LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. 10(2025)

LEGISLATIVE FRAMEWORK REGULATING DIGITAL MEDIA IN JORDAN AND ARAB COUNTRIES: A STUDY ON THE LEGAL DIMENSIONS

Yousef Awad Al-Mashaqbeh[1]

[1]Department of Journalism and Digital Media, Zarqa University, Zarqa, Jordan
Orcid: **https://orcid.org/0009-0006-1148-1585**

yalmashaqbeh@zu.edu.jo[1]

Abstract
This paper reviews the legal structures governing digital media in Jordan and some of the Arab nations, and their correlation with their legal aspects and their freedom of speech, privacy, and their governance online. Arab states have over the last ten years developed different laws to manage emerging issues like cybercrimes, misinformation, and protection of data. The Cybercrime Law No. 17 of 2023 in Jordan is a major reform since it clarifies the action of online character assassination as a criminal offense, but is also indicative of the wider trend in the region of valuing state security at the expense of digital rights. A method of comparisons with Egypt, Saudi Arabia, the United Arab Emirates and Lebanon makes it clear that there do exist similarities and divergences: a restrictive approach in Egypt and Jordan, a comprehensive and rights-oriented approach in the United Arab Emirates, a partial approach meeting international standards in Saudi Arabia and a weak and fragmented legislation in Lebanon. It also focuses on how local political, cultural, and economic environments affect the development of such laws and positions them in comparisons with some international examples, in particular, the rights-oriented GDPR introduced into the EU and the U.S. market-oriented, free-speech based. The results indicate that despite the improvement, the Arab laws on digital media are largely security-oriented and pose a threat to democracy. The recommendations include rights-based reforms, more judicial review, regional alignment, and civil society contribution to promote balanced, transparent, and international-consistent digital governance in the Arab world, which concludes the paper.

Keywords: Digital Media Regulation; Cybercrime Law; Freedom of Expression; Data Protection; Jordan; Arab Countries; Comparative Legal Analysis; International Standards; Cybersecurity; Human Rights.

Introduction

There has been no doubt that in the last 20 years media has undergone sweeping transformation whereby dependence on traditional sources of the media like print media and broadcast TV is being replaced with a digital dominated media. It is in Jordan that this transformation has been highly profound, with online news sources, blogs and social media networks like Facebook, Twitter and Tik Tok becoming the main avenues of communication, politics, and social life. In the broader Arab region, digital media has also been extremely integrated into the political and cultural culture, especially following the Arab Spring, of which online platforms were instrumental when it came to the mobilization and organization of the masses and a certain shaping of narratives.

Digital media has opened even more possibilities in the sphere of participation, free speech, and instant sharing of information as well as innovated challenges. The emergence of disinformation, hate speech, cybercrime, and privacy violations have caused the increasing interest of policy makers and legal scholars. In turn, the governments of Jordan and the rest of the Arab world have tried to present laws regarding the regulation of digital space and combating the danger of uncontrolled online content dissemination (Freedom House, 2024).

The digital media environment requires the creation of clear legal frameworks in controlling the environment. On the one hand, the legal framework is required to guard the societies against dangerous activities like incitement to violence, online abuse and dissemination of fake information. In other cases, over regulation, or legal formulations that lack clarity may be used to violate basic freedoms, especially the freedom of expression and information access, both of which are provided in international human rights instruments. Preserving societal order and securing freedom of press is one of the key dilemmas of the legislative strategy to regulating the digital world (Reporters Without Borders, 2023).

Scholars in Jordanian media environment have pointed out that one continuous challenge that remains a major problem within the Jordanian context has been containment strategies on journalists who tend to hurt professional indecisiveness. According to the results by Alsafouri (2020), self-censorship is also impacted by both soft and hard forms of containment, where there is a mixture of both legal and social constraints. These observations are very much applicable to the study of the effects of the digital media legislation since they help impart how even a law can indirectly strengthen a trend of journalistic self-censorship.

The argument on whether to regulate digital media or not is an issue of concern not limited to the legal control of Jordan and other Arab countries but also covering the national law adaptation to the international norms along with the satisfaction of local needs in terms of culture, political, and security needs. That is why the legal structures established in the region are a topic that should not be disregarded to figure out the way Arab states act to meet the demands of the digital age.

Research Problem and Objectives

The main issue that the current study is exploring is whether the laws that govern the digital media in Jordan and some selected Arab nations are effective in balancing both state control and human rights. More precisely, do such laws prevent online harms in societies without violating the essential rights, or do they gravitate toward repressive paradigms that freeze the democratic participation in the digital domain?

The objectives of the study are:

- To examine the legal framework that digital media in Jordan is regulated with special emphasis on the Cybercrime Law (17 of 2023) and the Media and Publications Law.
- To propose a comparative case study of digital media regulation in a few Arab nations of interest (e.g., Egypt, Saudi Arabia and the United Arab Emirates) to identify similarities and differences in approach to such a legal framework.
- To discuss the consequences of the development of these legal frameworks to freedom of expression, privacy and the trust of citizens in digital communication.
- To suggest to the policymakers how more balanced, transparent, and rights-based digital media regulations could be designed in the Arab world.

Research Methodology

The current study is comparative in nature and incorporates legal analysis of the current laws with secondary sources review, such as reports prepared by international freedom of press agencies, Freedom House, Reporters Without Borders (RSF), Committee to Protect Journalists (CPJ), etc. Case studies will be reviewed in Jordan and a few Arab countries to evaluate the application of such laws in reality as well as their inconsistency / compatibility with international practices of freedom of expression and digital rights. To provide a fuller picture of the

consequences of the digital media regulation in the terms of social and political implications, recent academic literature will be also referred to during the analysis.

Theoretical Framework

Definition of Digital Media in Legal Terms

The matter of digital media is all encompassing and complex as the term is used in the legal language. Nevertheless, the concept of digital media can hardly be accepted as a fixed term, leaving it rather vague most of the times. This confusion is because of the ever changing nature of digital platform which keeps introducing new type of communication and interaction that pushes the boundaries of the current legal system. Consequently, the concept is perceived differently in different jurisdictions depending on the nature of culture, politics, and regulations under which it is being operated. Therefore, the legal perception of digital media should be dynamic that resembles both the continuation of the conventional media operations and the innovativeness aspects in the digital era.

In a strict sense of definitions, digital media could be viewed on both a broad and a narrow perspective. In its comprehensive definition, digital media is defined as any kind of content that is spread using online technologies, including websites, blogs, social media, and streaming ("European Courts as Digital Media Regulat...", 2022). This broad definition encompasses the variety and the rapidly growing channels of communications available through the internet and other forms of digital infrastructures. On the other hand, in its limited meaning, the term can be limited to the modernization of conventional media forms into the digital one, including online newspapers, digital television, and electronic audience of print publications("European Courts as Digital Media Regulat...", 2022). The parallel of these two strands of definition is an indication of the difficulty associated with taking one, comprehensive definition that applies across the board when the definition of digital media tends to broaden as new technological applications and features are developed.

Regulatory issues are the other challenge in the legal environment of the digital media. National and international laws, policies, and standards that govern digital ecosystems around the world include a patchwork of varying, overlapping, and inconsistent ones. The result of such fragmentation is a regulatory landscape that is convoluted to traverse, as states are trying to exert their grasp on digital realms, and at the same time be subject to international commitments to the freedom of expression and human rights ("European Courts as Digital Media Regulat...", 2022). These contradictions in this framework not only confuse the soundness of legal norms but also the issue of implementation of such regulations beyond the national jurisdiction may also have some questions especially in the transnational context of digital places.

Another aspect of the legal definition of the digital media pertains to the intervention of the judiciary. Sometimes, in most situations, courts are referred to as co-legislators, who fill the loopholes opened by unclear or obsolete legal provisions. Case laws prove to be relevant sources in defending the limits of digital media, assigning liability to internet encounters, and balancing between the right to freedom of speech and privacy ("European Courts as Digital Media Regulat...", 2022). This legal practice highlights the dynamic and changing approach toward the regulation of digital media where legal meaning is not only determined through the legislative construction but is continually followed through interpretation, to derive meaning relative to the new technological realities.

To some extent research on Jordanian journalism demonstrates that the practices of containment are closely related to legal ambiguities and proffer confused provisions in media laws. Alsafouri (2020) The fear of punishment and prosecution by the law makes the journalists apply self-regulations, and this can be compared to the larger picture of mighty ambiguity in regulating the digital media. This fact further compliments the idea that although legislation is meant to hold people responsible it could be that it leads to the culture of silence and conformity instead of true expression.

The legalities of digital media are not confined to the definition and scope as numerous functional areas of legal effect are also present, which have a direct impact on the media producers, distributors, and consumers. Among the most important dimensions, one can mention the aspect of rights management, licensing, and contractual matters. Rights clearance and licensing of content pose tougher problems in the digital environment because the digital mediums permit the distribution of media products across the world with one click. This entwinement further increases the significance of well-defined legal agreements in order to safeguard the interest of both content creators and distributors with a view of respecting intellectual property well as fulfilment of contracts (Williams et al., 1998). In the absence of such protection, the chance of contention on the ownership and the right to distribution intensifies accordingly at the cost of the long-term sustainability of digital media industries.

Another implication is on the changing nature of legal standards based on technological innovation. As digital platforms spread and diversify, the legal systems are in constant pressure that requires them to modify their regulation framework. Copyright infringement, sharing of unauthorized contents, recovering of information, and privacy rights have been issues that depict the struggles of legislators in coping with the fast-changing technology. Within the legal circles, there is a strong sentiment that the prevailing laws should always be redefined or revised to keep up with new customs in the digital age, especially when it comes to the security of personal information and when one considers fair use of the content (Packard, 2010). By this, the legislation should be dynamic and progressive, with the capacity to counter the emerging risks and at the same time protect the already established rights.

However, critics claim that at times, technological advancements tend to overwhelm legal structures, and indeed, the speed of technological changes usually overtakes the ability of laws to react in a suitable way. Such a delay may cause regulatory gaps, when current regulations are not sufficient in meeting new challenges provided through digital platforms. As an example, recent challenges like the creation of content in artificial intelligence, the boosting of harmful speech with algorithms, and the jurisdictional conflict across borders serve as examples of how it is very challenging to apply the conventional concepts of the legal duty in the fast-evolving reality. So, concerns have been expressed regarding relevant outcomes to be achieved through existing legislative and judicial processes to regulate compliance and protection of rights whether in a more online or digital world (Reed, 2022; Packard, 2010).

Role of legislation in balancing freedom of expression and regulation

The relationship between freedom of expression and regulation has seen legislation play a more central role in the new digital age where the internet offers an open platform to express multiple opinions, political dialogue and sharing of information worldwide. As much as digital media enhances new participation and access opportunities that were otherwise unattainable, they have brought with them major problems in the form of harmful or illegal content, misinformation, and

breach of privacy. It is against this background that, legislation has become a strategic entity to balance between two competing necessities, which include the need to secure the foundational rights; especially the right to free expression and the need to ensure people and communities against the damage that the unregulated online communication may cause. This balance needs to be achieved so that online spaces should be at the same time safe and inclusive, and there is no necessity to jeopardize the democratic principles.

Mshaqaba (2021) accentuates that the influence of the legal regulation of the sphere of digital media in Jordan might impact journalistic activities in higher or lower limits of freedom or restraint. His conclusions indicate that the ambiguity of legal norms usually leads journalists to self-censorship, a fact that highlights the idea that the legal wording can disfavor the independence of the profession in a digitized media content.

The most fundamental issue in this balancing act happens to be legal frameworks drawing clear parameters that must be used to balance the freedom of information with the individual within a way that is not disproportionate. As an example, the General Data Protection Regulation (GDPR) in the European Union and Lei Geral de Protecao de Dados (LGPD) in Brazil are laws that offer rules on the treatment of personal data that contribute to preserving user privacy and, at the same time, allow expressing freedom of speech (Lima et al., 2024). These structures present the idea that regulation can be very empowering because it can protect the individual rights of people and encourage free flow of communication by building confidence in online spaces. On the same note, the hate speech laws are aimed at remedying the destructive nature of discriminatory or inciting communications using the intricate nature of free speech rights as a navigation tool (Thuku & Mbaaro, n.d.). In demonstrating this understanding of the possibility of certain threats posed to the social fabric, security and equality by uncontrolled harmful speech, these legal measures consider reasonable restrictions as a valid alternative to the rights framework.

Another aspect of such process of balancing is expressed in the realm of content moderation where both the state and private parties are becoming more engaged. An example is the internal moderation policy created by social media platforms where new policies regulate harmful content, misinformation and online harassment. Although these kinds of policies are sometimes needed to provide safe digital environments, they do generate the concern that these policies can be exercised in excess, with the private corporations, essentially, becoming the censors of speech and the authorities to curtail the speech in ways that did not require a high level of transparency and accountability (Lima et al., 2024; Şahin, 2022). An appropriate legislative response to such issues should offer mechanisms of oversight which guarantees moderation acceptable to democratic ideals and safeguarding users against any form of damages that might be meted on them without necessarily leading to excessive censorship. Researchers stress that effective legislation needs to be flexible toward new technological advancements and shifts in society, so that not only rules can help to ensure safety, but also guarantee freedom of the expression (Gomathy et al., 2024; Sieckmann, 2019).

International Models of Digital Media Regulation (EU, USA)

The topic of the regulation of the media within a digital environment reveals both the traditions of the legal cultures but also it reflects the richer cultural, political, and economic backgrounds. Some of the strongest global models include those formulated in the European Union (EU) and the United States (USA). Despite similar issues between the two regions, including combatting the spread of misinformation, preserving privacy of the users, and managing the activities of

online platforms, the approaches of regulation vary greatly. The EU has approached it with rights-based approach and therefore it has focused more on the rights of an individual embodied in using their freedom as well as security of their data and accountability of digital players. In comparison, the United States takes a subjective approach, with a market-based model emphasising free speech, innovation and limited state action, and this point can be attributed to the prominent place of the first amendment in the American constitutional regulations. The two opposing models also shed light upon how varied and different approaches to the digital media governance complexities can be.

The regulatory framework in the European Union can be described as being quite broad and highly focused on safeguarding the rights of an individual. The notable exponent of such approach is the General Data Protection Regulation (GDPR) that has now become an international standard regarding data protection regulations (Fukuyama & Grotto, 2020). Besides placing extremely stringent demands on any collection, storage and processing of a personal data, the GDPR also gives a substantial rights over digital identity to users, meaning that they can demand access, correct or delete their data. In addition to privacy, there are certain EU laws on more harmful existing online practices, including a law in Germany that penalizes social media platforms that do not take down hate speech and misinformation and requires strict time limits, with huge fines in case of failure (Fukuyama & Grotto, 2020). There is a reason that the EU displays such committed measures to making sure that digital spaces are safe, transparent, and respect the dignity of human beings, although such regulation sometimes can be very burdensome to the platform to comply with.

Conversely, there is a more liberal approach to control digital media in the United States whereby it embraces laissez-faire supported by the constitution which offers the freedom of speech under the first amendment. Such focus on free speech complicates the political and legal attempts to directly restrict the content made online, even in the misinformation or harmful speech cases (Fukuyama & Grotto, 2020). Rather, the most recent element of U.S. regulation debates has been indirect through regulation, including antitrust to combat the strength of large technology players and consumer privacy protection proposals (Monti, 2022). Comprehensive federal regulations on the same scale as the GDPR have not been established, however, thus leaving the U.S. regulatory environment more disjointed with state-level efforts, like the California Consumer Privacy Act (CCPA) filling the gap. Although this has been an innovative way that reduces government interference, it has been criticized as a way to give the users more exposure to data abuse, corporate excesses, and an unregulated harmful content.

The European Union (EU) and the United States (USA) differ more than in the regulation of the digital media regarding their legal traditions and underpinned by intellectual principles of regulatory approaches. These western attitudes play a significant role and have a powerful impact on the perception of the balance between freedom, responsibility, and state intervention in digital space of the respective regions.

Digital regulation is perceived as an important tool of safeguarding democratic values and securing individual rights according to European point of view. Digitalized space is viewed by the EU as part of the public space where the discussion should follow the rules of fairness, inclusiveness, and human dignity (Sanz, 2024). Regulatory interventions are therefore usually intended as rational extensions of enduring media legislation traditionally aimed to assure accountability, discourage media concentration of authority, and preserve the quality of debate.

In this sense, acts like the GDPR or the NetzDG are not viewed as an intervention into free speech but instead as a form of protection, which will make the digital space play a positive role in democratic debate (Fukuyama & Grotto, 2020). This view shows the EU powerful Case of rights-oriented approach such that regulation is placed in the context of taking care of citizens against abuses of power, by states or by the business enterprises.

In comparison, United States imposes the regulation of digital media in the framework of cultural and political scheme that values market freedom and innovation exceptionally highly. The attitude of the American regulatory environment is based on the historical distrust of government intervention, which involves the tradition of liberal economics and a constitutional adherence to freedom of speech. This has created a perception that digital space and non-state actors are more effective than the state to regulate online interactions leading to an affinity towards self-regulation and voluntary codes of conduct (May et al., 2004). Strict measures of regulation are quite unpopular in the political discourse in the U.S. as they are discussed as the possible threats to the entrepreneurial creativity, technological advancement and freedoms of the First Amendment. In more recent years, this philosophy has been supported by claims that the government intervention may limit the innovation in a field where renewed and speedy adaptation and competition are the driving factors (Bradford, 2023).

This difference between EU and U.S. approaches, thus, implies the difference of larger cultural values: European societies are more inclined to trust the role of regulation as their main protection device of democracy and individual rights, whereas the United States prefers the mechanisms of the market and individual liberties. Such political and cultural grounds are not only the explanation of the variations of the already existing laws but also the kind of acceptance or non-acceptance of the regulatory intervention when applied in each area.

Table1.Comparative Table: EU vs. USA Approaches to Digital Media Regulation

Aspect	**European Union (EU)**	**United States (USA)**
Regulatory Philosophy	Democracy- and accountability-focused, rights-based on the user, democratic-based, resting on the values of democracy and accountability (Sanz, 2024; Fukuyama & Grotto, 2020).	Laissez-faire-oriented, focused on the 1st Amendment and innovation, and imposing the least amount of involvement (May et al., 2004; Bradford, 2023).
Key Legal Frameworks	Data protection: the GDPR; fighting hate speech and fake news: the NetzDG (Fukuyama & Grotto, 2020).	The state-based legal framework (i.e. CCPA); the deployment of antitrust and voluntary practices (Monti, 2022).
Cultural Orientation	Regulation as a logical extension of old media legislations and a protection against impairment of discourse in the whole population.	High regard toward individual liberties, market based invention of entrepreneurs and self-determination.
Approach to Free Expression	Strongly roots in supporting freedom of speech but with moderation against dangerous material and sets restrictions on hate speech and disinformation.	The protection of the First Amendment renders the rules that govern harmful content hard politically and legally.
Public Perception	Regulation that is generally considered to be needed in terms of protection of democracy and social solidarity.	Regulation is something that can be very suspicious as it is sometimes projected as an intrusion by the government that can suppress free expression.

Legislative Framework in Jordan

The Jordanian legal framework that regulates the field of digital media and cyber-related crimes started developing in the last ten years under the influence of swelling popularity of cyber communication technologies and the surging in the number of internet crimes. This framework is based on two main legislations: the Cybercrime Law No. 27 of 2015 and the newer Cybercrime Law No.17 of 2023. In combination with each other, these laws signify the state in Jordan seeking control over the spaces of the digital world, defending people against threats of online hate, and the introduction of legal frameworks to punish the threat of electronic defamation, libel, slander, and character assassination. Nevertheless, the efficacy and efficacy of the legal system are contentious issues among academicians, policy makers, and civil society groups especially where there is a conflict between the interests of the state and safeguard of human fundamental rights.

Cybercrime Law No. 27 of 2015

The Cybercrime Law No. 27 of 2015 was the earliest piece of legislation that Jordan had its first piece of comprehensive legislation on dealing with crimes in the digital area. This was illegalized because of the use of electronic defamation, libel, and slander, something that had become highly frequent due to the adoption of social media and the creation of communication networks. Employing this criminalization of these acts, the legislation sought to protect the reputation of people and victims of character assassination by giving them judicial protection in the cyber space (Al-Zoubi, 2023).

Nevertheless, irrespective of these aims, the law was soon noticed to be rather narrow both in terms of its scope and estimated effect. As an example, most of the provisions of the 2015 law were dependent on the supporting legislations, especially the Jordanian Penal Code and the Code of Criminal Procedures to be executable. This interdependence pointed out the inadequacy of the law as a solitary tool in dealing with the cybercrimes effectively. Some critics said that the law passed in 2015 had no holistic framework that could deal with various and increasingly dynamic nature of cybercrime, including but not limited to financial fraud, hacking, online harassment and privacy infringement (Al-Zoubi, 2023). Additionally, the vagueness of the law was frequently attacked which gave way to wide interpretation and in other instances, exposure to abuse.

Moreover, the law was not sufficient to consider the fast changing technology and appearance of the new aspects of online abuse. Although it served as the basis of prosecuting some cybercrimes, it was not able to stay abreast with the global trends in digital regulation especially in data protection, standards of cybersecurity and protection against cross-border digital offenses. These deficiencies were calls to action in terms of a more modernized and comprehensive reaction to the current situation in the legal field and eventually led to the adoption of the 2023 Cybercrime Law.

Information Systems Crimes Law No. 30 of 2010

Information Systems Crimes Law No. 30 of 2010 is one of the initial legislation initiatives that the Kingdom of Jordan attempted to control in relation to criminal acts and to toughen the legal circumstances that could arise during electronic transactions. Being considered as an amendment to the Electronic Transactions Act No. 85 of 2001, this legislation was concerned with the new threat to the criminalization of digital technologies, such as unauthorized access to a much-needed information system or data manipulations, and other crimes which can be related to computer world (Faqir, 2013). The introduction of such a law represented an innovative move

towards cyber law in Jordan and this can be attributed to their increased sensitivity towards the importance of developing regulatory tools that specifically address the phenomenon of technological changes and the recent rise of digital crime.

Though it is questionable with intentions and is innovative, the law has attracted much criticism amongst legal academicians and practitioners. The major one is based on the un-concreteness of its provisions that have fostered interpretative ambiguities and difficulty in the enforcement process. General nature of terms used in the law, and the absence of specific definitions of important crimes have at times been a deterrent in applying the law as there have been loopholes that may be utilized by cybercrime offenders (Faqir, 2013). The law has also suffered criticism in that it has less guidance in terms of procedures. As compared to newer bills, it regulates very little in regards to how an investigation is conducted, how evidence is gathered, and how a prosecution needs to be done when it comes to cyber-crimes and that is why it is weak in execution.

In addition, the law has some legal and language flaws such as inconsistencies in the terminologies used and drafting flaws, making the laws difficult to implement and leading to possible uncertainty of legal interpretations. These failures serve to emphasize the need to continuously review and update the legislation in order to make it up to date and have the capability of dealing with the dynamism of the nature of the cyber threats. The shortcomings of the 2010 law hence illustrate the necessity of the following changes such as the installment of the Cybercrime Law No. 17 of 2023 that aimed at creating a more scrupulous, holistic, and technologically adequate terrorism against cyber-crimes in Jordan.

Cybercrime Law No. 17 of 2023

The Cybercrime Law No. 17 of 2023 is the most recent step toward legislative reform in the field of digital crimes in the Jordanian context, the new law is supposed to keep Citizens safe of the unknown dangers of the internet. The fact that the law directly criminalizes any activities of character assassination, which is understood as the deliberate moral ruin and social alienation of a person by spreading false allegations, rumors, or other defamatory materials in a digital environment (Al-Amawi & BALAS, 2024; Alqudah et al., 2024; Al-Amawi, 2023), should be considered one of the most outstanding aspects of the law in question. Because it is directly responding to such crime, the law of 2023 represents a major break with past legislation, which often addressed defamation and related harm in a more diffuse or piecemeal way, based on earlier laws, like the Cybercrime Law No. 27 of 2015 or the Information Systems Crimes Law No. 30 of 2010.

The legislation is a new approach that brings harsher punishment to the criminals due to a more pro-active approach towards cultivating the laws rather than simply punishing the offenders. This trend indicates that the Jordanian legislature is well aware of the social and psychological effects of online harassment and character assassination especially when it happens online where malicious arguments may be propagated instantly and in a permanently scarring impression. The 2023 law may be considered to fill existing gaps identified in the previous laws since it will be more legally explicit and include strict penalties as compared to the earlier laws in question (Alqudah et al., 2024; Al-Amawi, 2023).

In addition, the law is indicative of a wider legal transition of a more extensive liberal cyber legislation in Jordan. Compared to the past laws that were being criticized due to lack of specific points, procedural flaws, and insufficiency to account new cyber threats, the 2023 legislation

incorporates the current norms of the regulation of laws and is nearer to the practices of the world community in this direction. It highlights adherence to striking the right balance between personal and societal rights and the best interests of digital governance with the aim of protecting the reputation, deterring online crimes, and fostering a secure virtual space. The given evolution of the legislation indicates that Jordan actively copes with the present-day issues that are associated with the digital transformation and the intensifying spread of online platforms both on personal and professional levels.

Table2. Comparative Analysis of Jordanian Cybercrime Legislation (2010–2023)

Aspect / Law	**Information Systems Crimes Law No. 30 of 2010**	**Cybercrime Law No. 27 of 2015**	**Cybercrime Law No. 17 of 2023**
Purpose / Focus	Control offenses which are computer related; amendment to Electronic Transactions Act No. 85 of 2001 (Faqir, 2013).	Combat electronic defamation, electronic libel, electronic slander; ward off common cybercrime (Al-Zoubi, 2023).	Ridicules actions on the basis of character degradation and online defamation; broader umbrella against injury in the web (Al-Amawi & BALAS, 2024; Alqudah et al., 2024).
Scope of Offenses	Granted access without authority, data alteration, hacking, scanty coverage of the new cyber offenses.	Defamation electronically; electronic slander, libel; reliant on the Penal code and the Code of Criminal Procedure to be implemented.	In line with the above, character assassination, defamation, spreading false information; all sides of the coin of online reputation injuries are covered.
Strengths	The first statute of Jordanian cyber laws; first effort to control the computer crimes.	The legal licensing of electronic defamation and other crimes; outlined the means of prosecuting cybercrimes.	Modern system of law; defined offences; heavier punishments; more consistent with the international practice; covers the loose ends of older legislation.
Weaknesses / Criticisms	General clauses; tattoos of insufficiency; absence of procedural regulations; legal and terminology flaws (Faqir, 2013).	Scarcity of envisaging; inadequate laws; only good enough to curb cybercrime (Al-Zoubi, 2023).	None of the significant weaknesses have been reported so far; it is an active law-making effort that was intended to be implemented effectively, but its efficiency is not determined yet.
Penalties / Enforcement	Narrow and arbitrary; procedural	Moderate penalties; not so effective as it depends on	Greater and targeted punishment on character

	ambiguities are a drag.	the other laws.	assassination and slander; to enforce more strongly in court.
Technological Adaptation	Narrow; failed to take into account all aspects of new cyber threats.	Partial adaptation; there are certain gaps in internet changes in the approach.	Thorough adaptation; demonstrates the knowledge of the current digital platforms and social media patterns.
Legal Clarity	Succinct words; capable of wide interpretation.	Severe incomprehensibility; parts restrictive.	Great transparency; clear definition and stipulated guidelines to character assassination and internet defamation.

Table 2 shows the change in the Jordanian laws on cybercrime since the year 2010. It demonstrates the gradual increase in breadth and explicitness in the legal frameworks with an update in the initial Information Systems Crimes Law No. 30 of 2010 by narrowing the focus to cyber-related crimes and enshrining it in the Cybercrime Law No. 27 of 2015 and culminating with further expansion of the legal framework to cybercrimes in general and highlighting the offense of character assassination and intensifying its enforcement in the Cybercrime Law No. 17 of 2023. The table highlights the ongoing adjustment of the Jordanian laws to new digital risks and the strengthening of legal classification and safeguard of the person rights.

Legislative Framework Regulating Digital Media in Selected Arab Countries: Comparative Analysis

The legislative systems of selected Arab countries, namely Egypt, Saudi Arabia, the United Arab Emirates (UAE) and Lebanon that control the digital media environment prove to be very diverse, which points to the impacts of socio-political realities, the priorities of economies, and the achieved technological advancements. Countries have developed national legal mechanisms that support their situation in respect of digital trade, data protection, online safety, and cybersecurity. Whereas there are states that have developed comprehensive and future-oriented framework, other states are still struggling with issues of political uncertainty, institutional capabilities and growing technological needs. In this segment, a comparative evaluation of these frameworks is carried out in detail with strengths and weaknesses being brought out.

Digital Trade Regulations

In the United Arab Emirates, the digital trade has been embraced by the thorough e-commerce laws and regulations on data protection that composed a well-structured environment of digital business and transactions via the internet (Malkawi, 2023). These regulations make transactions safe and reliable and help strengthen consumer confidence and make the UAE the digital hub in the region.

Egypt on the other hand has designed a regulatory structure that is focused on the concept of digital transformation and modernisation of the services provided to people. The policies made within this framework are aimed at the e-government programs, ensuring cybersecurity, and the development of digital literacy, which in turn allows the country to become a much closer part of the global digital economy (Aboul-Dahab, 2025).

In Saudi Arabia, new law reforms have prioritized the upholding of international digital standards, especially to this end of safeguarding children online. Such attention can be explained by the increasing awareness of providing security to vulnerable groups and a safe digital environment to conduct business and communicate (Abobaker, 2024).

Data Protection and Cybersecurity

The UAE has created a robust legal framework to provide security to digital applications and focus on the criminal liability and judicial supervision as the main ways to provide compliance and digital safety of applications ("Criminal Protection of Digital Applicati…", 2024). These are some of the actions intended to prevent cybercrimes, ensure the privacy of the users, and integrity of the platforms.

In Egypt, The National Telecommunications Regulatory Authority (NTRA) has a dominant role regarding the digital compliance and the enforcements that protect the data. The NTRA supports the quality of the digital services they provide to the citizenry by coordinating the national cybersecurity plans which will ensure the data of the citizens remains safe in the process (Aboul-Dahab, 2025).

Lebanon, in its turn, offers a less detailed regulation environment. The persisting political unrest and divided institutional capabilities have undermined the tools and strategies to establish some strong laws on digital media as there is a gap in the protection of data, internet safety, and cyberspace control.

Challenges and Opportunities

In the entire Arab region, twofold dilemma arises, the first is how to gain successful integration into the global digital economy and, the second is how to deal with internal differences regarding the legal and regulatory systems. The leaders of digital governance include such countries as Saudi Arabia and the UAE that use the proactive approach in their policies and meet the international standards. Conversely, countries experiencing a less significant institutional capacity experience challenges with law enforcement or following the technological development (Valiakhmetova & Tsukanov, 2022).

In addition, the fast pace of digital technology development, such as social media, artificial intelligence tools and e-commerce applications, provides us with a constant challenge to the sufficiency of current legal systems. Policymakers in the region would thus need to seek continuous legislation updates that would make the law efficient, up to date and able to handle emerging threats to privacy, cybersecurity, and trust of people. Such a dynamic situation explains why comparative legal studies are relevant as the experiences of the more developed framework can be used to carry out reforms in the countries which aim to enhance their digital forms of governance.

Table3. Comparative Analysis of Digital Media Legislation in Selected Arab Countries

Aspect / Country	**United Arab Emirates (UAE)**	**Egypt**	**Saudi Arabia**	**Lebanon**
Digital Trade Regulations	General services e-commerce requirements and regulation of data safeguards, enables thriving	Digitalisation, e-government and cybersecurity planning (Aboul-Dahab, 2025).	New changes were made according to the international standards	Weak regulatory efforts; the development of digital trade laws is weaker because of the

	customer digital transaction (Malkawi, 2023).		(Abobaker, 2024); the focus on online child safety was brought upon.	political turmoil.
Data Protection	High accent level of criminal protection and court supervision; safe digital applications ("Criminal Protection of Digital Applicati…", 2024).	They are Enforced by National Telecommunications Regulatory Authority (NTRA) and safeguard citizens data and digital services (Aboul-Dahab, 2025).	Cybersecurity and digital safety reforms: part of this involved data protection; partial convergence with international best practice.	Poor, disjointed data protection system; there are gaps in regulatory responses.
Cybersecurity Measures	All-encompassing cyber security legislation; vigilance to cybercrime.	NTRA has gone to work at the national cybersecurity level; decent coverage.	Greater attention to their laws concerning safety and adhering to global standards in digital safety.	Poor levels of enforcement and split institutional capacity; great exposure to cyber risks.
Legislative Strengths	Modern, clear, comprehensive; enables innovation and trust in the digital markets.	Facilitates digitalization of transformation and quality of the public service; systematic regulatory agency.	Conforms to international standards; highlights internet security of needy groups.	There are limited regulations; there are no mechanisms of enforcement.
Legislative Weaknesses	Technology is changing very fast and thus requires constant upgrading.	There are enforcement and alignment gaps with emerging digital threats.	Incomplete coverage of the emerging cyber risks; enforcement issues are outstanding.	Legal effectiveness is hampered by political unpredictability and softness of the institutions.
Overall Digital Governance	A good role model in the area; forward	Average; enhancing the digital governance through organized	Mature; regulative emphasis and	A very poor performer; needs serious

	looking and holistic.	control.	regulation changes continue.	legislative and institutional changes.

Regional Patterns and Influences in Digital Media Regulation in the Arab World

Digital media regulations in the Arab world have severe regional trends caused by the interaction of multiple political ideas, economic drive, future technological progress, and cultural conservation. The patterns are not just coincidental happenings but are very much ingrained in the historical and socio-political matters of the individual countries. The regional factors are important in the view of understanding differences in approaches to govern digital media among the Arab states.

In most Arab nations, the curbing of digital media has become a highly used means of political control and silencing of opponents. States commonly introduce harsh laws and regulations to track net-activity, block information and silence the dissents. Such a strategy is noticeable in states, such as Egypt, where the government has resorted to digital repression strategies in order to take control of the discourse and restrict it (European Council on Foreign Relations [ECFR], 2022). Likewise, in Saudi Arabia, the government has been deploying surveillance and censorship through digital means in order to maintain its leadership and stave off critics (Piovesan, 2023).

This pattern indicates the general regional tendency toward the modern form of authoritarianism based on digital technologies and legal regulation of digital environments, so-called digital authoritarianism. It is observed that countries such as China and Russia and their models have been adopted and Arab regimes want to implement the features of the so-called Great Firewall and other surveillance systems to demonstrate digital sovereignty and manage the informational flows (Arab Center Washington DC, 2022).

Other factors that lend weight to the regulative form of digital media in Arab world are economic factors. Oil and gas-rich countries, like the UAE and Saudi Arabia, have engaged in massive investments in the digital infrastructure as a general effort in diversity of economies. Such investments are meant to ensure these countries become the pioneers of digital economy, attract foreign investment, and develop innovativeness.

As an example, the UAE has exerted its efforts to have robust e-commerce legislations and data protection rules, which creates an excellent digital trade environment (Malkawi, 2023). The said regulations aim at establishing a safe and appealing landscape to attract the operations of digital businesses, which considers the push of economic expansion versus the necessity to retain control over digital environments.

Mshaqaba (2023) demonstrates that the technological and professional issues of digital transformation of local media in Jordan including municipal television are significant. As institutions seek to absorb digital tools into content production, there is a shortage of highly skilled personnel in the sector to support enterprises in this regard and the support enabled by institutions is not sufficient, which reflects the scope of the regional fight towards digital governance.

Digital media control in the Arab world is dictated highly by cultural and religious values. Numerous states have laws that bring the media content into the framework of Islamic traditions and norms of the society. This is especially true in the UAE whereby a new media law (which goes into effect, May 29, 2025) will cause sweeping changes to the way influencers and digital

content creators conduct business. Strict ban on hate speech, misinformation, and privacy violation is explicitly stipulated in the law and resonates with the values of a country and stimulates ethical journalism hereby aligning media content (Times of India, 2025).

Likewise, in Egypt, the regulatory framework has policies that target the digital transformation described as the promotion of e-government and cybersecurity protection measures, as well as the fact that digital content should correspond to national cultural and ethical norms (Aboul-Dahab, 2025).

Digital media regulations have also undergone infamous imprints of regional conflicts and social movements. The Arab spring started in 2011 showed the effectiveness of the digital platform to influence the mass opinion and driving protest movements. As a reaction, governments across the region have increased their hold on digital media in order to avoid the occurrence of such outbursts. This has seen more censorship, surveillance and the enactment of laws undermining the freedom on the internet.

As another example, in Lebanon, activists have played a leading role in putting forward digital rights and fighting against censorship in the internet. Such efforts as the protection of digital rights and the fight against cyber repression by the government are carried out by such organizations as SMEX and indicate the constant struggle of digital freedoms against governmental attempts to establish control (Time, 2019).

Arab world is not an isolated entity in terms of approach taken towards digital media regulation, it is under the influence of the global standards and procedures. International governments including the United Nations and the European Union do have a part to play in the promotion of digital rights and the furthering of changes in the area. By giving technical support, pushing policy reforms and tracking the abuse of digital rights, these bodies affect the regulatory environments of Arab states (Number Analytics, 2021).

Finding and discussion

The comparison of legislative systems of the digital media in Jordan and the chosen Arab states has made some interesting findings. Such results highlight the complexity both of reconciling freedom of expression and privacy with public order, and of tackling the dilemmas raised by the sudden surge in digital platforms.

The results show that the legal framework of Jordan, especially the Cybercrime Law No. 17 of 2023, can be discussed as one of the most updated and straightforward attempts to combat the problem of character assassination, defamation, and online harassment in the region. In contrast with Lebanon, where things are not much better with limited and obsolete digital laws, Jordan has been active in the effort to modernize its laws in the digital sphere. Nevertheless, these reforms maintain the control of the state over digital freedoms and security over general trends in the Arab world.

Discussing the weaknesses of digital journalists, Mshaqaba (2022) mentions the inappropriate role of online news sources in the media literacy of Jordanian audiences. This restriction is part of the larger worry regarding whether the existing rules and regulations can keep up with the exponentially growing digital media and the extent to which citizens can be given knowledge to reflectively respond to the available information through such media.

The results of this research can be connected with previous review of the media practice in Jordan where containment has been found out as a major characteristic of the journalistic

landscape. As noted by Alsafouri (2020), the containment strategies are used in both the governmental and non-state spheres limiting investigative journalism and healthy discussion. This speaks to the claim that, although the current reforms on cybercrime in Jordan are undertaken in an effort to control malpractices through digital means, there are risks of buttressing the established trends of limited freedom of the press.

Comparatively, other countries like UAE and Saudi Arabia exhibit higher institutional ability to enforce the digital regulations mostly in data protection and cybersecurity. Egypt, however, sits more on the Jordanian side of limiting the laws; the reason is usually based on the necessity to protect national security and avert misinformation. These differences and similarities show that there is no coherent Arab policy: the general tendency is toward restrictive regulatory models.

One of the key findings is that Arab legislative structures are usually incapable to meet the fine balance between providing the digital rights of citizens and safeguarding the social order. In Jordan, although the media and publications law and the cybercrime law can be stated as defense mechanisms, due to vague provisions of these two laws, it has mostly been used to diminish free expression. Such tendencies are also evident in Egypt and Saudi Arabia as the ambiguity of law gives law enforcement authorities wide discretionary powers. This is in opposition to European ones such as GDPR, which are user-focused and data protection centered. Therefore, the findings tend to indicate that the Arab approach is still more of a state-oriented and not a rights-oriented approach.

The local interpretation shows the impact of socio-political realities on the regulation of digital media. Digital platform technologies tend to be perceived as a paradigm of modernization, as well as a danger to the stability of the regime in authoritarian political systems. This can be attributed to the fact that both in Arab governments there is the dual perception as governments spend their money in digital infrastructure building, and at the same time imposing very stringent restrictions on online liberties. Moreover, the cultural and religious values are also very important there and various laws directly target morality, decency, and cultural norms in relation to the regulation of digital areas. The legacy of the Arab Spring is still present, governments have increased control instruments on digital spaces in order to avoid another mobilization on such a large scale.

The results also draw implication on utterances about digital rights in the Arab world. To begin with, the freedom to express oneself on internet remains under threat because of the stifling interpretations of the cyber laws. Second, although some nations such as the UAE have been able to establish strong data protection regulations, there is no harmonized regional protection that ensures a balance in protection in the Arab world. Third, means of enforcement are inconsistent there, in the sense that in some countries like the UAE and Saudi Arabia, the institutional capacities to enforce are stronger whereas in other countries like Lebanon, they are with low political stability and government systems.

Conclusion

The paper has analyzed the legal frameworks of digital media in Jordan and some of the Arab nations and brought out their national peculiarities combined with regional trends. According to the findings, although major efforts have been taken to modernize and update legal frameworks, the current trend in the region is security-oriented over the rights-based one.

The Cybercrime Law No. 17 of 2023 in Jordan has developed as an interesting case because of its direct criminalization of character assassination. Nevertheless, the legislation indicates the wider regionalistic issue of placing the importance of state security and social stability ahead of safeguarding the freedom of expression and digital rights. When compared to Egypt, Saudi Arabia, and the UAE, Jordan and Egypt experience similar tendencies of restrictiveness, Saudi Arabia is on its way to adopting the frameworks better aligned with international child protection and requirements of the newly created cybersecurity department, the UAE has presented a well-developed framework especially on the issues of data protection and digital trading, and Lebanon is plagued by political instability as the sector is fragmented.

Increasing media credibility and independence is only possible by decreasing containment and establishing truth and transparency in media broadcasting that includes both the traditional and digital channels as Alsafouri (2020) argues. On the basis of this, it is suggested that Jordan and other Arab nations should not only restructure digital laws but also create a situation whereby journalists and other media practitioners are able to operate in a free manner without being unduly harassed by legal and political frameworks.

To promote the regulation of digital media in Jordan further, as Mshaqaba (2023) claims, regulatory change should not only be legislative since the government needs to make investments in the training of journalists and the implementation of new technologies at the institutional level. Absent similar parallel work, digital laws may resemble a formalistic and unrelated to practise zone.

Another argument derived through the regional analysis comes out in the fact that in the Arab world, political authoritarianism, cultural and religious values, and economic priorities heavily influence the regulation of the digital media. Although the path to digitalization has been funded, several of the legal provisions are both broad and general leaving governments with lots of discretional powers. Unlike international equivalents like the rights-based EU GDPR and the free-speech-focused regulation of the U.S., Arab states have not attained a balance and transparency of regulations, which both defend state interest integrity and citizens' rights adequately.

Recommendations

In light of these findings, the following recommendations are proposed:

1. The Arab states especially the Jordan and Egypt states should also amend existing cybercrime and media laws to suit the international standard of human rights in the respect of freedom of expression and the right to privacy. Offenses must be well articulated and have clear definitions in order to curb misuse of the legal provisions.
2. Similar to what is done by EU in GDPR and the UAE in its recent reforms, the Arab countries ought to enact broad data protection laws, enforcing user privacy laws, controlling personal data processing, and creating independent supervisory authorities.
3. Judges are needed to be more involved in the architecture of proportionality and equity in the application of the law in digital media. The online freedoms can be embraced by independent oversight of the judicial process in fighting arbitrary restrictions of the online freedoms.
4. With the interdependence instilled in the digital platforms, Arab states need to aim at more viable regional cooperation in digital governance. A good step would be to have a

consistency in regulations in cybersecurity, data protection and digital trade which would increase level of security and confidence of users.

5. Consultations and negotiations with the civil society organizations, digital rights activists, and media professionals should be conducted in the process of policymaking. Such a participatory attitude can be used to create legislation that might be composed to the needs of the society as opposed to being used as a tool of state interests.
6. In addition to legislative changes, governments ought to spend on digital literacy programs to ensure citizens have the awareness to enjoy online spaces. Educational campaigns will address not only the issue of spreading misinformation but also address the issue of cyber risks without involving restrictive legislations.

References

[1] Freedom House. (2024). *Jordan: Freedom on the Net 2024*. Retrieved from https://freedomhouse.org/country/jordan/freedom-net/2024
[2] Reporters Without Borders (RSF). (2023). *Proposed cybercrime law would deal new blow to press freedom in Jordan*. Retrieved from https://rsf.org/en/proposed-cybercrime-law-would-deal-new-blow-press-freedom-jordan
[3] *European Courts as Digital Media Regulators* (pp. 17–35). (2022). Edward Elgar Publishing eBooks. https://doi.org/10.4337/9781802203004.00006
[4] Reed, C. S. (2022). *Digital Media Law*. https://doi.org/10.4324/9781003197966
[5] Packard, A. (2010). *Digital Media Law*. https://www.amazon.com/Digital-Media-Law-Ashley-Packard/dp/1118290720
[6] Williams, A., Calow, D., & Higham, N. (1998). *Digital Media: Contracts, Rights and Licensing*. http://ci.nii.ac.jp/ncid/BA44850094
[7] Sieckmann, J.-R. (2019). *Legislation as Balancing* (pp. 133–152). Springer, Cham. https://doi.org/10.1007/978-3-030-12068-9_6
[8] Gomathy, C., Geetha, V., Vijaysimha, V., & Sreya, P. V. N. S. (2024). Balancing Freedom of Speech and Online Content Regulation. *Indian Scientific Journal Of Research In Engineering And Management*. https://doi.org/10.55041/ijsrem37504
[9] Şahin, Z. (2022). Evaluation of the law no. 7253 on amendment of the law on the regulation of broadcasts made on internet and combating crimes committed through these broadcasts in the context of freedom of expression and personal rights. *Euroasia Journal of Social Sciences & Humanities*, *9*(2), 28–44. https://doi.org/10.38064/eurssh.332
[10] Thuku, J., & Mbaaro, M. (n.d.). *Hate Speech Legislation and Freedom of Expression: Finding the Balance*. https://doi.org/10.61838/kman.isslp.1.2.5
[11] Lima, A. C., Montevilla, J. L., & dos Santos, L. A. C. (2024). *Regulação legal das redes sociais: proteção de dados e liberdade de expressão*. 37–38. https://doi.org/10.69849/revistaft/pa10202410212137
[12] Monti, G. (2022). Taming Digital Monopolies: A Comparative Account of the Evolution of Antitrust and Regulation in the European Union and the United States. *The Antitrust Bulletin*, *67*, 40–68. https://doi.org/10.1177/0003603X211066978
[13] Fukuyama, F., & Grotto, A. (2020). *Comparative Media Regulation in the United States and Europe* (pp. 199–219). Cambridge University Press. https://doi.org/10.1017/9781108890960.010

[14] Bradford, A. (2023). *Digital Empires*. Oxford University Press. https://doi.org/10.1093/oso/9780197649268.001.0001
[15] May, B. E., Chen, J. V., & Wen, K. (2004). The differences of regulatory models and internet regulation in the European Union and the United States. *Information & Communications Technology Law, 13*(3), 259–272. https://doi.org/10.1080/1360083042000289077
[16] García Sanz, R. M. (2024). Los «social media» en USA y en la UE: dos modelos legales distintos y un mismo problema para la Democracia. *Teoría y Realidad Constitucional*, *54*, 309–349. https://doi.org/10.5944/trc.54.2024.43316
[17] Al-Zoubi, M. (2023). Crimes of Electronic Defamation, Libel, and Slander under Jordanian Cybercrimes Law. *International Review of Law*, *12*(1), 267–284. https://doi.org/10.29117/irl.2023.0260
[18] Faqir, R. S. A. (2013). Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010. *International Journal of Cyber Criminology*, *7*(1), 81. https://www.cybercrimejournal.com/Faqir2013janijcc.pdf
[19] Alqudah, M., Al--Amawi, A., Khashashneh, T., & Balas, H. (2024). The Crime of Character Assassination in the Jordanian Cybercrime Law. *International Journal of Religion*, *5*(10), 3671–3684. https://doi.org/10.61707/gsfk2s22
[20] Al-Amawi, A. A. (2023). The Crime of Character Assassination in The Jordanian Cybercrime Law. *International Journal of Membrane Science and Technology*. https://doi.org/10.15379/ijmst.v10i2.2886
[21] Al-Amawi, A., & Balas, H. A. M. (2024). Digital character assassination in the Jordanian law. *Multidisciplinary Reviews*, *7*(11), 2024273. https://doi.org/10.31893/multirev.2024273
[22] Malkawi, B. (2023). *Legal approaches to the regulation of digital trade by Middle Eastern countries* (pp. 233–251). Edward Elgar Publishing. https://doi.org/10.4337/9781800884953.00024
[23] Aboul-Dahab, K. (2025). *Assessing Egypt's progress toward its digital transformation and collaborative regulation*. https://doi.org/10.2139/ssrn.5027167
[24] Abobaker, M. Y. (2024). Analysis of Saudi Arabia's Legislative Reforms to Strengthen Compliance with The Convention on the Rights of the Child and SDGS: Enhancing Online Protection for Future Generations. *Journal of Lifestyle and SDGs Review*, *4*(3), e02374. https://doi.org/10.47172/2965-730x.sdgsreview.v4.n03.pe02374
[25] Criminal Protection of Digital Applications in the UAE Legislation: A Comparative Study. (2024). *Pakistan Journal of Criminology*. https://doi.org/10.62271/pjc.16.1.489.504
[26] Valiakhmetova, G. N., & Tsukanov, L. (2022). Digital Challenge for the Arab World: Integration or Differentiation Factor? *Вестник Российского Университета Дружбы Народов*, *22*(2), 303–319. https://doi.org/10.22363/2313-0660-2022-22-2-303-319
[27] Arab Center Washington DC. (2022). *Mapping digital authoritarianism in the Arab world*. Retrieved from https://arabcenterdc.org/resource/mapping-digital-authoritarianism-in-the-arab-world/

[28] ECFR. (2022). *Iron net: Digital repression in the Middle East and North Africa*. European Council on Foreign Relations. Retrieved from https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/

[29] Number Analytics. (2021). *Digital rights in the Middle East: International influences and regional challenges*. Retrieved from https://www.numberanalytics.com/blog/digital-rights-middle-east-international-relations

[30] Piovesan, G. (2023). *Digital authoritarianism in the Middle East*. The Security Distillery. Retrieved from https://thesecuritydistillery.org/all-articles/digital-authoritarianism-in-the-middle-east

[31] Times of India. (2025). *UAE new media law explained: Here's what you need to know about key rules and penalties up to Dh1 million*. Retrieved from https://timesofindia.indiatimes.com/world/middle-east/uae-new-media-law-explained-heres-what-you-need-to-know-about-key-rules-and-penalties-upto-dh1-million/articleshow/121616419.cms

[32] Time. (2019). *Heirs of the Arab Spring*. Retrieved from https://time.com/5927349/heirs-of-the-arab-spring/

[33] Alsafouri, A. (2020). The impact of containment on the professional performance of journalists: A descriptive study from the perspective of Jordanian journalists. Al-Risalah Journal of Media Studies, 4(1), 11–34.

[34] Alsafouri, A. (2020). Mechanisms of preparation and television presentation of political programs and their impact on audiences: An analytical study. Al-Risalah Journal of Media Studies, 4(1), 35–60.

[35] Mshaqaba, Y. A. A. (2021). The legal regulation of digital media in Jordan and its impact on journalistic work. *The Egyptian Journal of Media Research, 77*(Part 3, Vol. 4), 2269–2293.

[36] Mshaqaba, Y. A. A. (2022). Media literacy and its application to the content of Jordanian news websites in light of the growth of digital media. *The Egyptian Journal of Media Research, 80*, 2089–2108.

[37] Mshaqaba, Y. A. A. (2023). Content production in digital media and the professional pressures affecting it: The case of digital television in Al-Mafraq Municipality, Jordan. *The Egyptian Journal of Media Research, 84*, 2063–2081.