

Electronic Administrative Policing and Its Role in Safeguarding Public Order in Cyberspace

1. Saleem. Asouli <https://orcid.org/0009-0006-4132-8194>
Saleem.asouli@anu.edu.jo Ajloun National University – Faculty of Law – Jordan

2. SHROUQ GHALEB M.Y ALSHAMAILAH

A doctoral student at the University of Jordan

salshamayleh@yahoo.com

1764-6745-0006-0009

3. Ahmad Al-Sarayrah

<https://orcid.org/0009-0009-3553-1075>

A.sarayrah@anu.edu.jo

Ajloun National University – Faculty of Law – Jordan

4 . NASHAT BANI HAMAD

Assistant Professor, Administrative Law, Faculty of Law, Irbid National University, ,
,Jordan

n.bani-hamad@inu.edu.jo

Abstract

This study aims to analyze the concept of electronic administrative policing as a contemporary development of the administrative policing function in light of rapid digital transformation and the migration of threats to public order into cyberspace. The study argues that, despite differing from traditional administrative policing in terms of technological tools and scope of application, electronic administrative policing retains its fundamental preventive function of safeguarding public order and preventing disturbances before they occur. Adopting an analytical legal approach, the research examines the legal framework governing electronic administrative policing, including cybercrime legislation, personal data protection regulations, and rules issued by competent regulatory authorities. Particular emphasis is placed on the challenge of balancing the expansion of administrative discretionary powers with the protection of digital rights and fundamental freedoms. The study further explores the legal and technical characteristics of electronic administrative policing, highlighting its preventive nature, its subjection to the principle of legality, and its reliance on advanced technological instruments such as electronic surveillance systems, artificial intelligence technologies, data analytics, encryption mechanisms, and digital content blocking measures. It also analyzes legal and technical responses to digital violations, including early warning mechanisms, content removal, account suspension, financial penalties, and the potential combination of administrative and criminal liability where necessary. The study concludes by addressing mechanisms for implementing international responsibility arising from unlawful acts in cyberspace, including compensation, restitution, guarantees of non-repetition, international sanctions, mediation, and arbitration, thereby contributing to strengthening the legal governance of the digital environment.

Control. Public Order. Digital Transformation. Electronic administrative: **Keywords**
Digital Spacs.

Introduction

The world today is witnessing a wide wave of digital transformation, which has led to the emergence of new behavioral patterns and risks within the cyberspace. This has compelled public administration to develop its tools and methods to preserve public order. Traditional administrative control alone is no longer sufficient to address challenges arising from cybercrimes, data breaches, the dissemination of illegal content, or threats to cybersecurity, creating a pressing need to establish an Electronic Administrative Control system as a modern extension of administrative powers in the digital domain.

This study aims to clarify the concept of electronic administrative control, outline its legal basis, and examine its legal and technical characteristics. It also highlights the mechanisms used by public authorities to monitor digital activities and curb electronic violations. Furthermore, the research addresses the remedial and punitive measures adopted in response to transgressions within cyberspace, as well as the mechanisms for enforcing international responsibility when unlawful acts have cross-border effects. Accordingly, this study seeks to provide a comprehensive framework for understanding the role of electronic administrative control as one of the most important tools for protecting digital security and public order amid rapid technological development.

Research Problem

The rapid digital transformations and the expanding scope of online activities have given rise to new challenges affecting public order within cyberspace. This has compelled public administration to develop control mechanisms different from traditional ones, while simultaneously safeguarding individuals' digital rights and freedoms. Despite the existence of multiple legislations and technical tools governing this domain, the scope of administrative practice in electronic administrative control, the nature of its instruments, and the extent of its legality continue to raise numerous legal and practical issues, particularly given the intangible nature of digital activity and the widespread incidence of cybercrimes.

Accordingly, the main research problem can be formulated as follows:

To what extent does electronic administrative control enable public administration to protect public order in cyberspace, and what are the legal limits and effectiveness of such control within the governing legal and technical frameworks, without infringing upon individuals' digital rights and freedoms?

Research Questions

- 1 . What is the legal framework on which public administration relies in exercising electronic administrative control within cyberspace?
- 2 . What are the main technical and legal characteristics of electronic administrative control, and how effective is it in addressing digital violations?
- 3 . How can a balance be achieved between protecting public order in the digital space and safeguarding individuals' digital rights and freedoms?

Significance of the Study

This study is significant as it addresses a contemporary topic, namely electronic administrative control, which has become an urgent necessity in light of digital advancement and the proliferation of cybercrimes. The study highlights the legal foundations of this form of control, demonstrates the extent to which public administration can protect public order in cyberspace, and ensures the preservation of individuals' digital rights and freedoms. Moreover, the research contributes to

understanding the interplay between modern technical tools and the legal powers granted to administrative authorities, thereby supporting a balanced approach to regulating and protecting the digital environment.

Research Objectives

- 1 . To define the legal framework of electronic administrative control and clarify the legislative and regulatory foundations upon which public administration relies to organize cyberspace and safeguard public digital order.
- 2 . To analyze the technical and legal characteristics and mechanisms used by public administration in exercising electronic administrative control, and to evaluate their effectiveness in countering violations and cybercrime activities.
- 3 . To assess the balance between administrative authority in electronic control and the protection of digital rights and freedoms, leading to a deeper understanding of how effective control can be achieved without infringing upon individuals' rights within the digital environment.

Study Delimitations

- 1 . Temporal Delimitation: The study focuses on the legal and technical development of electronic administrative control in Jordan, particularly following the enactment of the Cybercrime Law of 2015 and its amendments, as well as the Personal Data Protection Law of 2023.
- 2 . Spatial Delimitation: The study is confined to the Hashemite Kingdom of Jordan, as the legal and institutional framework within which the rules of electronic administrative control are applied.
- 3 . Subject Delimitation: The study is limited to the concept, legal basis, characteristics, and technical and legal mechanisms of electronic administrative control, along with its effectiveness in protecting public digital order without violating individuals' digital rights and freedoms.

Research Methodology

This research adopts a descriptive-analytical methodology by describing the legal framework of electronic administrative control and analyzing the relevant texts and legislation, particularly the Cybercrime Law and the Personal Data Protection Law.

The study also employs a comparative approach, comparing selected legal systems and international experiences in electronic control to highlight the extent to which Jordanian legislation aligns with modern practices.

Given the technical nature of the topic, a technical-analytical approach is utilized to examine the electronic tools and mechanisms used by administration to monitor cyberspace, such as surveillance systems, blocking mechanisms, and encryption.

By combining these methodologies, the research aims to provide a comprehensive analysis clarifying the effectiveness of electronic administrative control and its legal boundaries in protecting public order within the digital environment.

By combining these methodologies, the research aims to provide a comprehensive analysis clarifying the effectiveness of electronic administrative control and its legal boundaries in protecting public order within the digital environment.

Study Terms

- 1 . Electronic Administrative Control: A set of legal and technical procedures and measures exercised by public administration to protect public order within cyberspace and to prevent potential risks or cybercrimes before they occur [1].

2 . Public Order: The state of digital stability that administration seeks to maintain in the online environment, including cybersecurity, personal data protection, and the prevention of content or activities that may disrupt digital safety [2].

3 . Digital Transformation: The application of digital tools and systems in the exercise of administrative authority, including adopting electronic information systems, intelligent data management, and cloud computing, aiming to enhance the effectiveness of administrative control and improve the ability to monitor digital activities while preserving individual rights and protecting public order [3].

4 . Digital Space: An environment in which legal and administrative rules apply to ensure the protection of public order and digital rights. It encompasses all virtual environments where digital activities can have legal consequences, such as cybercrimes, data breaches, or dissemination of illegal content [4].

Research Plan

Chapter One: Concept of Electronic Administrative Control and Its Distinction from Traditional Control

Section One: Concept and Legal Basis of Electronic Administrative Control

Section Two: Characteristics of Electronic Administrative Control

Chapter Two: Means and Methods of Electronic Administrative Control

Section One: Means of Electronic Administrative Control

Section Two: Methods of Electronic Administrative Control

Chapter One: Concept of Electronic Administrative Control and Its Distinction from Traditional Control

The world is witnessing rapid digital transformations that have exposed public administration to new activities requiring a different type of protection, leading to the emergence of electronic administrative control. This chapter aims to define the concept of this modern control, its legal basis, and characteristics, in addition to clarifying the fundamental differences between it and traditional administrative control, through the analysis of legal texts and scholarly writings.

Legal principles constitute the fundamental foundations that guide the formation, application, and interpretation of law within a state, while simultaneously upholding morality and justice within the legal order. From a theoretical perspective, legal principles are not merely abstract norms; rather, they reflect the ethical values deeply embedded in society[5]. The legislative texts regulating the system of suspension of administrative decisions are not integrated and do not cover all aspects of the system in Jordan[6]. The principle of legality is a fundamental principle of international criminal law, requiring crimes and penalties to be clearly defined by law and preventing retroactive criminalization. Article 22 of the Rome Statute expressly reflects this principle[7]. The security and safety of international civil aviation require a continuous legal process based on the development and effective implementation of legal rules, respect for international obligations, and sustained cooperation among States and international organizations[8].

Electronic administrative policing is a modern extension of traditional administrative policing, aimed at protecting public order and preventing cyber threats before they occur. Despite its reliance on advanced technologies such as electronic surveillance, artificial intelligence, and data analytics, it remains subject to the principle of legality and must balance administrative powers with the protection of digital rights and fundamental freedoms[9].

Section One: Concept and Legal Basis of Electronic Administrative Control

Defining the concept of Electronic Administrative Control constitutes a fundamental step in understanding its scope and the limits of public administration's intervention in the digital space. Accordingly, this section addresses the nature of electronic control and the legal foundations on which it relies, which regulate the administration's powers in safeguarding digital public order.

Branch One: Nature of Electronic Administrative Control

Electronic administrative control is defined as the set of procedures and measures adopted by public administration to protect public order within the digital environment, including information security, data protection, and combating cybercrimes [10].

This type of control is applied to purely digital activities conducted via the Internet, social media platforms, and smart applications, making it inherently different from traditional control, which concerns physical and tangible activities.

Electronic administrative control is primarily preventive, aiming to prevent digital violations before they occur, such as system breaches, dissemination of illegal content, or threats to digital stability [11].

It requires advanced technical means, including data tracking, network monitoring, and early detection systems, as highlighted by recent studies on the scope of electronic control in light of technological development [12].

Branch Two: Legal Basis of Electronic Administrative Control

The legal basis of electronic administrative control is grounded in a set of legislative and regulatory rules that grant public administration the authority to intervene to protect public digital order.

Foremost among these rules is the Cybercrime Law, which defines acts considered digital crimes and grants administrative authorities powers to prevent them or trace their perpetrators [13].

Electronic control also relies on the Personal Data Protection Law, which obliges public and private entities to safeguard personal information and grants administration the authority to monitor compliance [14].

In addition to legislation, regulations and directives issued by relevant administrative authorities—such as telecommunications regulators or cybersecurity units—form part of the legal basis, defining procedures for website blocking, digital content monitoring, and network protection [15].

Section Two: Characteristics of Electronic Administrative Control

The nature of electronic administrative control requires an examination of its distinctive characteristics, which combine the traditional legal nature of administrative control with the technical features imposed by the digital environment. Accordingly, this section aims to clarify the legal characteristics governing electronic control, in addition to the technical characteristics that grant it effectiveness in addressing rapidly evolving digital risks.

Branch One: The Legal Characteristics of Electronic Administrative Control

Electronic administrative control is characterised by a set of legal features that confer upon it a distinct nature differing, in certain respects, from traditional administrative control.

The first of these characteristics is its preventive nature, as electronic control seeks to prevent digital violations before they occur through proactive monitoring of electronic activities[16]. Al-Shuraida emphasised that the essence of administrative control lies

in preventing disturbances to public order, and that this essence has remained constant even after part of the control authority shifted into the digital environment[17].

Electronic administrative control is also characterised as non-punitive control, since its primary objective is to preserve digital tranquillity, information security, and the protection of electronic rights, rather than imposing criminal sanctions, which remain within the jurisdiction of the judiciary[18]. Al-Basyouni explained that administrative control, regardless of the evolution of its tools, remains preventive rather than punitive, a principle equally applicable to electronic control despite its technological form[19].

Another legal characteristic is the broad discretionary authority granted to the administration in the field of electronic control, owing to the constantly evolving nature of cyberspace and the difficulty of establishing rigid rules capable of accommodating technological developments[20]. Nevertheless, administrative authorities remain bound by the principle of legality and by the obligation to respect rights and freedoms, particularly the right to digital privacy and freedom of communication, which necessitates a careful balance between protecting electronic public order and preventing administrative abuse[21].

Electronic administrative control is further distinguished by a hybrid legislative framework, combining general legislation—such as cybercrime and personal data protection laws—with regulatory decisions issued by competent authorities. This provides significant flexibility while simultaneously requiring clarity of rules and precise determination of administrative powers[22].

Branch Two: The Technical Characteristics of Electronic Administrative Control

The digital nature of electronic administrative control imposes a range of technical characteristics that enhance its effectiveness and distinguish it from traditional administrative control.

One of the foremost characteristics is reliance on electronic monitoring systems, which enable real-time supervision of digital activities through data tracking and analysis of user behaviour within cyberspace[23]. Cybersecurity studies indicate that the effectiveness of electronic control is closely linked to the continuous and accurate collection and analysis of information[24].

Electronic administrative control also relies on artificial intelligence technologies to detect or predict digital violations. Administrative authorities increasingly employ content-analysis algorithms and machine-learning techniques to identify abnormal patterns or harmful behaviour in digital environments[25]. This enables electronic control to process vast volumes of data more efficiently than traditional control mechanisms.

Another technical feature is network integration, whereby electronic control depends on cooperation among multiple entities—such as telecommunications regulators, cybersecurity units, and digital banking institutions—through shared platforms for exchanging information regarding digital risks[26]. Such integration constitutes a fundamental element in strengthening electronic protection, particularly against transnational cybercrime.

Electronic control further involves non-traditional technical measures, including website blocking, disabling harmful online pages, and protecting databases through encryption systems and advanced firewalls[27]. Regulatory frameworks issued by competent authorities confirm that these tools form an integral part of administrative control powers in the digital environment[28].

Finally, electronic administrative control is distinguished by its capacity for immediate response to violations through early-warning technologies, real-time monitoring, and automated intervention supported by artificial intelligence, making it more effective in preventing cybercrimes before their occurrence compared with traditional control mechanisms that require longer procedural timelines[29].

Chapter Two: Means and Methods of Electronic Administrative Control

Determining the means and methods of electronic administrative control constitutes a fundamental step in understanding how administrative authorities intervene within the digital environment. These mechanisms rely on advanced technologies that enable the administration to exercise its traditional functions through innovative approaches compatible with the nature of electronic risks. This chapter therefore examines the technical and legal means employed by the administration, followed by an analysis of the preventive and remedial methods through which these powers are exercised in cyberspace.

Section One: Means of Electronic Administrative Control

The means of electronic administrative control vary between technological tools based on modern digital systems and legal instruments grounded in legislative and regulatory frameworks governing the digital sphere. This diversity reflects the significant evolution of administrative control mechanisms in the electronic environment, enhancing the administration's ability to safeguard electronic public order.

Branch One: Technical Means of Electronic Administrative Control

Administrative authorities rely on several modern technological tools to monitor, regulate, and control digital activities.

Among the most significant of these tools are electronic monitoring systems, which enable real-time tracking of data and digital activities[30]. Al-Huneiti noted that digital monitoring constitutes the cornerstone of information security, as it allows the detection of cyber intrusions or network misuse before damage occurs[31].

Artificial intelligence technologies also represent one of the most important technical tools used in electronic administrative control. Administrative bodies increasingly employ machine-learning systems to identify suspicious patterns and abnormal digital behaviour[32]. These technologies facilitate the processing of massive volumes of data that cannot be handled through traditional methods, thereby strengthening the preventive capacity of electronic control[33].

Administrative authorities further rely on encryption technologies and database protection systems as essential technical measures to ensure the security of governmental and private information, particularly data relating to citizens[29]. The Jordanian Telecommunications Regulatory Commission has affirmed that advanced encryption systems constitute a fundamental pillar in protecting electronic public order[34].

Another important technical tool is website blocking, whereby administrative authorities possess the power to disable websites that threaten digital security or publish unlawful content[35]. This mechanism is considered one of the most effective means of addressing transnational cybercrime. Additionally, early-warning systems, based on data analysis and digital risk prediction, enable administrative authorities to intervene rapidly before harm materialises[36].

Branch Two: Legal Means of Electronic Administrative Control

In exercising electronic administrative control, the administration relies upon a broad legal framework encompassing digital legislation and regulatory systems governing cyberspace.

Foremost among these are cybercrime legislations, which grant administrative authorities supervisory and regulatory powers to address unlawful digital conduct[37]. Al-Basyouni observed that the development of administrative control necessitates continuous updating of the legal framework in line with technological transformations[38].

Legislation relating to personal data protection also constitutes a fundamental legal instrument of electronic control, granting administrative authorities the power to regulate data collection, processing, and storage in a manner that preserves individual privacy and prevents misuse[39].

Administrative regulations and electronic decisions likewise play an essential role in organising cyberspace. Competent authorities issue instructions concerning website regulation, licensing conditions, cybersecurity requirements, and measures preventing misuse[40].

Legal means further include bilateral and international agreements concerning electronic information exchange, particularly in combating transnational cybercrime requiring extensive international cooperation[41]. Al-Dhafiri emphasised that technological development has compelled states to expand international cooperation within the field of digital administrative control[42].

Finally, administrative authorities possess the power to issue electronic administrative orders, such as blocking orders, decisions to close unlawful webpages, or suspension of unlicensed digital services[43].

Section Two: Methods of Electronic Administrative Control

The methods adopted by administrative authorities in the field of electronic administrative control represent one of the most significant elements reflecting the State's capacity to protect public order in its modern forms, particularly digital public order, which encompasses information security, electronic tranquillity, and respect for individual rights within the digital environment.

Electronic administrative control operates through a combination of preventive and remedial mechanisms enabling the administration either to prevent digital violations before their occurrence or to address them after they arise, consistent with the established doctrine of administrative law that the function of administrative control is prevention before repression.

Within the electronic environment, this role assumes greater complexity due to the intangible nature of cyberspace, the multiplicity of risk sources, and the rapid dissemination of unlawful acts. Consequently, advanced technical and legal methods are required to respond effectively to the challenges of the information age while ensuring compliance with cybersecurity and cybercrime legislation.

Branch One: Preventive Methods in Electronic Administrative Control

Preventive methods are founded upon the principle of averting risk before its occurrence and constitute the first line of defence relied upon by administrative authorities to safeguard digital public order. These methods include a range of measures combining technological tools with legal regulation and public awareness initiatives.

First: Proactive Monitoring of Digital Activities

Early monitoring of digital activities represents one of the most important preventive methods employed by administrative authorities, enabling the detection of potential

violations before their occurrence, whether related to network security, unlawful online content, or cyber intrusion attempts. Administrative legal scholarship indicates that such intervention derives from regulatory powers granted to protect public order under cybersecurity legislation[44].

Monitoring may take various forms, including big data analytics, suspicious-pattern recognition systems, and electronic traffic tracking, thereby ensuring early identification of digital risks.

Second: Early Warning Systems

Competent authorities rely on digital early-warning systems capable of detecting cyberattacks or abnormal activities immediately upon occurrence, allowing rapid intervention to prevent escalation of harm. Several Arab legislative frameworks have adopted this approach by granting administrative authorities the power to issue digital alerts and warnings to institutions and individuals[45].

Third: Digital Awareness and Guidance

Digital awareness constitutes an integral component of preventive administrative control, aiming to enhance cybersecurity culture among users and clarify risks associated with unlawful network use and data protection requirements. Contemporary administrative jurisprudence emphasises that administrative control now extends beyond traditional coercive tools to include guidance and public education as mechanisms for protecting digital public order[46].

Fourth: Cyber Risk Management Policies

Administrative authorities develop proactive plans to address potential digital risks through threat assessment, vulnerability identification, and response planning. These policies form binding regulatory frameworks for public and private institutions and are typically grounded in national cybersecurity strategies imposing digital protection standards[47].

Branch Two: Remedial and Sanctioning Methods of Electronic Administrative Control

These methods represent measures adopted after the occurrence of a violation, aiming to halt its effects, remedy its consequences, and prevent recurrence. They combine immediate administrative actions with administrative sanctions that may ultimately lead to judicial proceedings.

First: Content Blocking or Account Suspension

Blocking or suspension constitutes one of the principal remedial measures employed by administrative authorities, particularly in cases involving unlawful content or violations affecting digital public order. Several Arab legislations recognise this administrative competence as a means of protecting society from cyber risks[48].

Second: Administrative Fines

Administrative authorities may impose fines on individuals committing electronic violations that do not rise to the level of criminal offences. Such fines are based on specific legal provisions and function as direct regulatory sanctions intended to ensure compliance without lengthy judicial procedures[49].

Third: Referral to Judicial or Criminal Authorities

Where a violation exceeds administrative responsibility and constitutes a cybercrime, the administration refers the offender to the competent prosecution authorities. This referral is grounded in national cybercrime legislation criminalising acts such as hacking, data manipulation, and dissemination of malicious software[50].

Fourth: Restoration of Digital Order and Damage Mitigation

Following a digital incident, competent authorities undertake technical measures to address vulnerabilities, restore data, and prevent recurrence. These actions form part

of what modern administrative doctrine describes as the rehabilitation of the digital public service, a concept emerging within the framework of protecting electronic public utilities[51].

Conclusion

This study has demonstrated that electronic administrative control has become an organisational necessity imposed by the nature of cyberspace and the risks it generates, which exceed the capacity of traditional administrative control mechanisms. The findings reveal that the effectiveness of electronic administrative control depends primarily upon the existence of a clear legal framework alongside the administration's reliance on advanced technological tools capable of ensuring preventive and efficient protection of digital public order.

The study further highlights the need to achieve a careful balance between administrative supervisory powers in the digital sphere and the protection of individuals' digital rights and freedoms, particularly in light of the expanding scope of electronic surveillance. The recommendations emphasise the importance of legislative development, strengthened judicial oversight, enhancement of technical capacities within administrative institutions, increased international cooperation, and the promotion of digital awareness.

Accordingly, electronic administrative control represents a modern regulatory framework in which law and technology intersect, requiring precise legal regulation capable of safeguarding public order within a secure digital environment without undermining individual rights and freedoms;

Findings

- 1 . The study confirms that electronic administrative control has become an urgent necessity in light of digital transformation and the growing prevalence of cyber risks, as traditional control mechanisms are no longer sufficient to address challenges arising within cyberspace.
- 2 . The legal framework governing electronic administrative control in Jordan remains in a developmental phase. Despite the existence of significant legislation, such as the Cybercrime Law and the Personal Data Protection Law, practical application demonstrates the need for more precise regulatory organisation.
- 3 . Electronic administrative control is characterised by a clearly preventive nature, aiming primarily at preventing digital violations through electronic monitoring, content blocking measures, and early-warning systems.
- 4 . Public administration enjoys broad discretionary powers in exercising electronic control, granting flexibility in addressing digital risks while simultaneously raising concerns relating to excessive surveillance and potential infringement of users' rights. Technological tools play a central role in strengthening administrative capacity to detect violations, particularly through.
- 5 . digital monitoring systems, encryption technologies, artificial intelligence applications, and data analytics.
- 6 . A continuing challenge exists in achieving equilibrium between protecting public order and safeguarding digital rights and freedoms, especially with the expansion of electronic monitoring and content restriction practices.
- 7 . International responsibility increasingly intersects with electronic administrative control, particularly where unlawful digital activities extend across borders, making compensation, restoration, and guarantees of non-repetition essential mechanisms for addressing digital harm.

Recommendations

- 1 . Developing a more comprehensive legislative framework governing electronic administrative control that clearly defines administrative powers, prevents abuse, and guarantees protection of citizens' digital rights.
- 2 . Strengthening judicial oversight over electronic administrative decisions, particularly those relating to surveillance and website blocking, in order to ensure compliance with the principle of legality.
- 3 . Enhancing the technical capabilities of administrative authorities through continuous professional training in digital monitoring and analytical technologies to improve preventive effectiveness.
- 4 . Adopting clear policies for digital privacy protection by defining the categories of data that administrative authorities may lawfully collect, process, and retain, in accordance with proportionality and necessity principles.
- 5 . Promoting international cooperation in combating cross-border cyber risks through information exchange agreements and coordinated regulatory mechanisms.
- 6 . Expanding digital awareness programmes aimed at individuals and institutions to foster a culture of cybersecurity and responsible digital behaviour.
- 7 . Encouraging the integration of artificial intelligence governance standards within administrative practice to ensure transparency, accountability, and protection against algorithmic bias in electronic control decisions.

References and Footnotes

1. Saad Al-Shreida, Administrative Law (Wael Publishing, Amman 2019) 124.
2. Hussein El-Sayed Basyuni, Principle of Administrative Control and Judicial Supervision (Al-Nahda Al-Arabiya, Cairo 1986) 48.
3. Youssef Nasser Hamad Al-Dhafeeri, 'Administrative Control and its Limits in Normal and Exceptional Circumstances' (2017) Journal of Law, Kuwait University 112.
4. Al-Dhafeeri (n 3) 115.
5. Ahmad Agus Ramdlany, Integrating Fiqhiyyah Legal Maxims and Positive Law Principles in the Formation of Indonesia's New National Criminal Code," Nusantara: Journal of Law Studies, Vol. 5, No. 1 (2026), p. 454, <https://doi.org/10.66325/nusantaralaw.v5i1.156>.
6. Saleem Asouli, Legal Problems of Article VI of The Jordanian Administrative Justice Law Concerning Formal Conditions for Suspending the Execution of Administrative Decisions: Comparative Study," International Research Journal of Multidisciplinary Scope (IRJMS), Vol. 6, No. 1 (2025), p. 1463, <https://doi.org/10.47857/irjms.2025.v06i01.02573>.
7. Talal Yassin Aleissa, Principle of Legality in International Criminal Law," Pakistan Journal of Criminology, Vol. 15, No. 4 (2023), p. 683).
8. Ziad Mohammad Al Wahshat, Saleem Asouli, Criminalization of Aircraft Hijacking in International Law," Social Science Forum Journal, ISSN: 0352-3608, E-ISSN: 1581-968X, p. 294.
9. Saleem Asouli, "Digital Administrative Policing and Its Role in Regulating Cyberspace: A Comparative Study between Jordan and Indonesia," Al-Biruni Journal of Humanities and Social Sciences, Vol. 04, No. 06, 2026, pp. 28–41, DOI: <https://doi.org/10.64440/BIRUNI/BIR0028>.
10. Ali Al-Huneiti, 'Cybersecurity and its Impact on Protecting Digital Public Order' (2020) Jordanian Journal of Law 67.

11. Jordanian Cybercrime Law No 27 of 2015, art 3.
12. Jordanian Personal Data Protection Law No 24 of 2023, art 5.
13. Telecommunications Regulatory Commission, Regulatory Instructions for Internet Services (Amman 2022) 14.
14. Al-Dhafeeri (n 3) 118.
15. Saad Al-Shreida (n 1) 125.
16. Al-Dhafeeri (n 3) 120.
17. Saad Al-Shreida (n 1) 132.
18. Jordanian Cybercrime Law No 27 of 2015, art 4.
19. Hussein El-Sayed Basyuni (n 2) 55.
20. Al-Dhafeeri (n 3) 123.
21. Basyuni (n 2) 125.
22. Ali Al-Huneiti (n 5) 70.
23. Al-Huneiti (n 5) 72.
- 24 . Mohamed Abu Roman, Digital Transformation and e-Governance (Safaa Publishing, Amman 2021) 144.
25. Telecommunications Regulatory Commission, Internet Services Regulatory Instructions, Amman, 2022, p.18.
- Abu Roman (n 19) 149.
26. Jordanian Cybercrime Law No 27 of 2015, art 12.
- Telecommunications Regulatory Commission (n 8) 18.
27. Jordanian Cybercrime Law No 27 of 2015, art 12.
28. Abu Rumman, previous reference, p.149.
29. See: Al-Huneiti, previous reference, p.70.
30. See: Al-Huneiti, previous reference, p.72.
31. See: Mohammed Abu Rumman, Digital Transformation and Electronic Administration, Dar Safaa, Amman, 2021, p.144.
32. See: Abu Rumman, previous reference, p.149.
33. See: Jordanian Personal Data Protection Law No. 24 of 2023, Art. 6.
34. See: Telecommunications Regulatory Commission, Internet Services Regulatory Instructions, 2022, p.18.
35. See: Jordanian Cybercrime Law No. 27 of 2015, Art. 12.
36. See: Al-Dhafiri, previous reference, p.131.
- Suleiman Al-Tamawi, The Mediator in Administrative Law (Dar Al-Fikr Al-Arabi,
37. See: Jordanian Cybercrime Law No. 27 of 2015, Art. 4.
38. See: Al-Basyouni, previous reference, p.55.
- 39 . See: Jordanian Personal Data Protection Law No. 24 of 2023, Art. 8.
- 40 . See: Telecommunications Regulatory Commission, Internet Services Regulatory Instructions, 2022, p.15.
41. See: Arab Convention on Combating Information Technology Offences, Cairo, 2010, Art. 12.
42. See: Al-Dhafiri, previous reference, p.138.
43. See: Internet Services Regulatory Instructions, ibid., p.19.
- Cairo 2010) 312.
- 44 . Mohamed Al-Saeed Al-Daqaq, Administrative Control and Protection of Public Order (Al-Nahda Al-Arabiya, Cairo 2015) 221.
- 45 . Al-Daqaq (n 24) 230.
- 46 . Abdullah Al-Kilani, 'Cybersecurity and the Role of Administrative Control' (2022) Legal Studies Journal 88.
- 47 . Al-Kilani (n 26) 94.

- 48 .Ahmed Hafez, Administrative Law and its Digital Applications (University of Jordan Publications, Amman 2019) 176.
- 49 .Hafez (n 28) 181.
- 50 .Jordanian Cybercrime Law No 27 of 2015, art 3.
- 51 .Ali Shukri, 'Protection of Digital Public Facilities' (2021) Public Law Journal 54.