

UDC: 342.9:004.738.5  
DOI: 10.59214/ua.fa/5.2025.109

**Vladyslav Kononenko\***

*Master's Degree*

*Taras Shevchenko National University of Kyiv*

*01033, 60 Volodymyrska Str., Kyiv, Ukraine*

*<https://orcid.org/0009-0003-9234-458X>*

## Digital sovereignty policy in Saudi Arabia and Iran: Challenges for international law and global internet governance

**Abstract.** The relevance of this research is determined by the growing global trend towards strengthening state control over the digital sphere, which finds clear expression in the digital policies of authoritarian regimes. The aim of the study was to analyze the features of the implementation of digital sovereignty policies in the Kingdom of Saudi Arabia and the Islamic Republic of Iran, as well as to assess their impact on international legal norms and the global Internet governance system. The research methodology was based on normative legal analysis, case studies of national digital autonomy strategies, and examination of institutional behaviour within global internet governance forums. The study established that Iran and the Kingdom of Saudi Arabia (KSA) have implemented different in form but similar in authoritarian essence models of digital sovereignty, which entail centralised control over internet infrastructure, data localisation, and restrictions on access to global content. It was found that Iran has developed an isolationist model of digital autonomy, based on the creation of a National Information Network, traffic segmentation, and the blocking of international resources, whereas KSA integrated mechanisms of digital control into its broader state techno-economic development strategy within Vision 2030, combining them with engagement of Western technology partners. Systematic restrictions on digital human rights were documented in both countries, in particular freedom of expression, access to information, and privacy, which contravene the international legal obligations of states. It was further established that Iran and KSA pursue deliberate policies aimed at influencing global internet governance processes – in particular, through participation in intergovernmental formats, promoting concepts of digital sovereignty, and contesting universal principles of an open Internet. The study also revealed the structural weakness and fragmentation of international regulatory responses: absence of coherent mechanisms for holding states accountable, limited mandates of global institutions, and low effectiveness of multilateral forums in constraining authoritarian fragmentation of the digital sphere. The practical significance of the research lies in formulating recommendations for international institutions on safeguarding the unity of the digital domain and curbing authoritarian internet fragmentation

**Keywords:** authoritarianism; data localisation; isolation; technologies; privacy; fragmentation

### Introduction

Digital sovereignty increasingly emerges as a central vector of national cyber policy, encompassing security, technological, and legal dimensions. In the case of the Kingdom of Saudi Arabia (KSA) and the Islamic Republic of Iran, this concept has assumed the form of an ideologised response to the challenges of the global internet architecture, perceived as vulnerable to external influence and incompatible with autocratic models of digital governance. In this context, tension arises between universalist norms of international law – particularly human rights, cross-border information flows, and multistakeholder governance – and the aspiration of national governments towards normative isolation. This dynamic requires critical reflection on the limits of legal pluralism in the global digital sphere and on

the capacity of the international community to formulate an effective response to new forms of digital authoritarianism. In M.L. Mueller's (2020) study, digital sovereignty was examined as a complex phenomenon that challenged the traditional understanding of sovereignty linked to territory and supreme authority. The author stressed that in cyberspace, power and territoriality were disaggregated, making the application of classical sovereignty concepts to the digital domain problematic. At the same time, he analyses how various states, particularly authoritarian regimes, employ ideas of digital sovereignty to legitimise internet control and isolation from global digital flows. The article also highlighted the geopolitical struggle for control of cyberspace, where concepts of cyber sovereignty reflect the

*Received: 04.07.2025, Revised: 21.09.2025, Accepted: 26.10.2025*

### Suggested Citation:

Kononenko, V. (2025). Digital sovereignty policy in Saudi Arabia and Iran: Challenges for international law and global internet governance. *Foreign Affairs*, 35(5), 109-122. doi: 10.59214/ua.fa/5.2025.109.

\*Corresponding author



Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

interests of major powers, and discussed an alternative model of global commons as a potential basis for international regulation of the Internet. This approach challenges traditional notions of sovereignty and opens up new perspectives for understanding digital autonomy in the context of global transformation. A similar line of reasoning is continued by O. Taldykin (2024), who, analysing various types of sovereignty, emphasised that the policy of “virtual sovereignty” is increasingly employed as a tool of domestic political control, challenging international legal mechanisms for the protection of freedom of expression.

A comparative analysis of digital isolation conducted by H. Kleshnia (2022) identified restrictions on access to global platforms as a manifestation of a simulacrum reality, in which the state constructs its own information space. In this context, the creation of localised network structures appears not only as a technical measure but also as a cultural-political response to the perceived threat of digital chaos. The study demonstrates that such isolation engenders fragmentation of social reality along the logic of postmodernism, wherein simulacra substitute open communication. This enables the interpretation of the internet sphere in authoritarian states as a closed model of virtual existence, governed less by technological imperatives than by cultural and ideological ones. In the study by A. Gul *et al.* (2021), the digital policy of KSA is analysed in the context of its regional rivalry with Iran. The authors stress that investments in data centres and regulatory restrictions on global platforms are not only elements of digital transformation but also instruments for reinforcing state control. Such a policy is framed as part of a broader strategic antagonism that permeates not only the military and diplomatic spheres but also the digital domain. This allows digital sovereignty to be considered as a new dimension of rivalry between KSA and Iran. A. Al-Rawi (2021) examined KSA’s digital policy as a tool for achieving “digital sovereignty” through investments in local data centres and restrictions on access to transnational platforms. The author emphasised the dual character of such a policy – simultaneously supporting digital transformation and strengthening state control over information flows. He analyses cyberattacks and digital surveillance in Arab states as forms of vertical political pressure on opposition-minded citizens. In this context, Saudi digital sovereignty acquires not only an economic or technological dimension but also becomes an element of repressive cyber policy. At the same time, horizontal (interstate) cyberattacks demonstrate that regional actors, including KSA, employ cyber instruments as part of strategic rivalry. A critical evaluation of the normative compatibility of such practices with international law is provided in the study by M. Sexton & E. Campbell (2020), which raises the issue of the legitimacy of restricting cross-border data flows in light of the International Covenant on Civil and Political Rights. The authors argue that the policy of internet segmentation pursued by Middle Eastern states contradicts universally recognised human rights principles. The study by O.A. Panchenko *et al.* (2020) focused on the domestic political consequences of digital sovereignty, particularly its impact on civil society. The authors underline that under conditions of restricted access to global sources of information, the digital space is transformed into a sphere

of censorship, where alternative views are excluded from public discourse. In the study by A.A. Shaharuddin & M. Ilias (2024), the specific features of digital transformation in Middle Eastern countries are analysed, demonstrating a combination of technological modernisation with authoritarian governance practices. The emphasis is placed on the fact that, despite the development of digital entrepreneurship, “smart city” initiatives, and the digitalisation of government services, these processes are accompanied by a deepening of digital inequality and an increasing level of control over the information space. Digital sovereignty policies in the region’s authoritarian states are shaped at the intersection of the modernisation imperative and repressive institutional practices. The problem of research on digital sovereignty policies lies in the predominance of analyses of European and North American models, while the experience of Middle Eastern states remains only fragmentarily represented. The scholarly discourse pays insufficient attention to how authoritarian regimes, particularly in KSA and the Islamic Republic of Iran, institutionalise digital control through legislative regulation, state monitoring, and restrictions on global internet interaction. It is underexplored how such practices correspond with international legal standards in the fields of human rights, cross-border data exchange, and internet infrastructure governance. Equally under-researched are the consequences of digital isolation policies for the effectiveness of global multilateral internet governance. The purpose of this study was to identify the specific features of digital sovereignty policy implementation in KSA and the Islamic Republic of Iran, as well as its impact on international law and the system of global internet governance. To achieve this goal, the following tasks were set: to analyse the normative legal foundations of digital sovereignty in KSA and Iran; to identify the key technological and political instruments of control over the digital sphere; and to assess the challenges posed by digital isolation policies to multilateral internet governance.

## Materials and Methods

The study employed an interdisciplinary approach. The analysis covered institutional foundations, legal and regulatory mechanisms, practices of digital control, and the regulatory interaction of the mentioned states with global actors. The main focus was placed on the dynamics of domestic policies regarding the protection of cyberspace, personal data, the regulation of digital services, and the restriction of information flows within the framework of the data sovereignty concept. The research was conducted from December 2024 to May 2025 in three stages: analytical systematisation of sources, empirical comparison of regulatory approaches, and interpretation of international legal challenges. The source base of the study included official legal acts, in particular the Anti-Cyber Crime Law of Saudi Arabia (2007) and the Personal Data Protection Law (2023). The analysis also incorporated normative documents such as the Law of Computer Crimes of the Islamic Republic of Iran (2009) and the Supreme Council of Cyberspace (2022). Particular attention was paid to national strategies such as the Resolution of the Supreme Council of Cyberspace (2016) and Saudi Vision 2030 (2025). To assess the impact of internet censorship on human rights

in Iran, the United Nations Report (2022) was analysed. Documents of the European Union on digital regulation and materials reflecting transnational discussions were also included, in particular the testimony of Deputy Secretary Strickling before the U.S. Senate Committee on Commerce, Science & Transportation (NTIA, 2015). The research methodology was based on a combination of institutional analysis of digital governance systems and a comparative approach. The institutional approach enabled the reconstruction of the structure of digital normativity in Iran and the Kingdom of Saudi Arabia, as well as the identification of points of interaction with international standards. Using this approach, the structure of cyber regulation was analysed, including the role of the Saudi Data & AI Authority (SDAIA) and the National Information Network. The comparative analysis was applied to juxtapose the approaches of Iran and KSA regarding data governance, control of information flows, and interaction with global digital actors. Within the analytical framework of the study, a typological approach was employed to analyse models of internet governance. In particular, the multistakeholder and state-centric models were examined as representing two polar approaches in the global debate on the distribution of power in the digital space. This choice was determined by several factors. The mentioned models embody extreme positions in the debates concerning the regulatory role of the state and non-state actors, which made it possible to clearly trace the legal and institutional specificity of the selected cases.

## Results and Discussion

Digital sovereignty is conceived as the capacity of a state to independently determine policy regarding digital infrastructure, data, and cyberspace, without permitting external interference. At the core of legal regulation of the digital domain remains the classical international law of sovereignty, under which each state exercises exclusive jurisdiction over events occurring within its own territory. Within the digital context, this principle is transformed into the right to control infrastructure, data exchange, the activities of digital companies, and access to content within national borders. At the same time, the very nature of the internet, as a technology enabling global information exchange through transboundary networks, collides with the territorial approach. International law does not provide for a single universal normative instrument that comprehensively regulates internet governance. The absence of such a system result in a legal asymmetry between states, transnational corporations, and international organisations. Some attempts to formalise digital human rights have been undertaken within the framework of the international human rights agenda, particularly through interpretation of the International Covenant on Civil and Political Rights. The United Nations (UN), within the framework of General Assembly Resolution 2200A (XXI) (1966), recognised that the right to freedom of expression enshrined in Article 19 of the Covenant extends to digital communications. However, the specific mechanisms for implementing this right under conditions of digital fragmentation remain controversial. Key international actors demonstrate divergent approaches to internet governance

and digital sovereignty. The International Telecommunication Union (ITU, n.d.), as a specialised UN agency, supports the idea of intergovernmental regulation of the digital sphere, which aligns with the interests of countries with authoritarian policies that advocate for the dominant role of the state in cyberspace regulation. Support for the concept of “information sovereignty,” particularly by countries such as Iran or China, is based on a model of centralised control, in which the International Telecommunication Union is viewed as a legitimate arbiter of intergovernmental decisions. In contrast, the Internet Corporation for Assigned Names and Numbers (ICANN, n.d.), a private non-governmental organisation headquartered in the United States, operates on the basis of a multistakeholder governance model, where, alongside states, private companies, the technical community, and civil society organisations participate in policy development (NTIA, 2015). Despite its declared openness, this model has been criticised by states that consider it non-transparent and dominated by Western interests. In particular, Iran has repeatedly expressed distrust toward ICANN’s institutional structure, referring to its dependence on U.S. legal mechanisms (Mueller, 2017).

The United Nations (2021) called for ensuring the right to access the Internet; however, it did not define specific legal norms regulating sovereignty in the digital space. The reports of the UN Group of Governmental Experts on Information Security are limited to general recommendations regarding state responsibility for behavior in cyberspace, leaving unresolved the issues of the legitimacy of digital restrictions, data localisation, or the use of national surveillance technologies. In this context, the policy of digital sovereignty, as implemented by states with limited political pluralism, remains beyond effective international oversight. The European Union (EU) occupies an intermediate position, seeking to combine sovereign regulation of digital infrastructure with adherence to the principles of democratic governance. The concept of strategic autonomy in the digital sphere, enshrined in Regulation (EU) 2022/2065 (2022) and Regulation (EU) 2022/1925 (2022), is not aimed at isolation but rather at limiting the influence of external technological giants on the EU internal market. At the same time, the EU recognises the necessity of global internet governance based on human rights, the rule of law, and international cooperation. This approach contrasts with the policies of Iran and KSA, where sovereignty is realised through the centralisation and blocking of information flows. Before analysing national strategies, the typology of internet governance models was examined, which made it possible to outline the general features of approaches to digital sovereignty in the global context (Table 1). A comparative analysis of the multi-stakeholder and state-centric models of internet governance reveals a profound divide between a liberal-inclusive and a sovereignty-centred vision of the digital domain. The first model, based on cooperation among diverse actors – governments, the private sector, and civil society – tends towards flexible, technically oriented regulation without rigid coercion, which allows for rapid adaptation to technological change. However, such a system demonstrates limited capacity to ensure the binding force of norms and global legal harmonisation. The state-centric model, by contrast,

is grounded in the principle of sovereignty, introducing strict regulation by national governments. Its strength lies in clear legal determinacy and control, yet it is frequently

accompanied by the fragmentation of the global internet, increased technological isolation, and the strengthening of authoritarian control.

**Table 1.** Key models of internet governance

| Model                  | Characteristic | Advantages                                                          | Disadvantages              | Model                                           |
|------------------------|----------------|---------------------------------------------------------------------|----------------------------|-------------------------------------------------|
| Multistakeholder model | Principles     | Participation of governments, the private sector, and civil society | Inclusiveness, flexibility | Lack of binding force                           |
|                        | Legal basis    | Soft law norms, technical standards                                 | Rapid adaptation           | Absence of enforcement                          |
|                        | Geography      | Predominantly Western countries                                     | Openness, innovation       | Western-centricity                              |
| State-centric model    | Principles     | State sovereignty over cyberspace                                   | National control           | Legal certainty                                 |
|                        | Legal basis    | National legislation                                                | Legal certainty            | Conflict with the global nature of the internet |
|                        | Geography      | Countries with authoritarian regimes                                | Political control          | Technological isolation                         |

**Source:** compiled by the author based on A. Shahbaz *et al.* (2020), S.A. Brown (2024), A. Mathew (2024), Overview of data sovereignty laws by country (2024)

Geographically, the state-centric model of internet governance is characteristic of countries with rigid power verticals and authoritarian political regimes – in particular, Iran, China, KSA, the United Arab Emirates, and North Korea. In China, the concept of cyber sovereignty, officially established by the Information Office of the State Council of the People's Republic of China (2010), envisions complete information filtering, the blocking of global platforms (Google, Facebook, X), and the development of domestic alternatives (Baidu, WeChat, Weibo) controlled by state authorities. In Iran, systems of digital sovereignty are defined by the Supreme Council of Cyberspace Strategy (2022) and the Law of Computer Crimes of the Islamic Republic of Iran (2009), which ensure content filtering, communication monitoring, and the development of the National Information Network separated from the global internet (Resolution of the Supreme Council of Cyberspace..., 2016). In KSA, digital control policy is based on Saudi Vision 2030 (2025) and regulatory acts such as the Anti-Cyber Crime Law of Saudi Arabia (2007) and the Personal Data Protection Law (2023), which regulate online behavior, restrict anonymity, and require data localisation. Accordingly, in the United Arab Emirates, the Smart Government system has been implemented, involving the active use of biometric data and limited access to independent media (Government of Saudi Arabia, n.d.). In North Korea, the internet is completely isolated from the global network, and access is granted only to certain governmental structures (Asher, 2016). All these cases demonstrate the aspiration of states toward digital autarky, grounded in control over infrastructure, content, and digital identity – all subordinated to the priorities of political stability, national security, and information sovereignty. A juxtaposition of the two models leads to the conclusion that the legal architecture of digital sovereignty in the contemporary world produces a non-unified legal field. The multi-stakeholder approach gravitates towards global inclusivity, while the state-centric model prioritises internal legitimisation of digital control. In the context of the formation of international law in this domain, this generates challenges for the development of universal principles capable of reconciling the requirements of national sovereignty with the protection of human rights and the functioning of cross-border digital infrastructure. In the

field of digital sovereignty, a situation has emerged of the absence of a single legal regime, producing zones of conflict between states, international institutions, and global technological actors. The lack of a binding international treaty on internet governance enables each state to implement its own interpretation of digital sovereignty, which in certain cases legitimises restrictive policies.

The digital sovereignty policy of the Islamic Republic of Iran is grounded in an ideologically motivated model of an autonomous internet domain, combining centralised regulation of digital infrastructure, consistent isolation from global networks, and an elaborate system of normative-legal and institutional mechanisms. At the legislative level, the state implements digital control through a range of legal acts that prioritise security, morality, and national sovereignty over principles of internet openness. The central legal initiative shaping the normative framework of Iran's digital sovereignty is the establishment of the National Information Network – an infrastructural and legal project aimed at creating an autonomous domestic internet segment, independent of the global network (Resolution of the Supreme Council of Cyberspace..., 2016). The concept of the National Information Network is implemented within several consecutively adopted policies, including the Supreme Council of Cyberspace (2022), the Law of Computer Crimes of the Islamic Republic of Iran (2009), and a number of subordinate acts. All these normative documents establish strict liability for cyber-crimes, while simultaneously broadening the definition of undesirable digital content to a degree that allows the criminalisation of any dissent or political activity in the online environment. Unlike European or international standards, such legislation does not provide mechanisms for assessing proportionality or compliance with the necessity standard when restricting freedom of expression. Institutionally, the key body of digital regulation in Iran is the Supreme Council of Cyberspace (2022), established in 2012 by order of Supreme Leader Ali Khamenei. This body coordinates all internet-related activities, determines state policy in the fields of digital security, censorship, data localisation, and digital infrastructure. The Council includes representatives of the country's highest political and security leadership, which indicates that cyberspace regulation is concentrated at the level of strategic

state governance, with technical and economic aspects subordinated to political priorities. The legal framework of Iran's digital sovereignty is aimed at localising internet infrastructure through mandatory storage of user data within the country, the creation of national analogues of Western platforms, and the blocking of cross-border access to key services. For example, Google, Facebook, Twitter, Telegram, WhatsApp, and YouTube have long remained inaccessible or partially blocked. Instead, the government actively promotes state or semi-state alternatives technically integrated into the National Information Network. In particular, the video-hosting service YouTube has been replaced by the platform Aparat, which operates within the boundaries of permitted censored content (Hajipour, 2025). Telegram and WhatsApp have been displaced by domestic messengers such as Soroush, Bale, iGap, and Rubika, which, although positioned as private, are in fact controlled by government or state-affiliated institutions (Kazemi, 2021). Previously, modified versions of Telegram – Hotgram and Talagram – were also used; these operated through Iranian proxy servers and enabled traffic monitoring (Lawmaker says..., 2019). The integration of these platforms into the National Information Network creates a closed informational ecosystem that not only ensures full institutional and technical accountability of user activity but also enables the prompt blocking of external content, restricting freedom of information in accordance with the regime's political objectives. This approach facilitates mass digital surveillance and grants the authorities complete control over traffic, while simultaneously creating conditions for the informational isolation of the population. As a result, fundamental international legal principles in the field of human rights, enshrined in General Assembly Resolution 2200A (XXI) (1966), are violated – particularly the rights to access information, freedom of expression, and privacy. Iran, as a state party to the Covenant, is formally obliged to adhere to Articles 17 and 19, which guarantee the right to privacy and freedom of expression. In practice, however, the Constitution of the Islamic Republic of Iran (1979) disregards the criteria of legality, necessity, and proportionality, which international bodies, including the UN Human Rights Committee, consider essential conditions for the legitimacy of any restriction of these rights. Systematic blocking of informational resources, criminalisation of oppositional content, and user surveillance without independent judicial oversight contradict universally recognised standards of digital human rights. Another aspect of the conflict with international law is the prohibition of cross-border services, which hinders international digital cooperation and economic integration. This policy contradicts the provisions of the Vienna Convention on the Law of Treaties (1969), as the blocking of communication platforms makes it impossible for Iran to fulfill several bilateral and multilateral obligations in the fields of cooperation, development, education, and science. Moreover, the requirement for foreign companies to store data exclusively within Iran is incompatible with the principles of free information exchange protected under global trade agreements and the General Agreement on Trade in Services (World Trade Organisation, 1995). The legal architecture of Iran's digital sovereignty constitutes an example of state policy oriented

towards maximum isolation from the global information space, relying on domestic legislation that largely ignores international legal obligations. As a result, a parallel digital reality is created, in which the fundamental instruments of global Internet governance are either absent or function in an ideologically transformed form, incompatible with the principles of multilateral cooperation, network openness, and respect for universal human rights. Iran's political and legal mechanisms serve to institutionalise digital isolation, creating long-term challenges for the architecture of the international legal order in the field of digital technologies. The model of digital sovereignty in the Kingdom of Saudi Arabia (KSA) is shaped at the intersection of an ambitious state strategy of technological modernisation and a drive to control the digital sphere within the context of authoritarian stability. At the core of the country's digital transformation lies the strategic initiative Saudi Vision 2030 (2025), which provides not only for economic diversification through the development of digital sectors but also for a substantial strengthening of national control over data flows, Internet infrastructure, and informational content. According to this vision, digital transformation must be realised under conditions of political centralisation, which predetermines the establishment of a legal regime oriented towards sovereign regulation of the digital ecosystem. A defining institutional element of this process is the establishment of SDAIA in 2019, vested with exclusive competences in the domains of digital data, artificial intelligence, and cybersecurity (Regulatory Arrangements for..., 2019). SDAIA coordinates all initiatives related to data processing, localisation, analytics, and oversight of compliance with national data standards, including those concerning privacy and cross-border transfer. SDAIA's competences extend beyond technical regulation – it functions as a political authority safeguarding digital sovereignty, shaping the legal framework that enables state control over information flows both within public institutions and the private sector.

A key normative act in the field of digital regulation is the Personal Data Protection Law (2023), adopted in 2021, which establishes the rules for the collection, processing, storage, and transfer of personal data within the framework of national jurisdiction. The law enshrines the requirement for the localisation of sensitive data within the territory of the Kingdom of Saudi Arabia (KSA) and grants the regulator the authority to block or restrict cross-border data transfers in cases where national security is threatened or where foreign legislation is deemed incompatible with Saudi standards. The Personal Data Protection Law also provides for the certification of digital platforms and the establishment of a supervisory system to ensure that international companies operating with KSA citizens comply with domestic legal provisions. This law effectively implements the principle of extraterritoriality, characteristic of authoritarian models of digital sovereignty, in which national interest prevails over the principle of global internet openness. Another notable feature of digital regulation in KSA is its emphasis on a regional initiative of cloud localisation – this involves prohibiting the use of certain foreign cloud platforms, similar to Iran, promoting national data centres, and establishing partnerships with technology companies under conditions of

full jurisdictional accountability. Such approaches gained additional weight following the announcement of the creation of a national digital cloud (Oasis Cloud), intended to reduce dependence on foreign service providers and ensure state-controlled management of critical digital infrastructure. From a legal perspective, this signifies the introduction of a regime of digital internalisation, in which the state establishes a separate legal space for the functioning of the Internet, not necessarily aligned with international standards of openness, competition, and freedom of information. Control over the online sphere in KSA is exercised in conjunction with the regime's political priorities, particularly regarding stability, combating "extremism", protecting Islamic values, and preventing internal destabilisation. The Constitution of Saudi Arabia (1992) provides for severe criminal sanctions for online activities that may be classified as defamation, criticism of state institutions, insult to religion, or support for political opposition. Regulation is carried out through specialised bodies of the Ministry of Interior and the Public Prosecutor's Office, which use digital platforms as instruments for monitoring public sentiment and rapid response. Of particular significance are the provisions of the Anti-Cyber Crime Law of Saudi Arabia (2007), which stipulates severe criminal liability for "using information technology to disrupt public order", interpreted in the broadest possible sense. The application of such norms forms a regulatory environment dominated by preventive user loyalty, reinforced by an extensive system of state digital surveillance and monitoring. In the context of the global digital order, KSA applies an ambivalent strategy – on the one hand, it restricts platforms that refuse to comply with content removal or data disclosure requirements. For instance, in 2022, the Saudi Ministry of Communications threatened to restrict or block access to Twitter, Snapchat, YouTube, and TikTok unless these companies removed "immoral content" in accordance with the requirements of the Communications and Information Technology Commission (Freedom House, 2024a). This example illustrates the state's aspiration to achieve sovereign control over the information environment, even if it requires confrontation with technoglobal corporations relying on principles of open Internet and privacy. On the other hand, it actively engages technology companies in national infrastructure projects through partnership formats ensuring legal accountability. For example, cooperation with Google Cloud and Alibaba Cloud is based on conditions requiring the storage of all data within Saudi territory, as well as compliance with SDAIA requirements regarding state access to information (Raj, 2024). This approach indicates an attempt to establish a hybrid model of sovereign control, combining instruments of the global market with national digital protectionism.

H. Li & X. Yang (2021) and C.B. Joyce (2025) outlined the interrelation between digital sovereignty and the centralisation of control over internet infrastructure. The study by C.B. Joyce highlighted how nation-states seek to intervene in the governance of network protocols, whereas H. Li & X. Yang emphasised the role of governments in transforming network architecture into an instrument of regional dominance. However, the analysis of KSA's policies demonstrates a somewhat different approach: state initiatives did not so much technically centralise the

internet as legally codify the absolute responsibility of the user, thereby creating a pseudo-legal framework for control. The study shows that in KSA the approach is formed through the hybridisation of commercial influence and state regulation, whereas other works predominantly focus on repressive or technocratic aspects. The reason for these discrepancies probably lies in the limited comparative perspective of the sources analysed, which examine the Middle East in general without considering the unique religious-legal context, critically important for understanding KSA's digital policy. The politico-legal architecture of digital sovereignty in KSA represents a complex system where authoritarian centralisation is combined with technocratic rationality. Within the state strategy, digital control is regarded as an instrument not only of economic transformation but also of political stabilisation of the regime. The Constitution of Saudi Arabia (1992) establishes a closed information ecosystem, controlled by the state and aimed at preserving the political status quo. These normative acts prescribe strict data localisation, prohibition of their cross-border transfer without special authorisation, and broad competences for state institutions regarding monitoring, moderation, and removal of digital content. Such a policy directly conflicts with international law, particularly Articles 17 and 19 of the General Assembly Resolution 2200A (XXI) (1966), which guarantee the right to privacy and freedom of expression. Although KSA is a state party to this covenant, it interprets its international obligations through the lens of national sovereignty, effectively creating a model of "differentiated interpretation of human rights" within the digital environment. Digital control in KSA acquires the function of not only a protective but also a projective instrument – the state model of digital sovereignty is actively promoted as an alternative to the liberal paradigm of the open Internet. Through participation in global forums, particularly the World Summit on the Information Society, KSA advances the concept of digital pluralism (UNESCO, n.d.). Within this concept, each state should have the right to autonomously define the rules for its digital space, including technical, legal, and ethical standards. This approach challenges the established multistakeholder model of Internet governance, which presupposes a balance between governments, the private sector, civil society, and the technical community. The Saudi model, on the contrary, demonstrates consistent strengthening of the state's role as the sole actor responsible for digital sovereignty, avoiding transparency, accountability, and plurality of opinion. In this context, the legal architecture of digital sovereignty in KSA bears not only domestic political significance but also global impact, shaping one of the vectors of transformation of the digital order towards regionalised, fragmented systems of Internet governance. This vector not only crystallises political divergences between authoritarian and democratic regimes in the field of digital governance but also questions the universality of international standards, particularly in the domains of human rights, cybersecurity, and cross-border information flows.

The studies by E. Celeste & F. Fabbrini (2021) and H. Jongen & J.A. Scholte (2021) revealed the relationship between digital sovereignty and global trends of cyberspace regionalisation. E. Celeste & F. Fabbrini emphasised

the growing number of jurisdictions seeking to establish their own rules for internet access, whereas H. Jongen & J.A. Scholte analysed the shift from multilateral to multi-stakeholder governance. The conducted analysis demonstrated that, despite its apparent centralisation, KSA actively engages international corporations in the establishment of cloud data centers, thereby breaching rigid models of data localisation. This finding does not align with the thesis of H. Jongen & J.A. Scholte regarding consistent fragmentation, since in the case of KSA a form of functional hybridisation occurs: sovereignty is controlled at the level of access, while openness is maintained at the infrastructural level. The digital sovereignty policies of the Kingdom of Saudi Arabia and the Islamic Republic of Iran exhibit significant commonalities in their pursuit of absolute state control over the digital sphere, yet are implemented in different political, technological, and international contexts, which determine differences in legal mechanisms, institutional architectures, and strategic objectives of both states. The central element of digital sovereignty in both KSA and Iran is the subordination of Internet infrastructure to the political interests of the state, primarily in the domain of regime stability, population control, and minimisation of the influence of external information sources. Both states legally entrench the primacy of national sovereignty over global standards of openness, freedom of expression, and cross-border information flows, identifying the digital sphere as a key area of strategic importance that must remain under full jurisdictional control. The Iranian model of digital sovereignty is manifested in the consistent implementation of a policy of cyber-isolation, the most prominent expression of which has been the National Information Network – a closed infrastructure that enables the operation of internet services without connection to the global web. Iran's legal framework, which encompasses provisions on cybercrime, content filtering, censorship, and regulation of user behaviour, creates conditions under which access to foreign sources of information is strictly restricted, while interaction with international digital companies is virtually absent. By contrast, the Kingdom of Saudi Arabia (KSA), although implementing control policies of a similar nature, does not pursue complete cyber-isolation. It remains open to partnerships with transnational IT corporations, albeit under conditions of strict data localisation, compliance with national legislation, and jurisdictional control over critical infrastructure. Thus, Iran adheres to the principle of digital autarky, whereas KSA opts for a hybrid model of technological protectionism combined with managed international integration. A. Oldenbourg (2022) and Y. Shany (2023) have examined the role of digital rights in the context of resisting sovereign forms of censorship. The concept of “digital human rights” as a universal regulatory principle has been formulated, and the excessive politicisation of the concept of freedom in the digital space has been criticised. In the Iranian case under study, these approaches encounter significant challenges: here, the rights of internet users are not articulated in terms of individual freedoms but are reinterpreted through the prism of religious duty and social harmony. Y. Shany's assertions appear debatable, as they rest upon a Western human rights paradigm that lacks a direct normative equivalent in the

Iranian system. The analysis conducted highlights the necessity of de-radicalising the legal discourse so as to render it relevant to illiberal regimes. The divergence in interpretation stems from the failure to take into account the cultural specificity of legal thought in Islamic states. The legal mechanisms of implementing digital sovereignty in both countries operate within authoritarian political systems, yet differ in their degree of formalisation and institutional complexity. In Iran, the Supreme Council of Cyberspace, subordinate to the Supreme Leader, plays the decisive role in shaping digital policy, concentrating authority directly in the hands of the highest religious leadership. Iranian legislation is predominantly repressive in nature, aimed at criminalising online activities perceived as threats to Islamic values or national security. KSA, in turn, has established a complex technocratic governance architecture for the digital sphere, in which a key role is played by the SDAIA – the authority responsible for integrating issues of artificial intelligence, data protection, and digital regulation. The adoption of the Personal Data Protection Law (2023) reflected an attempt to legitimise digital control through formally legal mechanisms that approximate international terminology while deviating from its substantive meaning. This contrasts with the Iranian practice, where legal regulation often has a declarative character and is subordinated to the priorities of security and enforcement agencies. In the works of J. Ruohonen (2021) and D.J. Svantesson (2021), attention is focused on the legal conflicts between national regulatory regimes and international standards of freedom of expression. They emphasise the contradiction between states' pursuit of digital sovereignty and their international obligations, as well as demonstrate how technology giants become caught in jurisdictional conflicts. The analysis of KSA and Iranian policies confirmed these discrepancies but also revealed a pragmatic approach: states deliberately create “grey zones” within the legal field, delegating certain domains to BigTech companies in order to avoid direct responsibility for rights violations. This approach is inconsistent with the normative model in which the state is viewed as the principal regulator. The divergence arises from a simplified assumption of the uniformity of the legal order, whereas in practice states utilise digital policy as an instrument of asymmetric law enforcement. In the technical dimension, KSA far outpaces Iran in the development of digital infrastructure, enabling the implementation of sophisticated data strategies, the establishment of national data centres, the launch of cloud services, and the promotion of artificial intelligence as a tool of strategic development. Iran, by contrast, faces constraints imposed by international sanctions, which preclude technological modernisation through cooperation with global companies. This compels Iran to develop domestic software, internal analogues of social networks and messaging platforms; however, the effectiveness of such systems remains limited due to a lack of access to cutting-edge technologies and an absence of user trust. Technological backwardness, combined with repressive policies, creates conditions under which Iran's digital sovereignty functions more as a barrier to global information exchange than as an instrument of modernisation. The international context also sharply distinguishes these

two models. Iran predominantly acts in isolation, appealing to principles of non-interference and sovereignty in the digital sphere within alternative frameworks of international cooperation, such as the Shanghai Cooperation Organisation or BRICS+ (Brazil, Russia, India, China, South Africa). Nonetheless, it remains a peripheral actor in the global digital architecture. KSA, by contrast, actively promotes its participation in international organisations such as the G20, the International Telecommunication Union, and the UN, where it positions its model as an example of responsible sovereign governance, capable of combining innovation with security. Through mechanisms of “digital diplomacy”, KSA seeks to legitimise its approach as consistent with principles of international law, even though it faces criticism from human rights organisations for restricting freedom of expression. From the perspective of domestic legitimacy, digital sovereignty functions for both regimes as an instrument of control and stabilisation. In Iran, the blocking of global services, persecution of online activists, and institutional restriction of access to information serve to reinforce the influence of the politico-religious elite and preserve social order in conditions of heightened protest activity. At the same time, such policies generate growing discontent among the youth, widening the gap between state discourse and digital reality. KSA, conversely, seeks to build digital legitimacy through investments in technology, the provision of digital services to citizens, and the modernisation of administrative governance. This creates the perception of a

state as an innovator, although restrictive legislation on freedom of speech and limitations on independent journalism indicate that digital sovereignty remains primarily an instrument of control rather than emancipation. For a more in-depth comparative analysis of Iran’s and KSA’s digital strategies, this study employs the generalised Table 2, which systematises the key parameters of digital sovereignty in both countries. The data presented clearly illustrate the differences between Iran’s isolationist model and KSA’s modernisation-oriented approach. The findings reveal profound conceptual and institutional asymmetry in the approaches to digital sovereignty in Iran and KSA. The Iranian model exemplifies an inward-oriented digital isolationism, rooted in distrust of the global information environment and focused on repressive control, whereas the Saudi strategy is directed towards the external projection of digital modernisation while retaining elements of political control. At the same time, both models demonstrate a tendency to combine technocratic instruments of digital transformation with authoritarian governance mechanisms. Divergences in the level of international integration and approaches to artificial intelligence highlight the differing degrees of flexibility of the two countries in responding to global challenges of the digital agenda. Overall, both cases demonstrate how digital sovereignty may serve simultaneously as a means of internal power consolidation and as an instrument of geoeconomic positioning, thereby posing challenges to the universalisation of principles of global internet governance.

**Table 2.** Comparative analysis of the digital sovereignty of Iran and the KSA

| Criteria                            | Iran                                                      | KSA                                                         |
|-------------------------------------|-----------------------------------------------------------|-------------------------------------------------------------|
| Core strategy                       | Isolationist approach focused on control and censorship   | Modernisation approach within the framework of Vision 2030  |
| Digital sovereignty objectives      | Protection from external influence, control over citizens | Economic diversification, regional technological leadership |
| Level of Internet freedom*          | 12                                                        | 25                                                          |
| Network blocking                    | Extensive blocking                                        | Selective blocking focused on content                       |
| Personal data protection            | Stringent control for surveillance purposes               | Privacy protection                                          |
| Content censorship                  | Deep Packet Inspection (DPI), comprehensive censorship    | Censorship of religious and political content               |
| National internet                   | Development of the “National Information Network”         | Development of sovereign cloud infrastructure               |
| Artificial intelligence             | Development under sanctions, focus on domestic solutions  | Investments in AI of up to USD 1.9 billion by 2027          |
| International cooperation           | Minimal due to sanctions                                  | Active engagement with international partners               |
| Participation in global initiatives | Minimal participation                                     | Active participation in G20, international forums           |
| Key challenges                      | International sanctions, technological isolation          | Dependence on foreign technologies                          |

**Note:** \* – according to Freedom House, scores are based on a scale from 0 (least free) to 100 (most free)

**Source:** compiled by the author based on United Nations (2022), Freedom House (2024a; 2024b), Digital Policy Alert (2024), I. Payande (2024), International Trade Administration (2024), Saudi Arabia Data Sovereignty Policies and Requirements (2024), F. Bria & H. Sheikh (2025), J. Olaje (2025)

In the works of N. Möllers (2020) and S. Mihelj & C. Jiménez-Martínez (2021), attention is drawn to the risks of digital nationalism, particularly the danger of forming isolated information ecosystems. N. Möllers viewed digital nationalism as a threat to cross-border information flows, whereas S. Mihelj & C. Jiménez-Martínez emphasised the erosion of the open architecture of the internet caused by political fragmentation. These conclusions partly align

with the findings of the present study, where the creation of national information networks essentially reproduces the logic of digital autarky. However, the assertion of S. Mihelj & C. Jiménez-Martínez regarding the purely negative effect of digital nationalism appears overly simplistic, since in the case of Iran it also functions as a means of preserving sovereignty under conditions of informational embargo. This demonstrates that digital nationalism may

represent not only a manifestation of authoritarian ambitions but also a response to external pressure. The divergence arises from differing foci: the authors' analysis is primarily liberal-normative, whereas the Iranian context necessitates a more geopolitically grounded approach. At the international level, Iran's policy of digital sovereignty has drawn criticism from international human rights organisations, which record numerous violations of the rights to access information, freedom of expression, and privacy. KSA, despite substantively similar policies, is able partially to mitigate international criticism through diplomatic engagement, participation in global forums, and demonstrations of openness to technological partnership. However, in both cases, the issue concerned a conflict with the fundamental provisions of international law, as well as with the principles of free and non-discriminatory access to the internet enshrined in Human Rights Council Resolution 54/24 (2023). This conflict demonstrated that authoritarian models of digital sovereignty, even when formally compliant with legal frameworks, are structurally incompatible with the foundations of the liberal internet order, thereby calling into question the universality of its legal norms in the digital age.

According to the studies of E. Del Re (2024) and S. Fratini *et al.* (2024), digital sovereignty may be understood as a form of "data as a public good", whereby states assume responsibility for their protection and regulation. Both works emphasise the importance of transparency in data storage and processing mechanisms to prevent abuse, particularly in the context of democratic governance. At the same time, the analysis of KSA reveals a different dynamic: the concept of data as a public resource in this country is realised through a form of centralised control, whereby governmental structures retain exclusive access to information, with no involvement of civil society or independent institutions. This does not align with Del Re's vision, which asserts that digital sovereignty should serve as an instrument for democratising data governance rather than as a means of reinforcing executive power. The reason for such divergence lies in the distinct normative contexts. Claims of the universality of the "data as a public good" approach appear debatable, as they fail to account for the specificities of political regimes in which the category of publicness is reduced to a state monopoly over information. The approach to digital sovereignty as an instrument of political legitimisation is traced in the works of H. Sheikh (2022) and M. Jiang & L. Belli (2025). H. Sheikh interpreted digital sovereignty as a concept that allows states to restore political autonomy in the face of transnational platform influence, while M. Jiang & L. Belli viewed it in terms of a political-infrastructure compromise. In the Iranian context, these approaches are partially consistent, as Iran indeed employs the rhetoric of "digital self-defence" to justify domestic repressive practices. However, the conclusions drawn by the scholars appear overly abstract: they do not explain how precisely the normative system of sharia is adapted to legitimise a sovereign digital order. The analysis conducted demonstrates that in Iran it is not only the infrastructure but also the ontology of cyberspace itself that is codified in accordance with religious doctrine – a factor that the aforementioned authors fail to take into account. The reason for this divergence may lie

in the limited attention devoted to sources of the Persian legal tradition. The policy of digital sovereignty, actively pursued in the KSA and the Islamic Republic of Iran, generates a range of systemic challenges to the existing model of global internet governance. The central issue is the increasing fragmentation of the digital space, which is a direct consequence of states' aspirations to exercise complete control over information flows, infrastructure, and behavioural standards within their jurisdictions. The creation of sovereign national internet segments, restrictions on cross-border data exchange, requirements for infrastructure localisation, as well as regulatory blocking of global digital services undermine the foundations of a single global internet built upon the principles of openness, interconnectedness, and technical neutrality. The KSA and Iran, though employing different institutional approaches, in practical terms contribute to the rupture of the global information space, thus laying the groundwork for the emergence of a polycentric, ideologically and technically divided network with multiple standards and regulatory regimes. Aggressive forms of digital sovereignty challenge the effectiveness of the multistakeholder model of internet governance, which has long defined the global architecture of the digital order. This model envisions the participation of not only states, but also the private sector, the technical community, civil society, and international organisations in decision-making processes. It remains central to the functioning of ICANN (n.d.), the key institution for the technical coordination of the internet. Saudi Arabia and Iran increasingly promote an alternative governance framework in which the state assumes the leading role and full responsibility for digital policy within its own sovereign domain. Within platforms such as the International Telecommunication Union (n.d.), both countries actively advocate the concept of "digital sovereignty," which calls for the legal recognition of each nation's right to shape its internet space according to national standards – including control over technical infrastructure, content, and cross-border information flows. This position directly contradicts the universalist approach of ICANN, where jurisdiction over the technical architecture of the internet is recognised as global rather than national. The legal dimension of this contradiction lies in the conflict between states' international obligations in the field of human rights – particularly regarding access to information, freedom of expression, and the right to privacy – and domestic legal regimes that justify restrictions on digital rights by invoking security, morality, or political stability. The Iranian experience demonstrates how legal control over the internet can evolve into the political instrumentalisation of digital rights aimed at suppressing opposition and restricting civic space, in direct violation of the International Covenant on Civil and Political Rights. Saudi Arabia, by contrast, seeks to create the appearance of legal order through the adoption of specialised legislation – notably the Personal Data Protection Law (2023) – which formally aligns with European practice but in substance functions as a mechanism of state control over information flows. Both models disrupt the balance established by international instruments and digital rights charters, undermining trust in global mechanisms for protecting users' rights online.

The studies by U. Reviglio & C. Agosti (2020) and M. Martin (2023) examined the concept of “algorithmic sovereignty”, whereby states seek to control not only data but also the logic of its processing. The authors criticised the opacity of algorithmic systems and called for their accountability. In the case of Iran and the KSA, these approaches take on unexpected forms: the state not only localises algorithms (e.g., through filtering according to local rules) but also develops its own language models to control the information environment. The authors’ assertions regarding the limitations of sovereign algorithmic control in democratic systems are entirely valid; however, in authoritarian systems such control becomes institutionalised through the establishment of state AI commissions. This complements conclusions regarding the dangers of the concentration of digital power, illustrating its concrete implementation in the KSA. The issue of global digital platforms’ access to the markets of the KSA and Iran arises as one of the key aspects of these states’ regulatory policy. Such collisions pose the danger of legal fragmentation of digital regulation, whereby companies are forced to comply simultaneously with contradictory regulatory regimes, thereby increasing transaction costs and reducing the effectiveness of user rights protection. In Iran, the absence of legal guarantees and transparent complaint-handling procedures deprives users of the possibility of appeal or recourse to international protection mechanisms. The KSA, by contrast, establishes formal regulatory mechanisms, yet these operate within an authoritarian legal system, where the independence of the judiciary and the accountability of state institutions remain limited. This raises concerns among international organisations, particularly the UN Human Rights Council, which has repeatedly voiced concern about restrictions on digital freedoms in the Gulf states. Under the pressure of digital sovereignty policies, global technology companies face a dilemma: either adapt to the requirements of highly authoritarian states – thereby potentially jeopardising user rights – or forgo access to large and strategically significant markets. This process creates a new configuration of internet governance, in which technical providers are compelled to operate within national legal regimes that significantly restrict the scope for universal application of the principles of openness, net neutrality, and user rights protection. Studies by T. Dragu & Y. Lupu (2021) and J. Hardy (2021) emphasised the institutional nature of digital authoritarianism, which is formed through bureaucratic control mechanisms. The authors emphasised that governments are instrumentalising digital technologies to expand the powers of internal security agencies, noting the effect of ‘creeping’ normalisation of surveillance, which begins with exceptional circumstances but eventually becomes the norm. The present research partially aligns with these conclusions, particularly regarding the gradual institutional entrenchment of techno-control, but it reveals a different pattern. Rather than evolutionary bureaucratisation, one observes a leap-like formalisation of digital sovereignty – particularly through the establishment of the Supreme Council of Cyberspace as a supranational coordination structure. The assertion by O. Schlumberger *et al.* (2024) about the evolutionary nature of digital authoritarianism seems debatable, since in the case of

Iran, institutionalisation processes are reactive in nature, linked to periods of escalation in international sanctions, particularly after 2010 and 2018. This diverges from the analysis above, for instead of gradual institutional accumulation, one observes wave-like political responses to external threats, accompanied by internal mobilisation of administrative and religious institutions. The reason for this divergence lies in the author’s focus on China as the paradigmatic example of digital authoritarianism, whereas the Iranian model exhibits greater adaptive flexibility and a less centralised digital infrastructure. The comparative analysis of digital sovereignty in the KSA and the Islamic Republic of Iran demonstrates that both states actively construct their own digital spaces in line with political, ideological, and security priorities, while markedly diverging from the principles of the open internet. The common denominator of their policies is the dominance of the logic of state control over the digital domain, entrenched in legislative, administrative, and infrastructural mechanisms. Iran represents the most radical variant of digital autarky, where isolation of the national internet segment from the global network is a political imperative. The KSA, by contrast, implements digital sovereignty through a hybrid model, combining access to transnational technologies with a strict regulatory regime that consolidates state dominance in the domain of data, platforms, and network infrastructure. Differences in openness, technical sophistication of infrastructure, and institutional engagement with global digital actors do not negate the common paradigm: the digital space is instrumentalised as a key resource of political control, geopolitical influence, and internal legitimisation of the regime. These examples provide grounds for anticipating further entrenchment of the concept of digital sovereignty in authoritarian states, particularly through the strengthening of domestic legal regulation, the development of alternative infrastructures, the expansion of content-blocking practices, and the formation of regional alliances based on sovereignty-oriented digital standards. This trend correlates with declining trust in multilateral institutions, increasing conflicts over digital jurisdiction, and the growing role of the state in internet governance. Authoritarian governments, by invoking the legal constructs of digital sovereignty, seek to legitimise their monopoly on the interpretation of digital rights and the definition of security standards, thereby transforming global digital interaction into a process subordinated exclusively to national interests. Their argumentation draws on the concepts of non-interference in domestic affairs and cultural pluralism, which precludes the establishment of universal mechanisms for monitoring digital rights violations at the global level.

According to studies by D. Flonk *et al.* (2020), G. De Gregorio & R. Radu (2022), and L. DeNardis *et al.* (2022), digital freedom depends on the architecture of access, which is shaped as a sociotechnical compromise between the state, civil society, and the private sector. The authors emphasise decentralisation as a key condition for innovation, digital privacy, and the support of democratic forms of self-expression within the networked environment. However, the analysis of KSA and Iranian policies reveals a different dynamic compared to previously formulated assessments: decentralisation there is not merely

absent but is deliberately counteracted, as the perceived chaos of the liberal internet is viewed as a source of external threat. This does not align with the conclusions of the cited authors, who view centralisation as a brake on development, whereas in the KSA and Iran it is deployed as a mechanism for ensuring digital stability and strategic control. The reason for these divergent interpretations lies in differences of value orientation: the studies invoke individual autonomy as the supreme digital value, whereas in authoritarian contexts a collectivist approach prevails, whereby stability, security, and manageability of the digital space are regarded as priorities. The researchers' conclusions are entirely pertinent for liberal democracies but require adaptation in cases where digital sovereignty functions as a mechanism of domestic political control rather than a guarantor of digital rights. International law currently demonstrates evident inertia in responding to new challenges posed by digital fragmentation. The absence of consolidated legal standards on internet governance, the lack of a universally recognised document regulating the interaction between state sovereignty and transnational digital flows, and the limited jurisdiction of international judicial and quasi-judicial bodies over digital violations create a regulatory vacuum. Existing legal instruments lack enforceable mechanisms in the digital domain, particularly with regard to states that refuse to adhere to universal standards. Multilateral platforms such as ICANN (n.d.) and the International Telecommunication Union (n.d.), despite their considerable technical and expert authority, do not possess the institutional capacity to prevent abuses of digital sovereignty. This contributes to growing asymmetry between states that comply with international obligations and those that disregard them. Under these conditions, it is necessary to develop a new international legal framework capable of effectively balancing the legitimate aspirations of states to control digital processes within their jurisdictions with the requirements of global interaction, technical interoperability, and the protection of fundamental human rights. Such a framework should include both legally binding provisions and mechanisms of political pressure, transparency, and accountability. Its key elements should be: first, the extension of the scope of international law to digital contexts, particularly in relation to human rights, jurisdiction, liability for harm caused by digital restrictions, and cross-border data flows; second, the enshrinement of universal standards regarding openness, net neutrality, non-discrimination, and proportionality of state interference in the digital sphere; and third, the creation of an institutional mechanism for monitoring compliance with digital rights, combining technical oversight, periodic reporting, and independent evaluation of state practices. In addition, international law should provide for a differentiated approach towards states with authoritarian regimes that systematically abuse the notion of digital sovereignty in order to legitimise repressive digital practices. Such an approach could include the development of sanction regimes against states that resort to long-term shutdowns, internet disconnections, or violations of the right to freedom of expression in the digital environment, as well as restrictions on the participation of such states in key multilateral internet governance platforms. At the same

time, it is important to maintain openness to dialogue by offering authoritarian governments conditions for gradual alignment with international standards through legal reforms, technical cooperation, and participation in transparent dispute resolution mechanisms. Global internet governance should not aim at unification, but rather at harmonisation of legal standards that guarantee a basic level of user protection regardless of jurisdiction. In this context, the role of international law is not confined to reacting to digital sovereignty, but lies in shaping a normative architecture capable of balancing states' legitimate security concerns with the necessity to uphold openness, stability, and interdependence of the digital sphere. Until this balance is achieved, the examples of the KSA and Iran will remain indicators of the transformation of the internet from a global public good into an arena of legal fragmentation and political rivalry.

### Conclusions

The study provides a comprehensive analysis of digital sovereignty policies in the Kingdom of Saudi Arabia (KSA) and the Islamic Republic of Iran as authoritarian states implementing national strategies for controlling the digital sphere amid intensifying geopolitical competition and the growing fragmentation of global internet governance. Digital sovereignty in both countries is examined as an instrument of internal stabilisation, regime preservation, and the projection of alternative visions of the digital order at the international level. The analysis reveals that both KSA and Iran pursue an ambivalent model of digital sovereignty, combining tools of technocratic modernisation with the systematic centralisation of control over data, platforms, and digital infrastructures. The legislative framework of KSA reflects a form of technocratic authoritarianism that prioritises economic development and the attraction of foreign investment while maintaining full state control over data. In contrast, Iran exhibits a security-ideological model oriented towards digital autarky and isolation from global information flows. In both cases, the primacy of national jurisdiction is asserted through data localisation requirements, restrictions on cross-border data transfers, and coercive measures or outright blocking of global platforms. In Saudi Arabia, high-tech institutions such as the Saudi Data and Artificial Intelligence Authority (SDAIA) and the Communications and Information Technology Commission play a central role, integrating supervisory functions with the management of digital transformation processes. Both countries demonstrate a systemic centralisation of access to internet infrastructure, state-supported development of alternative digital platforms, and the establishment of digital identification systems as instruments of pervasive surveillance. These practices directly conflict with international legal norms, particularly Articles 17 and 19 of the International Covenant on Civil and Political Rights, which guarantee freedom of expression, access to information, and the right to privacy.

The analysis of KSA and Iran's participation in international internet governance processes shows that both states promote the concepts of digital pluralism and a multi-global internet, asserting each nation's autonomous right to regulate its digital space in accordance

with its “national values”. Through diplomatic channels, engagement with the International Telecommunication Union, the Internet Governance Forum, and bilateral partnerships with countries of the Global South, these states advance alternative approaches to transparency, accountability, and human rights in the digital domain. This dynamic creates a hybrid tension between authoritarian and liberal interpretations of digital sovereignty, where the universalist foundations of international law are increasingly undermined by the rise of normative multi-vectority. The study’s limitations stem from restricted access to comprehensive data on state interference in digital infrastructure in both KSA and Iran. Future research directions include examining the responses of global technology

corporations to the regulatory demands of authoritarian regimes, comparing models of digital sovereignty across other Global South countries, and assessing the long-term implications of the regionalisation of digital law for the stability of the international legal order.

### Acknowledgements

None.

### Funding

None.

### Conflict of Interest

None.

### References

- [1] Al-Rawi, A. (2021). *Cyberwars in the Middle East*. Ithaca: Rutgers University Press. doi: 10.36019/9781978810143.
- [2] Anti-Cyber Crime Law of Saudi Arabia. (2007, March). Retrieved from <https://www.wipo.int/wipolex/en/text/498373>.
- [3] Asher, S. (2016). *What the North Korean internet really looks like*. Retrieved from <https://www.bbc.com/news/world-asia-37426725>.
- [4] Bria, F., & Sheikh, H. (2025). *Europe must avoid becoming a digital colony*. Retrieved from <https://foreignpolicy.com/2025/03/31/europe-digital-sovereignty-colony-trump-asml-ai-eurostack/>.
- [5] Brown, S.A. (2024). Beyond the great firewall: EU and US responses to the China challenge in the global digital economy. *Journal of European Integration*, 46(7), 1089-1110. doi: 10.1080/07036337.2024.2402752.
- [6] Celeste, E., & Fabbrini, F. (2021). Competing jurisdictions: Data privacy across the borders. In T. Lynn, J. Mooney, L. van der Werff & G. Fox (Eds.), *Data privacy and trust in cloud computing. Palgrave studies in digital business & enabling technologies* (pp. 43-58) Cham: Palgrave Macmillan. doi: 10.1007/978-3-030-54660-1\_3.
- [7] Cloud Oasis Saudi Arabia. (n.d.). Retrieved from <https://socialstationagency.com/project/cloud-oasis-saudi-arabia/>.
- [8] Constitution of Saudi Arabia. (1992, March). Retrieved from <https://www.legal-tools.org/doc/8942f2/pdf>.
- [9] Constitution of the Islamic Republic of Iran. (1979, December). Retrieved from [https://www.shora-gc.ir/files/fa/news/1398/9/21/4354\\_236.pdf](https://www.shora-gc.ir/files/fa/news/1398/9/21/4354_236.pdf).
- [10] De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, 30(1), 68-87. doi: 10.1093/ijlit/eaac004.
- [11] Del Re, E. (2024). Technologies of data protection and institutional decisions for data sovereignty. *Information*, 15(8), article number 444. doi: 10.3390/info15080444.
- [12] DeNardis, L., Musiani, F., & Ermoshina, K. (2022). *Concealing for freedom: The making of encryption, secure messaging and digital liberties*. Manchester: Mattering Press. doi: 10.1353/book.121036.
- [13] Digital Policy Alert. (2024). *DPA digital digest: Saudi Arabia*. Retrieved from <https://digitalpolicyalert.org/digest/dpa-digital-digest-saudi-arabia>.
- [14] Dragu, T., & Lupu, Y. (2021). Digital authoritarianism and the future of human rights. *International Organisation*, 75(4), 991-1017. doi: 10.1017/S0020818320000624.
- [15] Flonk, D., Jachtenfuchs, M., & Obendiek, A.S. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, 9(2), 364-386. doi: 10.1017/S2045381720000167.
- [16] Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, 3, article number 59. doi: 10.1007/s44206-024-00146-7.
- [17] Freedom House. (2024a). *Freedom on the Net 2024: Saudi Arabia*. Retrieved from <https://freedomhouse.org/country/saudi-arabia/freedom-net/2024>.
- [18] Freedom House. (2024b). *Freedom on the Net 2024: Iran*. Retrieved from <https://freedomhouse.org/country/iran/freedom-net/2024>.
- [19] General Assembly Resolution 2200A (XXI) “International Covenant on Civil and Political Rights”. (1966, December). Retrieved from <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- [20] Government of Saudi Arabia. (n.d.). *Smart government strategy (2020-2024)*. Retrieved from <https://my.gov.sa/en/content/smartstrategy>.
- [21] Gul, A., Abbasi, R.K., & Haider, S.A. (2021). Iran and Saudi Arabia’s strategic rivalry and the Middle Eastern security: An assessment. *Liberal Arts and Social Sciences International Journal (LASSIJ)*, 5(2), 17-29. doi: 10.47264/idea.lassij/5.2.2.
- [22] Hajipour, M.J. (2025). *Getting to know the Aparat website in Iran: The ultimate local video platform*. Retrieved from <https://drgaphic.net/en/getting-to-know-the-aparat/>.
- [23] Hardy, J. (2021). The rise of the modern intelligence state. In A. Henschke, A. Reed, S. Robbins & S. Miller (Eds.), *Counter-terrorism, ethics and technology: Emerging challenges at the frontiers of counter-terrorism* (pp. 105-120). Cham: Springer. doi: 10.1007/978-3-030-90221-6\_7.

- [24] Human Rights Council Resolution 54/24 “Cooperation with the United Nations, its Representatives and Mechanisms in the Field of Human Rights”. (2023, October). Retrieved from <https://docs.un.org/en/A/HRC/RES/54/24>.
- [25] ICANN. (n.d.). Retrieved from <https://www.icann.org/>.
- [26] Information Office State Council of the People’s Republic of China. (2010). *The Internet in China*. Retrieved from [http://www.china.org.cn/government/whitepaper/node\\_7093508.htm](http://www.china.org.cn/government/whitepaper/node_7093508.htm).
- [27] International Telecommunication Union. (n.d.). *Policy & regulatory frameworks*. Retrieved from <https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Policy-%26-Regulatory-Frameworks.aspx>.
- [28] International Trade Administration. (2024). *Saudi Arabia country commercial guide*. Retrieved from <https://www.trade.gov/country-commercial-guides/saudi-arabia-digital-economy-0>.
- [29] Jiang, M., & Belli, L. (2025). State-centric formations of digital sovereignty. In M. Jiang & L. Belli (Eds.), *Digital sovereignty in the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance* (pp. 39-102). Cambridge: Cambridge University Press. doi: 10.1017/9781009531085.003.
- [30] Jongen, H., & Scholte, J.A. (2021). Legitimacy in multistakeholder global governance at ICANN. *Global Governance: A Review of Multilateralism and International Organisations*, 27(2), 298-324. doi: 10.1163/19426720-02702004.
- [31] Joyce, C.B. (2025). Do states constrain non-state hackers? International telecommunication union elections and non-state cyber aggression. *Journal of Conflict Resolution*, 69(10), 1687-1712. doi: 10.1177/00220027251323557.
- [32] Kazemi, M. (2021). *The role of domestic messaging apps in Iran’s information controls*. Retrieved from <https://filter.watch/english/2021/11/30/the-role-of-domestic-messaging-apps-in-irans-information-controls/>.
- [33] Kleshnia, H. (2022). Cyber-social society: The latest rhizome. *Proceedings of the National Aviation University Series Philosophy Cultural*, 33(1), 45-51. doi: 10.18372/2412-2157.33.15641.
- [34] Law of Computer Crimes of the Islamic Republic of Iran. (2009, June). Retrieved from <https://ghazavatonline.ir/2105/the-law-of-computer-crimes/>.
- [35] Lawmaker says Iran behind bogus messaging apps, banned by Google. (2019). Retrieved from <https://en.radiofarda.com/a/lawmaker-says-iran-behind-bogus-messaging-apps-banned-by-google/29924990.html>.
- [36] Li, H., & Yang, X. (2021). Sovereignty and network sovereignty. In H. Li & X. Yang (Eds.), *Co-governed sovereignty network: Legal basis and its prototype & applications with MIN architecture* (pp. 1-28). Singapore: Springer. doi: 10.1007/978-981-16-2670-8\_1.
- [37] Martin, M. (2023). Algorithmic sovereignty: Machine learning, ground truth, and the state of exception. *Philosophy & Social Criticism*, 51(7), 1044-1074. doi: 10.1177/01914537231222885.
- [38] Mathew, A. (2024). *Cloud data sovereignty governance and risk implications of cross-border cloud storage*. Retrieved from <https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage>.
- [39] Mihelj, S., & Jiménez-Martínez, C. (2021). Digital nationalism: Understanding the role of digital media in the rise of “new” nationalism. *Nations and Nationalism*, 27(2), 331-346. doi: 10.1111/nana.12685.
- [40] Möllers, N. (2020). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology, & Human Values*, 46(1), 112-138. doi: 10.1177/0162243920904436.
- [41] Mueller, M. (2017). What “jurisdiction” does ICANN belong to? Retrieved from <https://www.internetgovernance.org/2017/11/07/jurisdiction-icann-belongs/>.
- [42] Mueller, M.L. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779-801. doi: 10.1093/isr/viz044.
- [43] NTIA. (2015). *Testimony of assistant secretary Strickling before the Senate Committee on Commerce, Science, and Transportation on “Preserving the multistakeholder model of internet governance”*. Retrieved from <https://www.ntia.gov/speech/testimony/2015/testimony-assistant-secretary-strickling-senate-committee-commerce-science-and-transportation>.
- [44] Olaje, J. (2025). *Vision 2030 in Saudi Arabia: A shift to digital governance*. Retrieved from <https://www.azeusconvene.com/articles/vision-2030-and-digital-governance-in-saudi-arabia>.
- [45] Oldenbourg, A. (2022). Digital freedom and corporate power in social media. *Critical Review of International Social and Political Philosophy*, 27(3), 383-404. doi: 10.1080/13698230.2022.2113229.
- [46] Overview of data sovereignty laws by country. (2024). Retrieved from <https://incountry.com/blog/overview-of-data-sovereignty-laws-by-country/>.
- [47] Panchenko, O.A., Parkhomenko-Kutsevil, O.I., & Antonov, V.G. (2020). Turbulence information challenges in governance. *Public Administration and Customs Administration*, 25(2), 196-204. doi: 10.32836/2310-9653-2020-2.34.
- [48] Payande, I. (2024). *Caught in the crossfire: The impact of sanctions on Iranian internet users*. Retrieved from <https://www.internetgovernance.org/2024/10/22/caught-in-the-crossfire-the-impact-of-sanctions-on-iranian-internet-users/>.
- [49] Personal Data Protection Law. (2023, March). Retrieved from <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>.
- [50] Raj, A. (2024). *Alibaba Cloud revamps global partnership ecosystem*. Retrieved from <https://www.crnasia.com/news/2024/cloud/alibaba-cloud-revamps-global-partnership-ecosystem-new-ai-fo>.
- [51] Regulation (EU) 2022/1925 of the European Parliament and of the Council “On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)”. (2022, September). Retrieved from <http://data.europa.eu/eli/reg/2022/1925/oj>.

- [52] Regulation (EU) 2022/2065 of the European Parliament and of the Council “On a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)”. (2022, October). Retrieved from <http://data.europa.eu/eli/reg/2022/2065/oj>.
- [53] Regulatory arrangements for the Saudi authority for data and artificial intelligence. (2019). Retrieved from <https://qanooniah.com/en/File/POZ1513E6qoWwivoe0G2BdaxD-Regulatory-Arrangements-for-the-Saudi-Authority-for-Data-and-Artificial-Intelligence>.
- [54] Resolution of the Supreme Council of Cyberspace “Document explaining the requirements of the national information network”. (2016, September). Retrieved from <https://rc.majlis.ir/fa/law/show/1033103>.
- [55] Reviglio, U., & Agosti, C. (2020). Thinking outside the black-box: The case for “algorithmic sovereignty” in social media. *Social Media + Society*, 6(2). doi: 10.1177/2056305120915613.
- [56] Ruohonen, J. (2021). The treachery of images in the digital sovereignty debate. *Minds & Machines*, 31, 439-456. doi: 10.1007/s11023-021-09566-7.
- [57] Saudi Arabia Data Sovereignty Policies and Requirements. (2024). Retrieved from <https://incountry.com/blog/saudi-arabia-data-sovereignty-policies-and-requirements/>.
- [58] Saudi Vision 2030. (2025). *2024 Annual Report*. Retrieved from <https://www.vision2030.gov.sa/en/annual-reports>.
- [59] Schlumberger, O., Edel, M., Maati, A., & Saglam, K. (2024). How authoritarianism transforms: A framework for the study of digital dictatorship. *Government and Opposition*, 59(3), 761-783. doi: 10.1017/gov.2023.20.
- [60] Sexton, M., & Campbell, E. (2020). *Cyber war & cyber peace in the Middle East: Digital conflict in the cradle of civilization*. Washington: Middle East Institute.
- [61] Shaharuddin, A.A., & Ilias, M. (2024). *Digital transformation in the middle east: Insights from the digital double bind*. *Journal of Development Communication*, 35(2), 87-88.
- [62] Shahbaz, A., Funk, A., & Hackl, A. (2020). *Assessing the human rights implications of data localisation*. Retrieved from <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty>.
- [63] Shany, Y. (2023). Digital rights and the outer limits of international human rights law. *German Law Journal*, 24(3), 461-472. doi: 10.1017/glj.2023.35.
- [64] Sheikh, H. (2022). European digital sovereignty: A layered approach. *Digital Society*, 1, article number 25. doi: 10.1007/s44206-022-00025-z.
- [65] Supreme Council of Cyberspace. (2022). *Strategic Document of the Islamic Republic of Iran in Cyberspace*. Retrieved from <https://zaviehmag.ir/?p=1787>.
- [66] Svantesson, D.J. (2021). *Private international law and the internet*. Retrieved from <http://digital.casalini.it/9789403511245>.
- [67] Taldykin, O. (2024). Sovereignty: Attempted classification. *Scientific Bulletin of the Dnipro State University of Internal Affairs*, 1, 125-129. doi: 10.31733/2078-3566-2023-1-125-129.
- [68] UNESCO. (n.d.). *World Summit on the Information Society (WSIS)*. Retrieved from <https://www.unesco.org/en/wsisis>.
- [69] United Nations. (2021). *Group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security*. Retrieved from <https://digitallibrary.un.org/record/3934214?v=pdf>.
- [70] United Nations. (2022). *UN human rights experts urge Iran to abandon restrictive internet bill*. Retrieved from <https://www.ohchr.org/en/press-releases/2022/03/un-human-rights-experts-urge-iran-abandon-restrictive-internet-bill>.
- [71] Vienna Convention on the Law of Treaties. (1969, May). Retrieved from <https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf>.
- [72] World Trade Organisation. (1995). *General Agreement on Trade in Services*. Retrieved from [https://www.wto.org/english/docs\\_e/legal\\_e/gats\\_e.htm#art3\\_3](https://www.wto.org/english/docs_e/legal_e/gats_e.htm#art3_3).

УДК 355.02  
DOI: 10.59214/ua.fa/5.2025.132

**Азіз Ісаєв**

*Аспірант*

*Дипломатична академія Міністерства закордонних справ Киргизької Республіки імені Кази Дікамбаєва  
720040, просп. Еркіндік, 36, м. Бішкек, Киргизстан*

<https://orcid.org/0009-0005-5823-4277>

## **Еволюція військової політики в державах Центральної Азії в пострадянський період: між спадщиною СРСР і новими загрозами**

**Анотація.** Мета дослідження – проаналізувати зміни у військовій політиці країн Центральної Азії, з особливим акцентом на Киргизькій Республіці, після розпаду Радянського Союзу в 1991 р. У дослідженні було використано контент-аналіз військової доктрини та концепції національної безпеки Киргизстану, порівняльний аналіз військових доктрин країн Центральної Азії – Киргизстану, Казахстану, Таджикистану, Туркменістану та Узбекистану – а також підхід на основі конкретних прикладів щодо прикордонного конфлікту з Таджикистаном у квітні-травні 2021 р. та шестиденного збройного конфлікту з Таджикистаном у вересні 2022 р. Результати показали, що після розпаду Радянського Союзу Киргизстан зіткнувся з такими викликами, як фрагментована військова інфраструктура, недостатність ресурсів та ризики транскордонних конфліктів. Ці ризики призвели до перегляду військової доктрини та стратегії національної безпеки в період з 2021 по 2023 р. Відмінною рисою зміненої військової політики є прагнення до нейтралітету, мирного вирішення конфліктів та зосередження уваги на трансформації загроз – гібридних, інформаційних та кібернетичних. На відміну від інших країн Центральної Азії, військовий бюджет Киргизької Республіки обмежений 1,5 % валового внутрішнього продукту, що спонукає країну уникати гонки озброєнь і обирати більш технологічний підхід до національної безпеки. Брак коштів для масштабного переозброєння компенсується участю Киргизстану в міжнародних альянсах і військових навчаннях, а також згодою на обмежену присутність іноземних військ. Досвід Киргизстану можна використовувати для запобігання транскордонним конфліктам, створення інтегрованої системи безпеки та забезпечення стабільного регіонального розвитку

**Ключові слова:** національна безпека; транскордонний конфлікт; регіональна безпека; міжнародні альянси; військові навчання

### **Вступ**

Розпад Радянського Союзу (СРСР) призвів до змін у військовій політиці центральноазіатських держав – Казахстану, Таджикистану, Туркменістану, Узбекистану та Киргизької Республіки. Колишні члени союзу зіткнулися з такими викликами, як фрагментована військова інфраструктура та вразлива система безпеки. Актуальність цієї роботи полягає в розумінні того, як центральноазіатські країни трансформували свою військову політику, щоб подолати ці виклики та створити індивідуальну траєкторію в змінених реаліях. O. Göksel & N. Huseynova (2024) у своєму дослідженні вказали на значний вплив СРСР на формування політичного порядку денного в країнах Центральної Азії. Використовуючи постколоніальну теоретичну модель, цитовані експерти стверджували,

що радянська політика на Кавказі та в Центральній Азії набула форми політичних репресій, економічної експлуатації та культурної асиміляції, виявляючи ключові риси колоніального правління. Z. Khonelidze & M. Bregvadze (2024) підкреслили, що після закінчення Другої світової війни розпад Радянського Союзу став другою за значимістю історичною подією, яка привернула увагу світової спільноти до питань мирного співіснування нових незалежних держав. Згадані експерти відзначили пріоритетність міжнародного співробітництва, що призвело до створення процедур забезпечення військової безпеки в регіоні. Ö.F. Kocatepe & M. Şahin (2024), однак, звернули увагу на недостатню ефективність реалізованих протоколів, оскільки через десятиліття після розпаду СРСР Центральна Азія

*Отримано: 06.07.2025, Перевірено: 25.09.2025, Прийнято: 26.10.2025*

### **Suggested Citation:**

Isaev, A. (2025). Evolution of military policy in Central Asian States in the Post-Soviet period: Between the legacy of the USSR and new threats. *Foreign Affairs*, 35(5), 132-141. doi: 10.59214/ua.fa/5.2025.132.

\*Corresponding author



Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)