SYRIA

ILA Country Report

INTERNET LEGISLATION ATLAS
www.internetlegislationatlas.org

SYRIA
Legal Framework

Constitutional Protection

The Syrian Constitution was approved in 1964 and revised in 2012 following the 'Syrian Uprising' in the early spring 2011. The rights to freedom of expression and privacy are guaranteed by the following articles of the Constitution:

- Article 36 protects the inviolability of private life and guarantees that "houses shall not be entered or inspected except by an order of the competent judicial authority in the cases prescribed by law".

- Article 37 further guarantees the protection of confidentiality of postal correspondence, telecommunications and radio and other communication in accordance with the law.

- Article 42 guarantees the protection of freedom of belief in accordance with the law as well as the right of every citizen to freely and openly express his or her views whether in writing or orally or by all other means of expression.

- Article 43 guarantees freedom of the press, printing and publishing, freedom of the media, including its independence, in accordance with the law.

- Article 44 further protects the right to assemble, peacefully demonstrate and to strike from work within the framework of the Constitution and in accordance with the law.

- Article 45 guarantees the freedom to form associations and unions on a national basis, for lawful purposes and by peaceful means which are guaranteed in accordance with the terms and conditions prescribed by law.

Regulation of online content

THE PENAL CODE

The Syrian Penal Code contains a number of speech offences that are equally applicable to the online environment. For instance, Article 285 of the Penal Code criminalises calls that "weaken national sentiment" in times of war. Similarly, Article 286 punishes the dissemination of false or exaggerated news that "weaken the spirit of the Nation". Under Article 287, the broadcasting abroad of false or exaggerated news that tarnishes the country's reputation is punishable by heavy fines and imprisonment of at least six months. Article 378 further criminalises defamation of the President, which is punishable by imprisonment between one month and one year, and six months in the case of defamation of the courts, the military or public authorities.

THE CYBERCRIME LAW 2012

While the Cybercrime Law does not contain content-related offences as such, it criminalises illegal access to computer systems and websites without having the right or authority or permission to do so. It also punishes with imprisonment and/or a fine anyone who copies, uses or discloses information obtained by such illegal access.

Regulation of media workers

THE PUBLICATIONS LAW 2001

Before the adoption of the Media Law in 2011, the print media was chiefly governed by the Publications Law 2001. Under that Law, the press was under tight government control. Newspapers were required to obtain a licence from the Prime Minister upon recommendation of the relevant minister in order to operate. Furthermore, anyone wishing to become an editor or owner of a periodical had to comply with a certain number of requirements in order to qualify for the position, including holding Syrian nationality, a college degree and a press card issued by the Ministry upon receipt of a letter from the Union of Journalists confirming a certain number of years of practising journalism. The Law provided for a number of other restrictions on journalistic and publishing activities. For instance, the press was prohibited from reporting on matters of national security, the activities of the army or anything affecting the 'unity of the community'. Insult, defamation and slander were also prohibited.

THE MEDIA LAW 2011

Following the Syrian uprising at the beginning of 2011, the Syrian government sought to liberalise the media sector and passed a new Media Law in August 2011, which repealed the Publications Law 2001. Among other things, the new Law proclaims that the media should be independent and that monopolies of media outlets should be prevented. The Law further removes prison sentences for a number of press offences and creates a limited right of access to information by journalists. Nonetheless, it is unclear if bloggers would be able to benefit from these provisions, as they may not qualify as journalists under Syrian law. They would therefore remain criminally liable for speech offences under the Penal Code

Furthermore, the new Media Law contains a number of restrictive provisions for the media. In particular, it provides that freedom of expression should be exercised responsibly and with consideration. The Law also replicates the provisions contained in the earlier statute prohibiting journalists from reporting on several matters, including national security, the activities of the army and religious issues, especially insofar as it might incite sectarian strife or defame religions. The publication by media outlets of any content related to incitement to acts of violence or terrorism is prohibited alongside anything that might harm state's symbols or might be in breach of an individual's privacy.

The Law also establishes a new press body, the National Council of Information. While the Council is nominally independent both financially and administratively, it is linked to the Cabinet, which approves licensing and accreditation of anyone who wants to establish a media outlet. It appears that the licensing provisions are equally applicable to online news outlets.

THE CYBERCRIME LAW 2012

A number of provisions contained in the Cybercrime Law 2012 are also relevant to journalistic work. In particular, the Law criminalises the violation of an individual's

private life on a communications network even if that information is correct. It therefore seems to replicate and adapt to the online environment the same prohibitions of the new Press Law regarding the publication of private information. Furthermore, the Cybercrime Law contains a provision criminalising the use of deception to obtain Internet users' personal or confidential information for criminal purposes. In the absence of a public interest defence, it is therefore possible that investigative journalists wishing to report on matters of public interest may be criminalised.

Regulation of Internet Intermediaries

Internet intermediaries are mainly regulated by the Cybercrime Law 2012. The Law lays down a number of obligations that Internet Service Providers (ISPs) and hosting providers must comply with. In particular, the Cybercrime Law requires ISPs to monitor and retain Internet traffic. It also provides a legal basis for Internet filtering and website blocking; the latter must be ordered by a court. In addition, professional communications service providers and website owners are required to publish their name, address and contact details. Failure to provide that information may result in the site being blocked by the authorities.

Nonetheless, the Law appears to allow for limited immunity of hosting providers for third-party content, provided they takedown content within 24 hours following: (a) a request by the content producer, (b) a court order or (c) obtaining actual knowledge of the illicit nature of the content at issue, which they are required to report to the executive.

At the same time, a number of provisions in the Cybercrime Law seemingly seek to superimpose the restrictions applicable to the press onto content and communications services online. However, the details of the mechanism whereby information may be removed, corrected or blocked is subject to further regulation by the executive. The Law further provides that it is an offence for an ISP or other communications provider to interfere with third-party content or to fail to comply with a court order or to fail to remove or correct content upon obtaining actual knowledge of its illegality. This is meted out with harsher sentences when failure to comply obstructs a criminal investigation. Finally, the Cybercrime Law provides that it is an offence to intentionally impede access to communications networks or services or websites.

Surveillance and Data Protection

We are not aware of any special law regulating the surveillance powers of the law enforcement agencies or intelligences services in Syria. However, the provisions of the Cybercrime Law 2012 suggest that ISPs are required to retain traffic data and communications data for the purposes of identifying content providers. The data retention period is determined by a commission working in concert with a technical standards body and the National Media Council. When served with a court order, ISPs are required to hand over the data retained in the course of providing access to the network. Failure to either retain or disclose the data is a criminal offence punishable by imprisonment or a fine.

The Cybercrime Law otherwise contains a number of provisions that purport to protect Internet users' rights to privacy and protection

of personal data. In particular, the Law criminalises the illegal access to information systems and interception of information. It further lays down the search and seizure powers of the authorities. While a court order is required to search emails and computer systems, both software and hardware may be inspected by police subject to the rules contained in the Criminal Procedure Code.

Net Neutrality and Access to the Internet

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

Country Analysis: Our assessment

The **Syrian Constitution** suffers from the same defects as many of the Constitutions in the MENA region. In particular, the protection of the rights to freedom of expression and privacy fall short of international standards on human rights. In particular, the provisions of the Constitution merely provide that these rights may be restricted "in accordance with the law". They therefore omit to provide that any restriction must pursue at least one of the legitimate aims enunciated in Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR) and be necessary and proportionate to that aim.

The **Penal Code** criminalises defamation, insult and slander in breach of international standards in this area. Criminal defamation has a notorious chilling effect on freedom of expression. For this reason, the UN Special Rapporteur has repeatedly stressed that defamation should be the subject of civil rather than criminal liability. The Syrian Penal Code further shields the President, the military and other public authorities from criticism. This is despite the well-established principle that public figures must be more tolerant of criticism than ordinary individuals because they inevitably and knowingly lay themselves to close scrutiny by entering the public arena. Similarly, UN bodies have made it clear that States parties should not prohibit criticism of institutions, such as the army or the administration. The Penal Code further lays down incredibly broad speech offences that would stifle legitimate discussions about political issues. This includes, for instance, the criminalisation of speech that might weaken national sentiment. The provisions of the Syrian Code are therefore out-of-kilter with international standards on freedom of expression.

Despite some limited progress in the new **Media Law 2011**, the press remains essentially under state control since licences can only be obtained with the approval of the Cabinet. It is unclear if the requirements to qualify as a journalist in Syria remain applicable. In any event, the provisions of the Publications Law 2001 display a corporatist approach to journalism, treating it as a profession rather than an activity that can be exercised by anyone. It is therefore in breach of international standards on freedom of expression. Of special concern are the provisions contained both in the Publications Law 2001 and Media Law 2011 that prohibit journalist from reporting on matters, which are clearly in the public interest, such as national security. This effectively means that

journalists are prevented from reporting on the Syrian conflict or the on-going terrorist attacks being carried out by the Islamic State of Iraq and Syria, which operates in country.

The **Cybercrime Law 2012** contains a raft of restrictive measures for free expression and the right to privacy. The most concerning provisions however are those requiring ISPs to retain Internet traffic for an indeterminate period of time in order to identify content providers. It is further unclear whether access to that data is subject to a court order or judicial oversight. Moreover, the Cybercrime Law provides a legal basis for website filtering and blocking. It further requires ISPs to monitor their networks in breach of international standards on free expression and privacy. Whilst the Law appears to offer limited immunity from liability to hosting providers, failure to restrict access to illegal content is punishable by criminal sanctions contrary to international standards in this area. It is further unclear how hosts are supposed to obtain actual knowledge of illegal activity in the absence of a court order. Other problematic measures include the criminalisation of anyone seeking to access a website without permission. This suggests that individuals could be criminalised for seeking to gain access to websites on a block list, such as foreign news sites providing information about the Syrian conflict. The Cybercrime Law further contains a number of privacy offences that would have a chilling effect on investigative journalism and reporting on public figures. All of the above measures are unjustified under international human rights law.

Recommendations

- The Constitution should be amended and reviewed in line with international standards on freedom of expression and privacy. In particular, the Constitution should provide that any restrictions on freedom of expression and privacy must be provided by law, pursue one of the legitimate aims under Article 19 (3) of the ICCPR and be necessary and proportionate in a democratic society.

- The speech offences contained in the Penal Code should be repealed.

- The Media Law 2011 should be repealed and replaced by self-regulation of the press.

- The Cybercrime Law 2012 should be entirely reviewed and at a minimum brought in line with the Cybercrime Convention 2001. More specifically:

• The provisions requiring ISPs to monitor their networks should be scrapped.

• The provisions criminalising ISPs and other Internet intermediaries for third-party content should be removed and replaced by immunity from liability for third-party content.

• Any liability for such content should be civil and limited to circumstances where the ISP failed to comply with a court order.

• Website blocking should only be ordered by a court.

• The provision requiring website owners and hosts to publish their personal data should be removed together with the provision laying down the sanctions for failure to comply with these requirements.

• The disclosure of private information without consent should generally be a civil

wrong; in any event, the use of deception to obtain personal data should be subject to a public interest or journalism exception.

• The provisions requiring ISPs to retain traffic data and content should be scrapped. ISPs should only be authorised to collect data which are necessary for business purposes. Any such data should never be retained for an unlimited period of time. Any provision of data should be retained for no longer than strictly necessary for business purposes. Any data lawfully retained by an ISP should only be accessible subject to a court order.

- Surveillance powers should be reviewed and regulated in line with international standards on the right to privacy.

- The adoption of an overarching framework on data protection should be strongly considered.

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

The policy review was conducted by Maharat Foundation. Staff from IGMENA program edited the final draft.