

JORDAN

ILA Country Report

JORDAN

Legal Framework

Constitutional Protection

The Jordanian Constitution was adopted in 1952 and lastly reviewed in 2011. The rights to freedom of expression and privacy are guaranteed as follows:

- Article 7 (2) of the Constitution provides that every infringement on rights, public freedoms and the 'inviolability of the private life of Jordanians' is a crime punishable by law.

- Article 10 stipulates additional protection to the right to privacy by providing that dwelling houses are inviolable and may not be entered except in the circumstances and manner prescribed by law.

- Under Article 18, all postal and telegraphic correspondence, telephonic communications, and the other communications means must be regarded as secret and must not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law.

- Article 15 guarantees the right to freedom of expression subject to certain limits, which must be laid down by law. In particular, Article 15 (1) provides the State shall guarantee freedom of opinion and that every Jordanian shall freely express his opinion by speech, writing, photography and the other means of expression, provided that he does not go beyond the limits of the law. Article 15 (2) further guarantees freedom of scientific research and literary, technical, cultural and sports excellence

provided that it does not violate the provisions of the law or public order and morality. Article 15 (3) guarantees freedom of the press, printing, publication and information media subject to regulation laid down by law. In particular, Article 15 (6) provides that ownership and resources of newspapers shall be regulated by the law. The Constitution further provides some level of protection to newspapers and other media by providing, under Article 15 (4), that they may not be suspended or their license revoked except by a judicial order in accordance with the provisions of the law. At the same time, Article 15 (5) provides for limited censorship on newspapers, publications, books and information and communication media in matters related to public safety and national defence purposes in the event of the declaration of martial law or an emergency.

Regulation of online content

THE PENAL CODE 1960 (AS AMENDED IN 2011)

The Jordanian Penal Code contains several speech offences that equally apply to online expression, including:

- Article 118 punishes "anyone who engages in acts, writings, or speeches not approved by the government that would subject Jordan to the danger of violent acts or disturb its relations with a foreign state" with a minimum of five years' imprisonment.

- Article 122 punishes with up to two years imprisonment anyone who insults a foreign state or head of state.

- Article 195 further punishes with one to three years' imprisonment anyone who attributes untrue actions or statements to the King. The Article criminalizes anyone "who proves audacity to insult his Majesty the King" or sends a text, audio or electronic message, or image or caricature of his Majesty the King "in a way that undermines the dignity of his Majesty." The same applies to any messages that insult the Queen, the Crown Prince, guardians of the Throne, or a member of a substitution committee.¹

- According to HRW reports, the Jordanian Penal Code also criminalises defamation of ordinary individuals, government officials and institutions. Libeling, slandering, or insulting regular citizens can result in up to three months, six months, or one month in prison consecutively. However, one can be charged with up to two years in prison for slandering public parties identified as the Parliament or one of its members, official institutions, courts, public administrations, the army, or their members on duty (Article 191). Insulting a public official can result in up to one year in prison and up to two years if the official is a judge (Articles 193 and 196). Insulting the national flag, symbols, or the flag of the League of Arab Nations can result in up to three years in prison (Article 197).

THE INFORMATION SYSTEM CRIMES LAW 2010

In August 2010, the Jordanian parliament passed the [Law of Information System Crimes 2010 \('ISC 2010'\)](#). The Law was adopted as an interim measure following a fast-track procedure, i.e. without parliamentary debates.

The ostensible purpose of the ISC 2010 was to quickly fill out the gaps left by the Electronic Transactions Act 2001, which only dealt with commercial transactions but did not address criminal activities carried out online. The ISC law was amended in June 2015.²

The ISC 2010 thus lays down a number of new 'cybercrimes', from online identity theft and the unauthorised use of credit card and banking information, to 'unauthorised access to information systems' and acts of sexual exploitation online. While many of the new provisions seek to fulfill Jordan's obligations under international law, such as the prohibition of incitement to terrorism and child pornography, the provisions of the Act are often overly broad, confusing and unduly restrictive of freedom of expression online. For instance:

- Article 3 criminalises "anyone who intentionally accesses a website or information system in any manner without authorization or in violation or excess of authorization". Among other things, Article 3 also contemplates the criminalisation of anyone who copies information from a website.

- Article 4 criminalises "anyone who enters, publishes, intentionally uses a program through the web or any information system to delete, add, damage, release, block, move, copy, or capture, or enable others to view data or hinder or impersonate the owner of the article without an authorization".

¹ Almasri, Reem (2015) "Mapping Digital Controls on Content in Jordan" 7iber Dot Com. Available at http://www.7iber.com/wireless_research/how-digital-content-is-controlled-in-jordan/

² <https://www.assawsana.com/portal/pages.php?news-id=218071> (in Arabic)

- Article 910 criminalises the promotion of prostitution online.

- Article 10 criminalises anyone who sets up a website to 'facilitate' terrorist activities or to support terrorist groups or to promote terrorist 'ideologies' rather than criminalising 'incitement' to 'acts' of terrorism.

- Article 11 criminalizes by no less than three months imprisonment "anyone who intentionally sends, resends or publishes data or information through the web or electronic websites or any information system any content of defamation, libel or slander" even if they were not directly involved in a crime.

- Article 12 punishes by no less than four months' imprisonment "anyone who intentionally and without authorization or in violation or excess of an authorization accesses a website or information system in any manner with the purpose of viewing data or information that is not available to the public and which touches upon national security, foreign relations of the Kingdom, general security or national economy."

- Article 13 allows judicial police to "confiscate devices, tools, applications, operating systems, the web, and all methods used to commit any listed crimes and keep all information relevant to committing any crimes"

At the same time, several especially contentious provisions were eventually removed from the Law when it was still in its drafting stages, including:

- A provision criminalising the "sending or posting of data or information via the Internet or any information system that involves defamation or contempt or slander";

- A provision criminalising the "spreading of ideas affecting national security or foreign relations of the Kingdom, as well as public safety or the national economy"; and

•Warrantless searches of media outlets.

THE TELECOMMUNICATIONS LAW 1995 (AS AMENDED)

Under Article 58 of the [Telecommunication Law](#), Internet Service Providers (ISPs) may block or suspend access to telecommunications services if beneficiaries of such services use it in a way that violates valid legislation or public morals. (Article 58)

Moreover, Article 75 (a) criminalises anyone who uses telecommunications services to deliver "threatening or abusive messages" or "messages contrary to public morals" or "spread false information" with the intent of spreading panic. The offence is punishable by imprisonment between 1 month and 1 one year and/or a fine of between JD 300 and 2000. Furthermore, Article 75 (b) criminalises any person who provides or contributes to the provision of telecommunications services in violation of public order or public morals.

THE ANTI-TERRORISM LAW 2006

"Passed in 2006 and amended in 2014, [the Anti-Terrorism Law](#)³ first extends the definition

³ Mapping controls on digital information in Jordan: <http://www.7iber.com/2014/04/anti-terrorism-draft-law-a-choice-between-security-or-speech/>

of terrorism to

“Any deliberate act or abstention of an act, or threat of an act, regardless of its causes, uses, or means committed to carry out a criminal act collectively or individually that could jeopardize the safety and security of society; or cause disorder by disturbing public order or causing terror among the people, or intimidating them, or jeopardizing their lives; or cause harm to the environment, or facilities, or public or private property, or facilities of international or diplomatic missions, or occupy any of them; or jeopardize national resources, or pose economic risk; or to force the legitimate authority or an international or regional organization to do any work or abstain from it, or disable the application of the constitution, laws, or regulations”

Speech online and offline can be easily considered an act by the Anti-Terrorism Law. This Law criminalises any expression of support for what can be considered terror on the Internet. This is reflected in Article 3:

“use of information systems, or the information network, or any other publishing or media tool, or establishment of a website to facilitate the conduct of terrorist acts or support terrorist groups, or an organization or a charity that performs acts of terrorism or market its ideas or funds it, or conducts any acts that subject Jordanians or their property to acts of hostility or reprisals.

The danger in this clause is two-fold. First, the lack of definition to what constitutes

“support” can extend support to the basic use of symbols and signs, and the sharing content that is considered to be supportive of terror. Second, the wide definition of what constitutes a terror act may subject a larger percentage of the society under this Law. The definition includes “any act that damages the environment, or disrupts public life.” Not only protests will be criminalised under this Law, but also, the sharing of a Facebook event that calls for a demonstration could then be considered support of a “terror” group. Finally, crimes committed under this Law fall within the jurisdiction of the State Security Court; a military court with a martial public persecutor. The state security violates one of the most important criterions of a fair trial, which is a “public trial”.⁴

Regulation of Media Works

In Jordan, the press is primarily regulated by the Press and Publication Law 1998. In its essence, the Law considers working in journalism without being a member in the Press Association a crime. The Law was amended in 2012 to make clear that the same restrictive requirements that apply to the print media also apply to “electronic publications”. Article 49 of the amended Law requires any “electronic publication that engages in publication of news, investigations, articles, or comments, which have to do with the internal or external affairs of the kingdom” to obtain registration and licensing from the Media Institute (Press and Publication Department formerly). The amended Law also gives the Department’s director the authority

⁴ Mapping Digital Content Research: <http://www.7iber.com/research/mapping-controls-on-digital-information-in-jordan/>

to order the block of unlicensed websites and electronic publications that violate the country's laws without a court order. This resulted in the blocking of over 300 websites in June 2013. The Law further makes clear that editors are liable for user generated content on their website. In particular, Article 49 of the Law prohibits the owner and editor-in-chief of an electronic publication from publishing comments deemed "irrelevant" or "unrelated" to the published article. A full translation of both the PPL 1998 as amended and the Press Association Law 1998 would be useful to: (1) check if other aspects of the PPL 1998 should be mentioned; (2) if there is anything of relevance in the PAL 1998.⁵

Regulation of Internet Intermediaries

There is currently no specific law protecting Internet intermediaries from liability for third-party content. Accordingly, Internet intermediaries are subject to the general tort law principles contained in the [Jordanian Civil Code 1976](#) and in the case of news sites to the Press and Publication Law 1998 as outlined above.

Under Article 256 of the Jordanian Civil Code, "a person is legally responsible for the damage caused as a result of his or her acts or omissions even if he is a non-discerning person." Furthermore, Article 288 of the Civil Code deals with various liabilities. In particular, Article 288 (b) provides that "any person who had actual power to supervise

and direct the person who inflicted the damage may be held liable even though he himself had no choice if the injurious act was committed by the supervised person while or because of performing the duties of his position." It does not appear that Article 288 has been used in the context of Internet intermediary liability. It is likely that a finding of liability would turn on the interpretation by the courts of what amounts to 'actual power to supervise and direct a person' and whether such a relationship exists between Internet intermediaries and their customers.

Surveillance and Data Protection

The right to privacy is chiefly protected by the Constitution. According to Article 18, electronic communications may not be intercepted or otherwise collected or viewed except by a judicial order in accordance with the provisions of the law. Nonetheless, according to Article 29 of the Telecommunication Law, one of the license conditions requires ISPs to provide the needed facilities to implement judicial and administrative requests related to the monitoring of communication. However, we are not aware of any law specifically regulating the powers of law enforcement and intelligence agencies in relation to digital communications.

Whilst there is currently no overarching data protection law in Jordan, a number of provisions scattered across different statutes afford some protection to personal data and the confidentiality of private communications. In particular, Article 71 of the Telecommunications Law provides anyone who spreads or discloses the content of any communication through a Public or Private

⁵ See Ibid.

Telecommunications Network or a telephone message which came to his knowledge by virtue of his post, or records the same without any legal basis, shall be punished by imprisonment for a period not less than one month and not exceeding one year, or by a fine not less than (JD100) and not more than (JD300), or by both penalties.

Furthermore, Article 76 prohibits any person from intercepting, obstructing or altering the contents of a message carried through the telecommunications networks or encouraging others to do so. The offence is punishable by imprisonment for a period not less than one month and not exceeding six months, or by a fine not more than (JD200), or by both penalties.

Net Neutrality and Access to the Internet

We are not aware of any specific provisions guaranteeing access to the Internet or protecting the net neutrality principles.

Country Analysis: Our assessment

The Constitution seemingly attempts to comprehensively protect the right to freedom of expression under Article 15. It guarantees freedom of opinion, freedom of expression, freedom of scientific research and 'literary, technical and sports excellence'. Freedom of the press is also guaranteed. At the same time, Article 15 fails to meet international standards on freedom of expression in several respects. First, it does not encompass the

broader right to seek, receive and impact information and ideas of all kinds regardless of frontiers and through any media, which is guaranteed under Article 19 of the International Convention on Civil and Political Rights (ICCPR). Secondly, limitations on the right to freedom of expression are inconsistent with Article 19 (3) of the ICCPR, which enshrines that any limitation on the right to freedom of expression must not only be provided by law but must also pursue one of the legitimate aims exhaustively enumerated under that Article and be necessary and proportionate in a democratic society. By contrast, the Jordanian Constitution only refers to restrictions 'provided by law' without specifying that any such restriction must pursue one of the legitimate aims under international law and be necessary and proportionate to that aim. Thirdly, Article 15 (3) – (6) of the Constitution entrenches regulation of the press by the state contrary to international standards as well as the possibility of suspending the exercise of the right to freedom of expression in times of an emergency.

The right to privacy benefits from stronger protection. At the same time, it is not extended to the protection of family life. Importantly, like the right to freedom of expression, the Constitution fails to provide that any restriction on the right to privacy must comply with the three-part test, i.e. that restrictions must not only be provided by law but also pursue a legitimate aim and be necessary and proportionate in a democratic society.

Online speech is regulated both by the general Criminal Law and the specific offences created under the Press and Publication

Law, Information System Crimes Law and the Telecommunications Law. The biggest obstacle to digital content is nonetheless the **Press and Publication Law 1998** that requires a license from a government authority for any “news” publishing entity about Jordan. A recent amendment has now clarified that these requirements equally apply to online news sites. The overarching definition of an “online publication” could further be interpreted to reach social media sites and blogs which in turn places a pre-publishing censorship that imposes arduous conditions in order for websites to get licensed and be allowed to publish.⁶ Anyone who intends to start a website that “provides analysis” on Jordan is also subject to additional restrictions. Licensing and registration are illegitimate under international law. The violation is even more egregious when such licensing and registration must be sought from government bodies. The special rapporteurs on freedom of expression confirmed this position in their 2005 Joint Declaration where they stated that “no one should be required to register with or obtain permission from any public body to operate an ISP, website, blog or other online information dissemination system, including Internet broadcasting.” Similarly, the UN Human Rights Committee has confirmed in its General Comment no. 34 that general state systems of registration or licensing of journalists, “whether on the Internet or elsewhere”, were incompatible with the ICCPR. Accordingly, the website sanctioning powers of the Press and Publications Department are equally illegitimate.

The **Jordanian Penal Code** contains a number of speech offences that are in breach of international standards on freedom of expression. For instance, defamation and libel against the King and public authorities are criminalised. It is well-established; however, that public figures must tolerate a greater level of criticism because of the public nature of their function or activities and those criminal sanctions have a chilling effect on freedom of expression. Other offences, such as Article 118 of the Penal Code, are drafted in overly broad terms and highly likely to hinder the ability of journalists to report on matters of public interest, including foreign relations or national security.

Similarly, the **Information System Crimes Law 2010** contains a number of offences, which are drafted in a way that is both confusing and hopelessly vague. Article 3, for instance, effectively criminalises anyone who accesses or copies information online without authorization. Yet, it remains unclear what constitutes ‘authorisation’ in the context of websites and information systems, which are publicly available. Article 11 is equally unclear, criminalising ‘unauthorized’ access to websites which contain information on matters of national security or foreign relations “not available to the public”. Again, not only is it unclear what constitutes ‘authorization’ in this context, but the lack of any clarification as to which information may be “publicly available” means that it will be impossible for ordinary users to foresee in what circumstances they might be criminalised for accessing information online concerning matters of national security or foreign affairs in general (especially leaked information). Moreover, and in any

⁶ See Enhancing Internet Media Freedom in Jordan: <http://www.7iber.com/wp-content/uploads/2015/04/Enhancing-Internet-Media-Freedom-in-Jordan-Research-Project-FINAL.pdf>

event, Article 11 fails to provide for a public interest defence. It therefore imposes undue restrictions on the right to freedom of expression and freedom of the press to report and investigate on matter of public interest. Both provisions are clearly in breach of international standards on freedom of expression.

Internet users in Jordan not only face criminal sanctions for what they say online. Article 58 of the **Telecommunications Law** provides a basis for disconnecting users or blocking their access to telecommunications services when they use their Internet connection in ways that violate applicable laws or 'public morals'. Accordingly, Internet users could potentially be disconnected from the Internet for visiting websites deemed 'immoral'. It is unclear what 'immoral' entails or what authority would make such determinations. Similarly, Internet users could face imprisonment or hefty fines for sending 'abusive' messages across telecommunications networks. 'Abusive' is not defined and is in any event an inherently vague and subjective term.

While the lack of specific regulation of **Internet intermediaries** is positive, as noted above, it would be highly desirable for a law to fully insulate them from liability for third-party content. Internet intermediaries should only be required to restrict access to online content following a court order.

Although the Constitution and the Telecommunications Law both provide some degree of protection to online communications, this is insufficient to satisfy international law requirements. The Telecommunications Law, for instance, requires ISPs to provide the

necessary facilities to the competent parties to implement the judicial and administrative orders related to tracing the telecommunications specified in those orders (Article 29). In particular, **surveillance powers** should be clearly laid down by law in line with international standards on the right to privacy. Equally, a strong overarching law protecting **personal data** would be highly desirable.

Recommendations

- The Constitution should be reviewed and brought in line with international standards on freedom of expression.

- The speech offences contained in the Penal Code should be repealed, in particular lese-majesty, disrupting relations with friendly countries, undermining the system of governance, criminal defamation and 'insult' offences.

- Article 118 of the Penal Code should be repealed as overly broad. Only incitement to violence, hostility and discrimination should be penalized consistent with the requirements of Article 20 of the ICCPR and the UN Rabat Action Plan.

- Articles 3 to 5 and Article 13 of the Information System Crimes Law 2010 (ISC 2010) should be reviewed and brought in line with the equivalent provisions in the Budapest Convention on Cybercrime. Any references to 'websites' or 'information' should be dropped. Instead, reference should only be made to 'computer systems' or 'computer networks' and 'data' where appropriate. Article 13 should only allow the confiscation of communication

devices under a court order.

- Article 10 ISC 2010 should be amended to criminalise ‘incitement to acts of terrorism’ rather than the ‘promotion of terrorist ideologies’. The new ‘incitement to terrorism’ offence should comply with the requirements of international law.

- Article 12 ISC 2010 should be repealed and replaced by an offence of illegal access to a computer that would include an element of dishonest intent to obtain data, the infringement of security measures and a public interest defence consistent with the Cyber-crime Convention.

- Anti-Terrorism Law should narrow down the scope of what is considered terrorism and strictly define what constitutes “promotion” of terrorist thoughts and narrative on the web.

- National security offences should be narrowly defined in line with international standards on freedom of expression, including the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

- Communications monitoring requests should be issued by a judicial order only, and not administrative orders as the Telecommunication Law entails.

- Internet disconnection should only be permitted in circumstances where beneficiaries fail to pay their subscription fees. Article 58 of the Telecommunications Law should be amended accordingly.

- Article 75 (a) of the Telecommunications

Act should be amended. In particular, ‘abusive messages’, ‘messages contrary to public morals’ and ‘spreading false information with the intent to create panic’ should be struck out. Article 75 (b) should be struck out entirely.

- The Press and Publications Law 1998 should be repealed and replaced by self-regulation of the press.

- Internet intermediaries should be granted immunity from liability for third-party content by law.

- Surveillance powers should be clearly laid down by law in line with international standards on the right to privacy.

- The authorities should consider adopting a strong overarching legal framework protecting personal data.

- The net neutrality principle should be protected by law.

This report is a joint publication between Hivos' IGMENA program and ARTICLE 19.

The policy review was conducted by 7iber. Staff from IGMENA program edited the final draft.

This work is provided under the Creative Commons Attribution-ShareAlike 3.0 Unported License.

