

The Role of Public Law in Addressing Cybersecurity Threats to Information Security

Professor Dr. Mostafa Fazaeli ¹, Doaa Abdulameer Qasim ²

¹Professor of International Law, Faculty of Law, University of Qom , Qom, Islamic Republic of Iran

m.fazayeli@qom.ac.ir

²PhD Candidate, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran

Douaa.alamir@yahoo.com

HOW TO CITE: ABSTARCT

Mostafa Fazaeli, Doaa Abdulameer Qasim (2026). The Role of Public Law in Addressing Cybersecurity Threats to Information Security. International Journal of Special Education, 41(22s), 863-873

Amidst the rapid technological advancement and the expansive proliferation of digital information, information security has emerged as one of the most complex and critical legal and social challenges in the digital age. This study examines the conceptual and general legal framework of information security, highlighting cyber threats that endanger critical public utilities. It assesses the effectiveness of public law tools in confronting these risks through modern legislation, specialized regulatory bodies, and effective oversight mechanisms. The study also emphasizes the role of remote litigation as an innovative mechanism that enhances the speed and efficiency of legal responses, reflecting the pivotal role of public law in organizing the relationship between the state and individuals within a complex digital environment.

The research underscores that cybersecurity cannot be reduced to a purely technical issue but requires a comprehensive legal and social perspective, positioning public law as the primary framework for safeguarding the public interest and protecting fundamental digital rights. The study concludes with strategic recommendations aimed at enhancing the efficiency of legal and regulatory tools, enabling them to address the complex challenges of the digital era while maintaining a delicate balance between security and freedom, thereby reinforcing the concept of digital sovereignty and simultaneously protecting individual rights.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Keywords: Information Security, Cybersecurity, Public Law, Cyber Threats, Legal Oversight, Remote Litigation.

Introduction

The contemporary world is experiencing an unprecedented digital revolution that has

transformed daily life and imposed a new reality on both individuals and states. With the rapid shift towards electronic administration and increasing reliance on digital data, information security has

become one of the most urgent challenges. Cyberattacks are no longer isolated disruptive attempts; they have evolved into systematic threats that endanger state sovereignty, institutional stability, and the integrity of vital interests.

In this context, public law emerges as a central tool expected to confront these challenges, serving as the traditional guardian of public order and the regulator of the relationship between administrative authorities and society. Cyber threats, however, transcend geographical boundaries and classical legal constraints, operating in an open, constantly evolving space. This compels public law, including its constitutional and administrative components, to reconsider its tools and seek new mechanisms capable of addressing an exceedingly complex digital reality.

Information security protection is no longer solely a technical responsibility; it has become a shared duty between technical institutions and legal authorities. Public law, as the governing framework of the relationship between the state and society, must therefore engage directly in this struggle, necessitating updates to its rules, expansion of its functions, and development of regulatory and supervisory tools suitable for a digital environment that defies traditional legal borders.

This study analyzes the theoretical and practical interaction of public law with these digital challenges and examines its capacity to keep pace with cybersecurity threats affecting information security within state administrative structures. The research plan addresses the concepts, mechanisms, legislation, shortcomings, and potential developments.**Significance of the Study**

This study is significant because cyber threats represent one of the most prominent risks to state security in the digital age, particularly concerning information security within public institutions. Public law – through legislation and administrative

and supervisory functions – is a crucial instrument for organizing and safeguarding this digital space.

The study gains further importance because public law originally developed within a traditional framework based on sovereignty and public service principles, while cyber threats emerge in a dynamic, borderless environment that is difficult to regulate under classical legal frameworks. Understanding how public law adapts to such threats and keeps pace with rapid digital transformations represents a meaningful contribution to bridging the existing knowledge gap in this area. The study also highlights the urgent need for updated or new legal tools that enable public authorities to efficiently protect their digital infrastructure while establishing clear accountability and oversight mechanisms to prevent failures or shortcomings in responding to cyberattacks.

The timing of this research adds to its importance, as digital attacks on state institutions are increasing, with the development of sophisticated cybercrime tools and the expanding use of technology in public service delivery. Consequently, public law serves as the first line of defense in regulating and managing this new reality.

Research Problem

With the acceleration of digital transformation in public institutions, cyber threats are no longer purely technical issues; they have become legal and regulatory challenges that directly affect administrative sovereignty and legitimacy. As the information space expands and official entities rely on electronic systems for data processing and service delivery, cyberattacks threaten not only data confidentiality but also the continuity of public utilities and the integrity of administrative decisions.

Public law, in its classical form, was established to regulate the relationship between administration and individuals and to protect public order. Today, it faces a new reality imposed by the digital environment, characterized by cross-border challenges, legislative ambiguity, and an increasing

need for flexible and effective mechanisms. The central research question thus arises:

To what extent are public law tools effective in addressing cybersecurity threats to information security, and does this branch of law possess sufficient means to protect public digital interests in light of evolving threats and shifting modalities?

Chapter One

The Conceptual and General Legal Framework for Protecting Information Security

Information security is no longer merely a technical issue; it has emerged as one of the most pressing challenges facing the institutional structures of states in the digital age. This applies both to the nature of the information being protected, the methods used to breach it, and the magnitude of damages resulting from its violation.

With the escalation of cyber threats and the development of digital crime tools, there has arisen an urgent need for a comprehensive review of the legal framework governing information security, particularly within public law. Public law bears the responsibility of protecting digital public order and safeguarding the vital interests of both individuals and the state. Understanding the nature of information security and its legal boundaries constitutes the first step in assessing the effectiveness of legal rules in preventing cyberattacks and deterring their perpetrators.

This issue intersects with technical definitions, legislative regulations, and institutional safeguards, making the need for an integrated conceptual and legal framework indispensable. Cyber threats have become a constant concern for public institutions due to their potential to infiltrate systems, disrupt operational capacities, or even target a state's infrastructure.

This chapter is divided into two main sections: the first examines the concept of "information security" in the cyber context, while the second addresses cyber threats to information security and their impact on public utilities.

Section One: The Concept of Information Security in the Cyber Context

Amidst the rapid digital transformations characterizing the contemporary world, the term "information security" has become one of the most frequently used concepts due to its direct relevance to the lives of individuals, institutions, and states. Understanding this modern concept requires tracing its linguistic roots, which illuminate its deeper meanings and fundamental conceptual structure. The term is composed of two primary elements: **"security"** and **"information,"** each bearing significant meaning in the Arabic language that informs contemporary understanding.

The word "security" in Arabic is associated with tranquility and peace, as opposed to fear¹. This meaning is referenced in multiple places in the Qur'an, such as: "[He] who feeds them against hunger and secures them from fear" [Qur'an, Surah Quraysh: 4], where security is presented as a divine blessing countering hunger and fear. Similarly, "Enter it in peace, secure" [Qur'an, Surah Al-Hijr: 46] portrays security as a state of psychological and physical safety within paradise.

Linguistic sources define security as serenity, reassurance, and the absence of worry². It represents a state in which a person is free from fear, whether regarding personal safety, property, honor, or any other interest. It encompasses both protection from danger and the guarantee of rights³. Hence, in linguistic terms, security extends beyond mere protection from tangible threats to include a sense of confidence and trust—a principle fully aligned with the modern concept of

¹ Rouhi Al-Baalbaki, Al-Mawrid Dictionary, 7th edition, Dar Al-Ilm Lilmalayin, Beirut, 1995, p. 777.

² Al-Zabidi, Murtada bin Muhammad, Taj al-Arus min Jawahir al-Qamus, edited by a group of scholars, supervised by Abd al-Sattar Ahmad Faraj, Kuwait:

Ministry of Awqaf and Islamic Affairs, 1399 AH / 1979 CE, vol. 34, p. 184.

³ Ibn Manzur, Muhammad bin Makram, Lisan al-Arab, 1st edition, Dar Sader, vol. 1, Beirut, Lebanon, 2000, p. 163.

information security, which involves not only preventing threats but also fostering digital trust among individuals and institutions within electronic environments⁴.

The second component, “information,” is derived from the root *‘-l-m*, which denotes knowledge, understanding, and certainty. Linguistically, knowledge (*‘ilm*) is “grasping the reality of a matter,” while information refers to “documented or comprehended knowledge that can be communicated and understood⁵.” In modern usage, the term encompasses all forms of stored, transmitted, and utilized knowledge—whether digital or paper-based, simple or complex, private or public.

Thus, **information security** refers to a state of confidence and assurance in handling data, concerning its confidentiality, integrity, and availability—three fundamental pillars recognized in all contemporary information security theories⁶.

The technological advances of recent decades have added a new dimension to this concept: the cyber domain, which introduces the term **cybersecurity**.⁷ Originally, “cyber” referred to steering a ship, metaphorically applied to guiding and protecting digital systems from disruption or collision⁸. With the advent of the Internet, “cyber” came to signify the digital space—a non-physical environment resulting from the interconnection of devices, networks, databases, users, and automated control systems⁹.

Thus, the linguistic concept of information security, while grounded in the original meanings of “security” and “information,” has evolved in the modern context to denote advanced digital protection, leveraging artificial intelligence, behavioral analytics, preventive systems, and closely tied to national sovereignty and public policy.

This conceptual expansion has influenced contemporary legislation, which increasingly recognizes that information security is not merely a technical matter but a component of national security, requiring legal intervention, strategic planning, and international cooperation. In general terms, information security can be understood as the set of technical and organizational measures designed to protect information and digital systems from unauthorized access, alteration, destruction, misuse, or disclosure. Protection encompasses multiple dimensions, including data integrity, information confidentiality, and availability when needed, making it a core element of any reliable technological infrastructure¹⁰.

Legally, however, Iraq still lacks a comprehensive codification of information security. Cybersecurity-related provisions are scattered across general penal or regulatory laws, creating gaps in addressing contemporary digital threats¹¹. Despite gradual state awareness of this field, the legislative framework remains fragmented, underdeveloped, and insufficiently monitored

⁴ M. M. Raad Khudair Salibi, “Enhancing Cybersecurity in Iraq: Challenges and Opportunities,” *International Studies Journal*, issue ninety-nine, 2024, p. 509.

⁵ See link: p. 3 – Tafsir Al-Qur’an by Osama Suleiman – Definition of Knowledge in Language and Terminology – Al-Maktaba Al-Shamela, accessed 10/7/2025.

⁶ Mohammad Al-Saeed Khashabah, *Management Information Systems*, University Publishing House, Cairo, 2008, p. 22.

⁷ See the following link: Information Security: Concept, Importance, and Components, accessed 11/7/2025.

⁸ The term “Cyber” is derived from the Greek word “Kybernetes,” which means “helmsman” or “navigator.”

⁹ Shaban, Abdul Aati Atiya, et al., *Al-Mu’jam Al-Waseet*, 4th edition, Al-Shorouk International Office, “Arabic Language Academy”, Egypt, 2004, p. 28.

¹⁰ J. Radwan, “Cybersecurity: A Priority in Defense Strategies,” *Al-Jaish Journal*, Military Publications Foundation, Algeria, issue 603, January, 234, p. 14.

¹¹ Ahmad Abis Nema Al-Fatlawi, “Cyber Attacks: Their Concept and the Arising International Responsibility in Light of Contemporary International Regulation,” *Al-Muhaqqiq Al-Hilli Journal of Legal and Political Sciences*, vol. 8, no. 4, College of Law, University of Babylon, Iraq, 2016, p. 616.

against cyber risks. This highlights the urgent need for specialized legislation that clearly defines information security, identifies the elements of cybercrime, delineates the responsibilities of public and private entities, and establishes mechanisms for oversight, monitoring, and rapid response. Such legislation must be comprehensive and flexible, keeping pace with rapid developments in digital crime and enhancing deterrence and prevention mechanisms.

Iraq faces real challenges in implementing legal protection for information security, including low cybersecurity awareness among public institution employees, limited specialized personnel, and underdeveloped IT infrastructure with vulnerabilities that hinder advanced protective measures. Nevertheless, there are opportunities to improve information security in Iraq through international best practices, collaboration with specialized organizations offering support and expertise, and developing national capacities—creating a national front capable of safeguarding Iraq's digital space.¹²

Section Two: Cyber Threats to Information Security and Their Impact on Public Utilities

In recent decades, the world has undergone a comprehensive digital transformation reshaping daily life. Computers and the Internet have become essential elements in social and economic structures, as well as in managing the affairs of individuals and institutions alike. The impact of this transformation extends beyond individual or institutional transactions, affecting the deep structures of government and public administration. Reliance on digital systems and information infrastructure has become the norm in operating public utilities, delivering services,

making decisions, and safeguarding sovereign data.

However, this broad engagement with the digital space brings with it novel, unconventional, cross-border, and often invisible risks, now collectively referred to as **cyber threats**. The severity of these threats has increased with greater dependence on information and communication technologies. They are no longer theoretical possibilities or isolated incidents but a daily reality that threatens the stability of information systems, the integrity of data, the continuity of public services, and even state security itself.

Cyberattacks increasingly target critical state resources and information infrastructure. Their objectives have expanded beyond simple device damage or service disruption to include theft, espionage, distortion, and systematic sabotage of state digital systems. Sensitive public institutions in sectors such as security, energy, education, health, and finance have been affected, making **information security** an integral component of national security.¹³

Cyber threats can be classified into three main categories based on their targets, each revealing the nature of risks and potential vulnerabilities:¹⁴

1. Threats targeting computer hardware and software components

Computer components—whether tangible hardware or intangible digital systems—are primary targets for cyberattacks, especially with increasing institutional and administrative reliance on technological infrastructure for managing public utilities and sensitive data. Attackers aim to paralyze devices and systems, denying institutions the ability to perform essential functions. Threats to physical components include attempts to disable or destroy input units (keyboards,

¹² Mustafa Ibrahim Salman Al-Shammari, "Cybersecurity and Its Impact on Iraqi National Security," *Journal of Legal and Political Sciences*, College of Law and Political Sciences, University of Diyala, vol. 10, no. 1, 2021, p. 152.

¹³ Zahraa Emad Muhammad Kalantar, "Adapting Cyber Attacks under International Law," *Al-Kufa*

Journal of Legal and Political Sciences, vol. 1, no. 1/44, 2020, p. 52.

¹⁴ Rizk Ahmad Samudi, "The Right to Self-Defense as a Result of Cyberattacks under International Public Law Rules," *University of Sharjah Journal of Legal Sciences*, vol. 15, no. 2, December 2018, p. 346.

scanners), output units (monitors, printers), and storage media (hard drives, USB drives), which house institutional databases, communications, and official documents. Damage to these components can paralyze public services or disrupt critical service delivery.

Even more critical are threats targeting intangible components, the core of computer operations, including software, operating systems, databases, and stored or transmitted information¹⁵. Such attacks are difficult to detect and contain and often employ complex tools such as **malware**, including **ransomware**, which encrypts sensitive files and demands payment—usually in digital currency—for decryption. When public utility systems are targeted, the consequences can include institutional crises, as seen in several countries where hospitals, ports, or fuel distribution networks were incapacitated for hours or days due to similar breaches¹⁶.

Loss of devices or data extends beyond technical disruption to sovereign dimensions, particularly when stolen information pertains to security ministries, intelligence institutions, national security files, or diplomatic affairs. Any technical malfunction or data loss may threaten the public interest, hinder public services, and undermine citizen trust. Public law in many countries, including Iraq, remains inadequately prepared to address these complex crimes. While hackers' tools evolve rapidly, legal and procedural protections respond slowly, leaving space for extensive damage without clear statutory deterrence or defined responsibility for public entities.

2. Threats targeting networks and information infrastructure

With the accelerated digitization of administrative work and the expanded use of internal and external networks in operating state utilities,

information infrastructure—especially communication and data exchange networks—has become a vital link connecting various governmental entities, from central ministries to field offices. Increasing reliance on digital networks exposes them to complex cyberattacks that threaten operational capacity, data integrity, and service reliability.

These threats manifest in offensive actions targeting the state's network infrastructure, taking various forms, such as disrupting servers or overloading them through¹⁷ **Distributed Denial of Service (DDoS) attacks**, which flood the network with a stream of false requests, thereby slowing its operation or causing complete shutdown. Such attacks often specifically target government websites providing direct services to citizens, such as birth registration systems, identity issuance platforms, or tax services, which practically leads to widespread administrative paralysis and disruption of public service delivery.

Third: Threats Targeting Digital Data and Information

At the heart of the digital revolution affecting public institutions, digital data and information constitute the most valuable and vulnerable assets for cyber attackers. This information—including official documents, administrative transactions, citizen data, and governmental correspondence—forms the vital material upon which policies are built, public affairs are managed, and decisions are made. Therefore, any threat targeting this data is, in essence, a direct threat to the administrative and sovereign security of the state.

Chapter Two

The Effectiveness of Public Law Tools in Countering Cyber Threats

¹⁵ Mohammed Al-Eidani, "Cyber Threats and Information Crimes," *Al-Ijtihad Journal for Legal and Economic Studies*, vol. 13, no. 01, 2024, p. 20.

¹⁶ Israa Sharif Jijan, "Chinese Cybersecurity: A Study in Motives and Challenges," *Political Issues Journal*, issue 56, p. 35.

¹⁷ Ibrahim Ahmad Abd Al-Samurai, "Cybercrime in International Law," *Cihan University Erbil Journal of Humanities and Social Sciences*, vol. 6, no. 2, 2022, p. 146.

With the increasing reliance on technology across all aspects of life, **public law** plays a pivotal role in establishing legal and regulatory frameworks that protect the cyber domain from complex and evolving threats. The effectiveness of these legal tools, however, extends beyond enacting legislation; it also depends on their practical application, monitoring, and utilization of modern technologies that enhance enforcement efficiency, such as **remote litigation mechanisms**.

This chapter aims to examine the effectiveness of public law tools in countering cyber threats through two primary sections. The first section focuses on the role of public law in regulating and protecting cybersecurity, highlighting available mechanisms and the challenges of implementation, with the Iraqi experience presented as a contemporary example. The second section addresses **remote litigation** as a modern mechanism that enhances the effectiveness of public law, allowing rapid response and flexibility in confronting cyber risks by facilitating access to justice and ensuring effective judicial oversight in a dynamic digital environment.

Section One: Public Law and Cybersecurity Protection – Mechanisms and Challenges

In the digital age, public law is no longer merely a traditional framework regulating the relationship between the individual and the state or controlling the operation of public institutions according to legality and public interest. It now faces a complex challenge imposed by technological breakthroughs and cyber transformations permeating the core of modern social, economic, and administrative structures. The concept of “security,” especially in its cyber form, can no longer be addressed in isolation from fundamental legal-philosophical questions regarding the individual’s position vis-à-vis the state, the limits of authority, and the extent to which individual

freedoms may be sacrificed to maintain public order¹⁸.

The essence of public law, in its original principle, stems from the idea of **the general will**, embodied in rules that regulate communal life, balance rights and freedoms, and uphold state sovereignty as the sole guarantor of security and stability. However, this balance is challenged when cybersecurity enters the equation. Cybersecurity is not confined to the physical realm; it encompasses the informational domain—the space of data, communications, and digital information—where private and public, individual and collective, civil and political interests intersect. This raises a complex legal and philosophical question: does the state have the right to impose strict legislative and regulatory measures to ensure its digital security, even at the expense of individual freedoms in cyberspace?

If public law serves as the state’s tool to regulate public affairs, does it possess sufficient flexibility and efficiency to address unconventional, dynamic, and inherently intangible threats? Does the individual remain a partner in policy formulation, or merely an object of protection and surveillance?

Addressing these questions requires understanding the dynamic relationship between “law” and “security.” Contemporary legal studies, particularly within the **critical security studies** framework, suggest that individual security is not necessarily achieved through increased state control, but through enhancing citizens’ ability to manage their data, protect their privacy, and participate in digital policymaking. Conversely, public law—whose legitimacy derives from the pursuit of the public good—must adapt its tools (rules, institutions, procedures) to protect the national cyber domain without becoming a repressive or overly technical instrument limiting freedoms in the name of security.¹⁹

¹⁸ Bin Arabia, Riyadh, “Asymmetric Threats in Cyberspace: Fourth-Generation Warfare as a Model,” *Scientific Research Notebooks*, vol. 10, no. 1, 2022, p. 463.

¹⁹ Azmi Bishara, *The Question of the State: Thesis on Philosophy, Theory, and Contexts*, Doha/Beirut: Arab Center for Research and Policy Studies, 2023, pp. 167-168.

Modern states, especially in Western contexts, have developed an understanding of public law as a guardian of rights, balancing security and freedom. Yet, in diverse contexts—including Iraq and other developing countries—there remains a tension between the demands of cybersecurity and concerns about excessive digital regulation through strict penal laws or poorly supervised executive bodies. This is particularly evident in the legal ambiguity surrounding clear electronic legal dealings²⁰. Here, public law must redefine itself, not merely as an administrative tool but as a mechanism for **governing emerging risks in an open and complex digital environment**²¹.

Thus, the relationship between public law and cybersecurity is not one of subordination but of **foundational interaction**. The state cannot guarantee digital security without a robust, transparent legal framework establishing boundaries, rights, defining the scope of cyber policies, outlining the duties of competent authorities, and ensuring individual rights to oversight and accountability. Conversely, individuals cannot assert digital rights in an unregulated space characterized by technological chaos or reliance on foreign companies and global control centers.

Public law today functions as the **ethical and institutional intermediary** between security and freedom. It seeks to establish a legal infrastructure that encourages protective technologies without allowing their misuse to restrict the public domain. This requires a renewed vision that makes public law more receptive to modern cyber principles, such as the right to encryption, freedom of access

to information, personal data protection, and open governance²².

The state is now obliged—through public law mechanisms—to conceptualize **digital sovereignty**, extending beyond geographic boundaries. Achieving this requires citizen participation, legislative modernization, creation of specialized independent bodies, and integration of cyber strategies with general public policies rather than limiting them to security agencies. In this context, the Iraqi experience exemplifies structural challenges hindering the effectiveness of public law tools in cybersecurity. Despite growing official awareness of digital threats, Iraq still lacks a comprehensive national law regulating information security and cyber protection. This legal absence represents a major weakness, limiting the state's ability to organize preemptively and constraining its capacity to implement long-term preventive strategies.²³

The **draft Cybercrime Law**, which has been on the agenda for more than a decade, remains stalled in the House of Representatives without being enacted, leaving the cyber environment exposed to legal and technical chaos and weakening legal deterrence against cybercrimes. Likewise, there is a notable absence of an independent **national cybersecurity authority**, resulting in fragmented and limited institutional coordination. Existing initiatives, such as the **Rapid Response Team** under the National Security Advisory, lack legal independence and face challenges related to efficiency, resources, and institutional legitimacy.

At the organizational level, the state's digital infrastructure suffers from dependence on foreign

²⁰ Faiz Muhammad Hussein, *Philosophy of Law*, University Publishing House, Cairo, 2007, p. 13.

²¹ For example, the Iraqi legislator in Article 88 of the Civil Code No. 40 of 1951 allowed the use of technological means: "A contract (by telephone) or by any similar method shall be considered as made between those present in terms of time and between absentees in terms of place." The legislator also allowed judges to benefit from scientific advancements—without limitation—in deriving judicial evidence, as clarified in Article 104 of the Evidence Law No. 107 of 1979: "The judge may

benefit from scientific advancements in deriving judicial evidence."

²² Othman Salman Gilan Al-Aboudi, *The Impact of Electronic Development on Principles of Public Function*, 1st edition, Publisher: Sabah Sadiq Jaafar Al-Anbari, Baghdad, 2011, p. 7.

²³ Tariq bin Abdullah bin Saleh Al-Omr, *Electronic Litigation Rulings*, PhD dissertation in Comparative Jurisprudence, Imam Muhammad bin Saud Islamic University – High Institute of Judiciary, Department of Comparative Jurisprudence, 1430 AH, p. 2.

systems and networks and weak sovereign infrastructure, complicating protection efforts and exposing cyber sovereignty to external interference. Moreover, the local private sector and state institutions still lack comprehensive technical awareness regarding the nature of digital threats, which further exacerbates the vulnerability of the digital environment and reduces the ability to respond promptly to attacks.²⁴

Section Two: The Role of Remote Litigation in Enhancing the Effectiveness of Public Law in Addressing Cyber Challenges

In pursuit of modernizing administrative and judicial systems to meet the demands of the digital age, new institutional practices have emerged that go beyond providing online administrative services to deeply influencing judicial work itself. Among these practices, **remote litigation** has become prominent, introducing a novel legal and technical reality where public service intersects with the digital environment, intertwining the right to litigation with cyber challenges²⁵.

Judicial facilities are among the most critical public institutions linked to individuals' rights and welfare, requiring a high level of security and reliability. As these facilities transition to digital modes, they become increasingly susceptible to threats such as attacks on judicial infrastructure, document leaks, session disruption, or impersonation of parties involved. The risk is heightened in sensitive cases, such as criminal cases, administrative disputes, or matters affecting national security or public order.

In this context, remote litigation raises fundamental public law issues concerning **legitimacy, fair trial guarantees, and oversight of public institutions**. The state, as a sovereign entity, is constitutionally obliged to provide a judicial system that ensures judicial impartiality, defense rights, data confidentiality, and procedural integrity. These principles may be undermined by electronic vulnerabilities or system malfunctions, which imposes a heightened responsibility on public administration and the legislature to draft flexible and adaptive legal frameworks.

Judicial work is no longer confined to courtroom halls; it is now conducted partially or entirely through digital media, including **audio-visual sessions, online platforms for pleadings, document exchange, and decision issuance**²⁶. While this transformation promises easier access to justice, shorter dispute resolution, and institutional efficiency, it simultaneously exposes the judiciary to latent digital vulnerabilities, especially in the absence of adequate legal and technical safeguards ensuring procedural integrity and fairness.

Remote litigation represents a **direct integration of a traditional public service—the judiciary—into an open and vulnerable cyber environment**, creating dual challenges: protecting individuals' privacy and participatory rights while preserving judicial authority and the legitimacy of decisions²⁷.

The importance of these challenges was amplified globally, and in Iraq specifically, by attempts to implement remote litigation during emergencies

²⁴ Mustafa Ibrahim Salman Al-Shammari, "Cybersecurity and Its Impact on Iraqi National Security," *Journal of Legal and Political Sciences*, College of Law and Political Sciences, University of Diyala, vol. 10, no. 1, 2021, p. 152.

²⁵ Bassem Ali Khisan, "Security in Cyberspace: Study of Threats and Confrontation Strategy," *College of Heritage University Journal*, Baghdad, vol. 1, no. 36, 2023, p. 23.

²⁶ Dr. Safaa Otani, "The Electronic Court: Concept and Application," published in *Damascus University Journal of Economic and Legal Sciences*, vol. 28, no. 1, 2012, p. 170.

For more information, see: Arezoo Ghazanfari; Abbas Sheikholeslami; Ali Akbar Esmaeili, "A Comparative Study of the Burden of Proof in Claims Based on Scientific Evidence in Iranian and English Law," *Iranian Journal of International and Comparative Law*, vol. 3, no. 1, 2025, pp. 181-203.

²⁷ Dr. Akram Fadel Said, "Protecting Databases from the Risks of Unauthorized Transfer and Unlawful Competition," Unpublished lectures presented to postgraduate (Master's) students, Department of Private Law, College of Law, Al-Nahrain University, Academic Year 2013–2014.

(e.g., the **COVID-19 pandemic**) or in regions with weak physical judicial infrastructure. Experiences indicate that digital infrastructure alone is insufficient without clear legal frameworks regulating it, providing safeguards against breaches, and holding public entities accountable for cyber incidents that invalidate procedures or compromise data.

Thus, remote litigation is not merely an ambitious technical experiment; it is a practical model reflecting the evolving relationship between public law and digital space risks. It raises essential questions regarding the adequacy of administrative and constitutional rules in managing this new form of judicial work, particularly in the event of cyberattacks targeting judicial infrastructure, interference in proceedings, or breaches of litigants' privacy. Remote litigation involves using **audio-visual communication technologies and electronic platforms to manage the judicial process from registration to judgment**, without requiring the physical presence of parties in courtrooms.

While this development offers clear administrative and legal benefits, it simultaneously introduces new cyber threats, particularly in environments lacking secure information systems or mature legislation governing such complex digital judicial processes. These processes involve advanced technical systems, including recording and broadcasting tools, judicial data management, digital identity verification, and session confidentiality—all potential targets for hacking, breach, or tampering.

Even though remote litigation may appear strategic during public health emergencies, natural disasters, or to enhance access to justice in remote areas, it should not be reduced to a mere technical solution. It must be **legislatively and organizationally grounded** and built upon three main pillars:

1. Clear legislation defining the scope of remote litigation, usage conditions, and legal guarantees.
2. A secure digital infrastructure protected against breaches, employing strong encryption, regular software updates, and trained technical personnel.
3. Effective judicial and administrative oversight to prevent manipulation of session content or case outcomes²⁸.

In this framework, the Iraqi experience remains at a nascent stage regarding remote litigation. Although some laws have been enacted to facilitate these procedures—such as **the Electronic Signature and Electronic Transactions Law No. 78 of 2012**, which lays the groundwork for digital transformation, and other laws permitting electronic means in contracts and commercial transactions—the judicial system still lacks a comprehensive infrastructure to enable a safe and effective transition to fully electronic litigation.

From a security standpoint, the absence of a dedicated cybersecurity law in Iraq represents a significant gap in protecting judicial data and correspondence, potentially allowing unauthorized interference in the digital judicial system, exposure of sensitive information, or influence over the course of justice. Cyber threats in this context go beyond technical sabotage; they also **undermine public trust in judicial integrity**, a matter of critical importance in a society striving to consolidate the rule of law and institutional credibility²⁹.

Conclusion

In conclusion, it is evident that **information security in the digital age** has evolved from being merely a technical issue to a complex legal and social matter that requires a sophisticated legal framework capable of responding to the rapidly evolving challenges of cyberspace. In this context,

²⁸ M. Nafi' Bahr Sultan, "Electronic Jurisdiction of Iraqi Courts," published in Tikrit University Journal of Legal and Political Sciences, no. 3, year 1, p. 16.

²⁹ Marwan Salem Al-Ali, "Strategic Challenges of Iraqi National Security under International Changes," previous reference, p. 66.

public law instruments emerge as a fundamental pillar for ensuring an effective balance between protecting cybersecurity and preserving the fundamental rights and freedoms of individuals. These instruments do not merely impose regulatory controls or organize the relationship between the state and society; they also establish the **legal and institutional framework** through which digital threats can be addressed efficiently and transparently, while safeguarding digital sovereignty and ensuring accountability and oversight. Thus, public law becomes not just a rigid set of rules enforcing order, but an integrated system that keeps pace with technological and social transformations, enhancing the state's ability to protect its security and public interests in a rapidly changing digital environment.

I. Findings

The study highlights several key findings, including:

1. The concept of information security in the digital environment extends to **technical, legal, social, and administrative dimensions**, necessitating the modernization of laws and procedures to keep pace with the multifaceted nature of cybersecurity.
2. There is a **clear legislative gap in Iraq** due to the absence of a comprehensive cybersecurity law and the weakness of independent regulatory bodies, which hampers the state's capacity to confront digital threats and protect the national cyber environment.
3. Integrating **remote litigation** into the judicial system effectively enhances the speed and efficiency of addressing cybersecurity-related cases, provided that strong legal frameworks and specialized training programs for judges and practitioners are in place.
4. Protecting **individual digital rights**, such as privacy and access to information, must be an integral part of cybersecurity strategies to prevent protective measures from turning into oppressive tools that restrict freedoms.

5. Weaknesses in **qualified human resources** and institutional coordination among relevant authorities in Iraq negatively affect the effectiveness of public law instruments in countering cyber threats, highlighting the need to strengthen institutional and human capacities.

II. Recommendations

Based on the study, the following recommendations are proposed:

1. **Enact a comprehensive cybersecurity law** that keeps pace with technological developments and establishes principles for protecting digital rights, while clearly defining the mandates and powers of competent authorities.
2. **Establish independent regulatory bodies** with clear authority and sufficient resources to manage national cybersecurity, ensuring effective coordination between various governmental and private entities.
3. **Develop and operationalize remote litigation mechanisms** in cybersecurity cases through supportive legislation and continuous training programs for judges and judicial staff to ensure optimal implementation.
4. **Enhance cybersecurity awareness and culture** among public employees and staff in both the public and private sectors, emphasizing the risks of cyber threats and the importance of best practices in data protection.
5. **Adopt a comprehensive national cybersecurity strategy** with clear implementation plans, measurable performance indicators, and participation from multiple governmental and societal sectors.
6. **Strengthen international cooperation** between Iraq and specialized countries or organizations in the field of cybersecurity to exchange expertise and effectively address cross-border threats, while investing in human capacity building through integration of cybersecurity in educational curricula and advanced training programs for specialized personnel to raise institutional readiness.