TUNISIA

ILA Country Report

INTERNET LEGISLATION ATLAS
www.internetlegislationatlas.org

TUNISIA
Legal Framework

Constitutional Protection

The new Tunisian Constitution was adopted by the National Constituent Assembly on 26 January 2014 and promulgated on 27 January 2014. The following provisions are of particular importance:

- Article 31 guarantees the rights to freedom of opinion, thought, information, expression and publication. It prohibits also any prior control on these liberties.

- Article 32 further guarantees the right to information and the right of access to information. The State should also work to guarantee the right of access to communication networks.

- Article 33 protects academic freedoms.

- The right to privacy is protected by Article 23, which guarantees the right to private life, the sanctity of the home and the confidentiality of correspondence, communications as well as the protection of personal data are guaranteed by Article 24.

- Article 49 provides that all rights and freedoms guaranteed by the Constitution may only be further regulated by law insofar as necessary and proportionate in a democratic society with a view to protect the rights of others, public safety, national security, public health and morals. These rights and freedoms could not be undermined by any constitutional amendment.

- Article 102 provides that the Judicial Authority "assures … the protection of rights and freedoms".

- Article 120 provides that the Constitutional Court is competent to hear referrals for a preliminary ruling on the constitutionality of certain articles of a law. Individuals involved in judicial proceedings can challenge the constitutionality of a particular statutory provision before the domestic courts, which may then ask the Constitutional Court to rule on the issue. In other words, individuals have an indirect remedy to enforce their constitutional rights.

- Article 128 stipulates the creation of the Human Rights Commission that should play an important role in protecting the liberties and rights enshrined in the new Constitution. Also, the Media Commission created by virtue of Article 127 of the Constitution has the duty to ensure respect of the freedom of expression.

Regulation of Online Content and Media Workers

Tunisia has not enacted laws regulating specifically online content.

Decree-law 115/2011 on the Freedom of Press, Printing and Publishing (also known as the Decree-law 115 or as the new Press Code) was adopted by Tunisia's interim authorities in November 2011. It superseded the 1975 Press Code, which imposed several restrictions on journalists' right to free expression. In particular, Article 11 of the Decree-law 115 guarantees the protection of journalistic sources.

This protection has been recently confirmed also in the new 2015-26 Law on Fight against Terrorism and Money Laundering voted on 25 July 2015 as Article 37 extends to journalists the protection of the professional secrecy.

However, the definition of journalists in the Decree-law 115 is restrictive. In order to qualify as a 'professional' journalist, it is necessary to obtain a bachelor's degree or an equivalent diploma and to have journalism as a regular and main activity and main source (Article 7). The press card is granted by an independent commission to any person who meets these conditions according to Article 8. Bloggers or ordinary social media users may therefore not qualify, although the Tunisian courts extended sometimes the protection provided by Decree-law 115 to these categories (e.g. Court of Appeals decision dated 14 February 2013, case No 2500).

The new Press Code also abolished prison sentences for defamation and insult but did not decriminalise defamation and insult altogether. Therefore, journalists found guilty of such crimes must pay a fine (Article 56). Moreover, the equivalent speech offences under the Penal Code enacted in 1913 are still in force. Accordingly, defamation and slander are criminalised under the Penal Code and subject to prison sentences. For instance, under Article 128 of the Penal Code, insulting public officials, institutions, administrative or judicial authorities is crime punishable by up to two years in prison. Article 226 of the Penal Code further creates offences against public morals, while Article 121 (3) makes it an offense to "distribute, offer for sale, publicly display, or possess, with the intent to distribute, sell, display for the purpose of propaganda, tracts, bulletins, and fliers, whether of foreign origin or not, that are liable to cause harm to the public order or public morals." The Article carries a penalty of six months to five years in prison. Defamation and calumny are criminalised by virtue of Articles 245-247 of the Penal Code and punishable by prison sentences. These and other speech-related provisions equally apply to things published online.

Also, Article 86 of the 2001 Telecommunication Code provides that any person who harms or disturbs the tranquillity of other persons through telecommunication networks is subject to up to one year of imprisonment. Unfortunately, Tunisian Courts sometimes use this Article or the Penal Code (Article 128 and 245-247) and ignore Article 56 of the Dercee-law 115 (e.g. the Court of Cassation decision on 28 November 2013, case No 1055104, the Tunis Court of First Instance decision on 25 February 2012, case No 617). This jurisprudential trend results in jail sentences against journalists in some cases and lack of coherence in the jurisprudence with regard to Article 56 of the Decree-law 115 that limits the sanction for defamation to a fine.

Regulation of Internet Intermediaries

In Tunisia, the liability of Internet Service Providers (ISPs) is governed by the Decree No 2014-4773 dated 26 December 2014 fixing the conditions and procedures to grant the authorisation of the activity of supplying Internet services (hereafter Decree 2014-4773). This Decree superseded the Decree No.97-501 of 14 March 1997 concerning value-added

telecommunications services (hereafter the 1997 Telecommunication Decree) and abrogates (implicitly) the Regulations of 22 March 1997 concerning the specifications for setting up and operating value-added Internet telecommunications services.

Under Article 1 of the 1997 Telecommunications Decree, producing, providing access to, disseminating and hosting information by way of electronic services is subject to the 1975 Press Code. Article 14 further provides that all ISPs must designate a director responsible for the content that travels across their networks in compliance with this Code. Read together, these provisions mean that ISPs are liable for third-party content. The Decree does not provide for any exceptions.

Article 9 of the 22 March 1997 Ministerial Order on the Regulations on the Specifications for Setting-up and Operating Value-Added Internet Telecommunications Services further expands on the obligations of ISPs in relation to content. In particular, the director responsible for online content is required to constantly monitor content to ensure that no information contrary to public order or good morals remains on the network. Moreover, the director is required to archive hardcopies of content as may be necessary for the purposes of court proceedings and keep such archives for one year. When an ISP closes down or ceases to provide Internet services, the director responsible for online content must turn over all of the ISP's archives to the Tunisian Internet Agency 'without delay'. Furthermore, under Article 8, ISPs are required to submit a list of their subscribers to the authorities on a monthly basis.

The Decree 2014-4773 represents a progress comparing to the 1997 Decree and Regulations. Yet, the ISPs have the duty, according to Article 11(3-4) of the first Decree, "to meet the requirements of the national defence, security and public safety in accordance with the legislation and regulation in force" and to "provide to the relevant authorities all the means necessary for the performance of his duties, in that context, the provider of Internet services shall respect the instructions of the legal, military and national security authorities". The ISPs may be required, therefore, to cooperate with the public authorities as needed and this may imply divulgation of customers' information or imposing some restriction on Internet navigation. However, the same Decree provides more safeguards for freedom of expression as it imposes on the ISPs the obligation to "respect the international convention and treaties ratified by Tunisia" (Article 11(5)). This includes, inter alia, the International Covenant on Civil and Political Rights. Moreover, the Decree provides the Internet user with more guarantees for their rights that were denied by the 1997 Telecommunication Decree. Thus, the ISPs are bound to keep the personal data of the customers confidential and not to divulgate them to any third-party (Article 14).

Surveillance, Data Protection and Encryption

The circumstances in which surveillance operations may be authorised under Tunisian law are unclear. It appears that the main legal basis for ordering the interception of communications in the context of criminal investigations is Article

53 of the Code of Criminal Procedures. Under that Article, investigative judges are given broad investigating powers to order any act conducive to the revelation of both exculpatory and incriminating evidence. The provisions of Decree No 20134506, which establishes the Technical Telecommunications Agency (ATT), further suggest that surveillance operations linked to the investigation of ICT-related crimes are judicially authorised (see further below).

As stated above, Article 11 of the Decree 2014-4773 provides that ISPs are required to respond to the defence and national security needs of the country subject to the conditions laid down in the legislation in force. It also specifies that the ISPs must comply with instructions received from judicial, military and security authorities as well as provide the means necessary for the performance of their functions. The same obligations are imposed on the Telecommunication Virtual Networks Operators by Decree No. 2014-412 of 16 January 2014, which lays down the conditions under which operators of virtual networks are authorised to operate. It therefore appears that some surveillance operations are not subject to judicial oversight.

As regards investigations into ICT-related crimes, the recently established ATT is tasked with the provision of technical support to judicial investigations into such crimes. In this context, it is also entrusted with overseeing the exploitation of 'national systems of data traffic control' in line with data protection law and international human rights treaties. The ATT is a government agency under the authority and financial control of the ICT Ministry. With the exception of one judge, the ATT's Followup Committee is composed of representatives from various ministries and government agencies, including interior, national defence, ICT, justice, data protection and human rights.

Notwithstanding the above, the protection of personal data is guaranteed by Law No.2004-63 of 27 July 2004. The Data Protection Authority ('INPDP') operates under the authority and control of the Ministry of Justice. It is composed of 15 members, including a representative from the Prime Minister's Office, the ICT Ministry, the Ministry of Defence and the Ministry of Interior as well as four magistrates. The INPDP is tasked with authorising certain types of data processing and generally overseeing that data protection legislation is respected. In particular, the INPDP authorises processing of sensitive data, including data about philosophical or political opinions, trade-union affiliation, religious convictions and ethnic origin. The Law otherwise guarantees a number of rights to data subjects, such as the right to oppose data processing, or seek the correction of data held about them. However, it does not contain an exception or exemption for the protection of freedom of expression, including the exercise of journalistic, artistic, literary or cultural activity. It also provides that personal

data obtained in the course of data processing cannot be used to defame anyone.

Finally, it is important to note that the 2014 Decree does not impose any restriction on encryption, while the use of encryption without authorisation was punishable by up to five years imprisonment under the 1997 Telecommunications Decree.

Net Neutrality and Access to the Internet

As noted above, the Tunisian Constitution seeks to guarantee the right of access to communication networks. At the same time, we are not aware of any specific laws or draft legislation seeking to promote such access, for instance in remote areas, or fostering a competitive environment for ISPs. Equally, the protection of net neutrality does not appear to be an issue in Tunisia. While net neutrality may be protected in practice, it is not protected by primary legislation. Nonetheless, Article 14 of Decree No. 2014-412 of 16 January 2014 provides that operators of virtual private networks must guarantee the neutrality of their services to their clients. Also, Article 14(1) of Decree 2014-4773 imposes the same obligation on the ISP who is bound to "take necessary measures to ensure the neutrality of his services".

Other Issues

While not directly relevant to freedom of expression online, it is worth noting that the Tunisian government has taken a number of steps to promote a new culture of transparency in Tunisia. In particular, the interim government adopted Decree-law 2011-41 guaranteeing access to administrative documents. A draft law on freedom of information was submitted to the Parliament on 18 August 2014 as well as legislation with a view to protecting whistleblowers.

Country Analysis: Our assessment

The **Tunisian Constitution** guarantees a strong level of protection to the rights to freedom of expression and information as well as the right to privacy in line with international standards on human rights. Moreover, individuals have a remedy at their disposal to challenge the constitutional validity of certain statutory provisions.

As noted above, there are no laws dealing specifically with **online content** in Tunisia. This is in line with the legislation of most democracies, which only tend to have separate laws to deal with defamation, hate speech, incitement to terrorism etc. These laws apply to all forms of expression regardless of the media.

At the same time, existing **speech offences** under the Penal Code, such as defamation of public officials, hate speech, and insults, **the Telecommunication Code** and **the 2011 Press Code** fall short of international standards on freedom of expression. While the new Press Code contains many positive features, such as the protection of journalistic sources, it remains too limited in its scope, since the status of 'professional journalist' may only be obtained subject to certain conditions. Accordingly a blogger is more likely to receive

a prison sentence for the same offence as a journalist (e.g. criminal defamation). Moreover, and in any event, we believe that speech offences such as criminal defamation are in violation of international standards on freedom of expression.

The legal framework governing **intermediaries' liability** was improved as the provisions contained in the 1997 Internet Regulations were abrogated, such as the requirement for ISPs to submit a list of their subscribers to the authorities on a monthly basis. However, the new text does not guarantee explicitly immunity from liability to Internet intermediaries for content produced by third parties.

While **surveillance** may no longer be the norm following the fall of the Ben Ali regime, the legal framework governing surveillance powers does not appear to have been reformed to ensure its compliance with international standards on privacy. The Criminal Procedure Code and various legal texts cited above are far from adequate to provide the level of legal certainty and protection of privacy rights required under international human rights law. The new **2013 Decree** raises issues both in terms of the independence of the organisation tasked with 'assisting' judicial investigations in ICT-related crimes and the guarantees offered to ensure the protection of Internet users' rights to privacy when implementing measures of 'data traffic control'.

This is all the more important given that the **data protection framework** is clearly insufficient to guarantee the protection of Internet users' personal data. In particular, the independence of the Tunisian Data Protection Authority from the government needs to be enhanced to avoid any arbitrary government interference. Moreover, the lack of exemptions for journalistic and other activities involving the exercise of the right to freedom of expression means that the law is open to abuse.

However, the new l**aw 2015-26 on fight against terrorism and money laundering** requires in its Article 57 a judicial authorisation for any surveillance of communication networks or interception of communications aiming at investigating the alleged terrorist activities. These positive provisions in the new law should be included also in the Code of Criminal Procedures to ensure all investigation procedures are in line with internal standards with regard to the respect of the privacy.

Recommendations

- Bloggers and citizen journalists should not be regulated other than by way of the same civil and criminal laws that apply to non-Internet users, subject to our recommendations below concerning the 2011 Press Code.

- The 2011 Press Code should be amended to entitle bloggers to source protection.

- The 2011 Press Code should be amended to decriminalise defamation.

- The 2011 Press Code, Penal Code and the Telecommunication Code should be harmonised with regard to defamation to avoid contradiction. Meanwhile, the Tunisian courts should adopt a liberal interpretation of the law and stop using the Penal Code and Telecommunication Code against journalists.

- The hate speech provisions should be more tightly drafted in line with international standards on freedom of expression.

- The law should be amended to explicitly require that only the courts may grant a blocking/filtering/removal order subject to the principles of necessity and proportionality;

- The law regarding the protection of personal data should be amended in order to protect bloggers and citizen-journalists against penal sanctions planned by this law.

- The independence of the Data Protection Authority should be improved mainly by reviewing its structure and the nomination process of its members and their status to avoid any potential political interference.

- The Code of Criminal Procedures should be amended to include the judicial authorisation for any surveillance of communication networks or interception of communications aiming at investigating the alleged crimes.

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

The policy review was conducted by Amor Boubakri (independent consultant). Staff from IGMENA program edited the final draft.