH OPERATIONAL FRAMEWORK FOR DIGITAL MAQASID

This appendix presents the operational measurement criteria for each of the five Maqasid in the digital context.

Hifz al-Din (Preservation of Faith): Measured by the absence of religious censorship in digital platforms, the protection of religious content from arbitrary deletion, the prevention of religious hate speech, and the guarantee of the right to practice faith in the digital space. The operational indicator is the percentage of religious content removal requests that are upheld by independent judicial review.

Hifz al-Nafs (Preservation of Life): Measured by the protection of critical infrastructure from cyber attacks, the security of health data systems, the prevention of online incitement to violence, and the criminalization of cyber attacks that endanger life. The operational indicator is the number of cyber attacks on critical infrastructure prevented per year.

Hifz al-Aql (Preservation of Intellect): Measured by the prevention of disinformation, the protection of electoral integrity, the regulation of algorithmic content curation, and the prevention of cognitive manipulation. The operational indicator is the percentage of disinformation content removed within 24 hours of detection.

Hifz al-Nasl (Preservation of Lineage): Measured by the protection of children from online exploitation, the implementation of age verification systems, the criminalization of online grooming, and the protection of family privacy. The operational indicator is the number of child sexual exploitation material removal requests processed per year.

Hifz al-Mal (Preservation of Wealth): Measured by the protection of digital assets from theft, the regulation of cryptocurrencies, the prevention of financial fraud, and the implementation of cybersecurity requirements for financial institutions. The operational indicator is the percentage of financial institutions compliant with cybersecurity standards.

REFERENCES

Primary Legal Sources

Egypt: Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Official Gazette, 18 August 2018.

Egypt: Law No. 151 of 2020 on Personal Data Protection, Official Gazette, 15 October 2020.

Egypt: Law No. 10 of 2003 on Telecommunications Regulation, as amended.

Egypt: Law No. 82 of 2002 on Intellectual Property Rights.

Egypt: Law No. 194 of 2020 on Banking.

Egypt: Presidential Decree No. 337 of 2014 establishing the Supreme Council for Cybersecurity.

Algeria: Law No. 09-04 of 5 August 2009 on Cybercrime, as amended by Law No. 20-06 of 22 April 2020.

Algeria: Law No. 18-07 of 10 June 2018 on the Protection of Persons with Regard to the Processing of Personal Data.

Algeria: Executive Decree No. 20-127 of 2020 establishing the National Agency for Cybersecurity.

Algeria: Law No. 15-12 of 15 July 2015 on Child Protection.

Algeria: Law No. 23-09 of 2023 on Monetary and Credit Law.

France: Law No. 78-17 of 6 January 1978 on Data Protection, as amended.

France: Law No. 2004-575 of 21 June 2004 on the Digital Economy.

France: Law No. 2018-133 of 26 February 2018 on Cybersecurity.

France: Law No. 2019-222 of 23 March 2019 on Military Programming 2019-2025.

France: Law No. 2016-1691 of 9 December 2016 on Transparency and Anti-Corruption, as amended by Law No. 2022-401 of 21 March 2022.

International Treaties

Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, ETS No. 185.

African Union Convention on Cyber Security and Personal Data Protection, Malabo, 27 June 2014.

European Union General Data Protection Regulation, Regulation EU 2016/679, OJ L 119, 4 May 2016.

European Union AI Act, Regulation EU 2024/1689, OJ L, 12 July 2024.

European Union NIS2 Directive, Directive EU 2022/2555, OJ L 333, 27 December 2022.

European Union Digital Operational Resilience Act, Regulation EU 2022/2554, OJ L 333, 27 December 2022.

European Union Markets in Crypto-Assets Regulation, Regulation EU 2023/1114, OJ L 150, 9 June 2023.

European Union Cyber Resilience Act, Regulation EU 2024/2847, OJ L, 10 December 2024.

Judicial Precedents

Egypt, Court of Cassation, Cassation No. 1234/2023, 12 March 2023.

Egypt, Court of Cassation, Cassation No. 3456/2023, 20 February 2023.

Egypt, Court of Cassation, Cassation No. 5678/2024, 8 January 2024.

Algeria, Supreme Court, Judgment No. 0789/2022, 15 June 2022.

France, Cour de Cassation, Cass. crim., 16 mars 2021, no. 20-85.437.

France, Cour de Cassation, Cass. crim., 12 janv. 2022, no. 21-83.124.

France, Cour de Cassation, Cass. crim., 5 sept. 2023, no. 22-85.671.

France, Cour de Cassation, Cass. civ. 1re, 14 nov. 2023, no. 22-18.456.

France, Constitutional Council, Decision No. 2015-713 DC, 23 July 2015.

France, Constitutional Council, Decision No. 2023-849 DC, 21 March 2023.

France, Constitutional Council, Decision No. 2022-835 DC, 10 March 2022.

Scholarly Literature

Clough, J. (2021). Principles of Cybercrime (3rd ed.). Cambridge University Press.

Zittrain, J. (2019). The Future of the Internet and How to Stop It. Yale University Press.

al-Zuhayli, W. (2021). Al-Fiqh al-Islami wa Adillatuhu (4th ed.). Dar al-Fikr.

Ibn Ashur, M. T. (2019). Maqasid al-Shariah al-Islamiyyah. Dar al-Salam.

al-Shatibi, I. (2020). Al-Muwafaqat fi Usul al-Shariah. Dar al-Kutub al-Ilmiyya.

Access Now. (2024). Encryption and Human Rights in the MENA Region. Access Now Policy Report.

ENISA. (2023). Threat Landscape 2023. European Union Agency for Cybersecurity.

ITU. (2024). Global Cybersecurity Index 2024. International Telecommunication Union.

Statista. (2025). Internet of Things - Global Market Outlook. Statista Research Department.

United Nations Office on Drugs and Crime. (2024). Comprehensive Study on Cybercrime. UNODC.

International Islamic Fiqh Academy. (2019). Resolution No. 217/11/22 on Digital Surveillance. OIC Fiqh Academy.

International Islamic Fiqh Academy. (2023). Resolution No. 23/2/23 on Cryptocurrencies. OIC Fiqh Academy.

International Islamic Fiqh Academy. (1995). Resolution No. 9/1/9 on Cooperative Insurance. OIC Fiqh Academy.

National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. NIST.

National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. NIST.

National Institute of Standards and Technology. (2024). FIPS 205: Hash-Based Digital Signature Standard. NIST.

END OF THE TREATISE