Tunisia: Digital Communications Code 2020

May 2020

Legal analysis

Executive summary

In this analysis, ARTICLE 19 reviews the compatibility of the draft Digital Communications Code 2020 (the Draft Code) with international standards on freedom of expression.

The Draft Code is an ambitious piece of legislation that seeks to regulate a potentially very substantial sector of the Tunisian economy. The Draft Code aims to update the existing legal framework and foster Tunisia's digital economic development. As such, the Draft Code seeks to amend and streamline various legal provisions and provide a uniform vision for the governance of electronic communications. It is also meant to bring Tunisian law in line with international best practices in the area of digital communications.

In the analysis, ARTICLE 19 outlines our key concerns with the Draft Code against Tunisia's obligations under international human rights law. We conclude that the Draft Code contains some positive provisions on intermediary liability and a relatively limited number of problematic offences. Nonetheless, some key challenges remain. In particular, there is a lack of clear structure of the Draft Code; clear definitions of key terms and concepts are missing from the Draft Code or are used inconsistently throughout; and the licensing regime is confusing and remains under the control of the executive rather than being overseen by an independent authority.

In addition, the intermediary liability rules could be further clarified and be brought more closely in line with international standards on freedom of expression and best practice such as the Manila Principles on Intermediary Liability.

ARTICLE 19 urges the Tunisian Government and legislators to amend the Draft Code to address these concerns and to bring the Draft Code into line with the highest international standards in this area.

Summary of recommendations

- The protection of human rights, especially the rights to freedom of expression, privacy and non-discrimination, should be explicitly mentioned as a key objective of the Draft Code.

- The Draft Code must be re-structured and different aspects of the new licensing regime made clearer. Too many rules are left to be determined by government order and should instead be clarified in the Draft Code.

- Several definitions, including electronic communications service, online platform operator, Internet services, Internet Access service, and vital and sensitive infrastructure, must be narrowed or clarified in accordance with international standards or best practice.

- The licensing regime must be overseen by an independent Authority, not the Executive.

- Any mandatory measures necessary for the protection of children should be spelled out in the law, compliant with international standards on the protection of freedom of expression and privacy and subject to parliamentary scrutiny.

- The independence of the National Electronic Communications Agency must be guaranteed in law, including through provisions on funding arrangements and membership. The Agency must be accountable to Parliament, not the Executive;

- Intermediary liability rules must clarify that actual knowledge of illegality can only be obtained by a court order. More generally, they should be in line with the Manila Principles on Intermediary Liability.

- The offences contained in Articles 250 and 251 must be deleted.

Table of contents

Introduction

In May 2020, ARTICLE 19 analysed Tunisia's Draft Digital Communications Code (the Draft Code). The Draft Code is an ambitious piece of legislation that seeks to regulate a potentially very substantial sector of the Tunisian economy. In its statement of reasons for the Draft Code, the government said that the current legal framework was out-of-date and that a new, more competitive, approach was needed to foster Tunisia's digital economic development. The Government has also explained that the draft Code seeks to update and streamline various legal provisions to provide a uniform vision for the governance of electronic communications. The Draft Code is also meant to bring Tunisian law in line international best practice in the area of digital communications.

In this analysis, ARTICLE 19 outlines our key concerns with the Draft Code against Tunisia's obligations under international human rights law, in particular Article 19 of the International Covenant on Civil and Political Rights. We also offer specific recommendations on how each section discussed below may be modified to ensure their compatibility with international standards. While ARTICLE 19 focuses on key concerns for freedom of expression in the Draft Code, the absence of comments on other sections does not signal our endorsement.

ARTICLE 19 concludes that the Draft Code contains some positive provisions on intermediary liability and a relatively limited number of problematic offences. Nonetheless, some key challenges remain, including: a lack of clear structure of the Draft Code, a lack of clear definitions of key terms and concepts, which are used inconsistently throughout the Draft Code and a confusing licensing regime that remains under control of the executive rather than being overseen by an independent authority. In addition, the intermediary liability rules could be further clarified and be brought more closely in line with international standards on freedom of expression and best practice such as the Manila Principles on Intermediary Liability.

We urge the Tunisian Government to follow the recommendations in this analysis and we stand ready to provide further support in this process.

Applicable international human rights standards

The right to freedom of expression

The right to freedom of expression is protected by Article 19 of the Universal Declaration of Human Rights (UDHR),[1] and given legal force through Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[2]Tunisia ratified the ICCPR in 1969 and is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19 of the ICCPR. Furthermore, the right to freedom of expression is also guaranteed in Articles 31 and 32 of the Constitution of the Republic of Tunisia.

The scope of the right to freedom of expression is broad. It requires States to guarantee to all people the freedom to seek, receive or impart information or ideas of any kind, regardless of frontiers, through any media of a person's choice. The UN Human Rights Committee (HR Committee), the treaty body of independent experts monitoring States' compliance with the ICCPR, has affirmed that the scope of the right extends to the expression of opinions and ideas that others may find deeply offensive.[3]

While the right to freedom of expression is fundamental, it is not absolute. A State may, exceptionally, limit the right under Article 19(3) of the ICCPR, provided that the limitation is:

- **Provided for by law**; any law or regulation must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly.

- **In pursuit of a legitimate aim**, listed exhaustively as: respect of the rights or reputations of others; or the protection of national security or of public order (*ordre public*), or of public health or morals;

- **Necessary and proportionate in a democratic society**, i.e. if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.[4]

Thus, any limitation imposed by the State on the right to freedom of expression must conform to the strict requirements of this three-part test. Further, Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law.

[1] Through its adoption in a resolution of the UN General Assembly, the UDHR is not strictly binding on states. However, many of its provisions are regarded as having acquired legal force as customary international law since its adoption in 1948; see *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).
[2] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, UN Treaty Series, vol. 999, p. 171.
[3] See HR Committee, General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, para 11.
[4] HR Committee, *Velichkin v. Belarus*, Comm. No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

Freedom of expression online and intermediary liability under international law

In 2012, the UN Human Rights Council (HRC) recognised that the "same rights that people have offline must also be protected online."[5] The HR Committee has also made clear that limitations on electronic forms of communication or expression disseminated over the Internet must be justified according to the same criteria as non-electronic or "offline" communications, as set out above.[6]

While international human rights law places obligations on States to protect, promote and respect human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights.[7] Importantly, the UN Special Rapporteur on freedom of opinion and expression (Special Rapporteur on FOE) has long held that censorship measures should never be delegated to private entities.[8]In his June 2016 report to the HRC,[9] the Special Rapporteur on FOE enjoined States not to require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means. He further recognised that "private intermediaries are typically ill-equipped to make determinations of content illegality,[10] and reiterated criticism of notice and takedown frameworks for "incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation," i.e. the danger of "self- or over-removal."[11]

The Special Rapporteur on FOE recommended that any demands, requests and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under Article 19 (3) of the ICCPR.[12]

In their 2017 Joint Declaration on freedom of expression, 'fake news', disinformation and propaganda, the four international mandates on freedom of expression expressed concern at "attempts by some governments to suppress dissent and to control public communications through [...] efforts to 'privatise' control measures by pressuring intermediaries to take action to restrict content."[13] The Joint Declaration emphasises that:

> [I]ntermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

In his April 2018 report, the Special Rapporteur on FOE noted that States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in

---

[5] HRC Resolution 20/8 on the Internet and Human Rights, A/HRC/RES/20/8, June 2012.
[6] General Comment No. 34, *op cit.*, para 43.
[7] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The UN Human Rights Council endorsed the guiding principles in HRC resolution 17/4, A/HRC/RES/17/14, 16 June 2011.
[8] Report of the Special Rapporteur on FOE, 16 May 2011, A/HRC/17/27, paras 75-76.
[9] Report of the Special Rapporteur on FOE, 11 May 2016, A/HRC/32/38, paras 40 – 44,
[10] *Ibid.*
[11] *Ibid.*, para 43.
[12] *Ibid.*
[13] Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, adopted by the Special Rapporteur on FOE, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 3 March 2017.

accordance with due process and standards of legality, necessity and legitimacy.[14] He went on to state that States and intergovernmental organisations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship. He also recommended that States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.

As a state party to the ICCPR, Tunisia must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 ICCPR as interpreted by the UN Human Rights Committee and that they are in line with the special mandates' recommendations.

Online content regulation under international law

The requirement that all limitation imposed by the State on the right to freedom of expression online must conform to the strict requirements of this three-part test have been endorsed and further explained in several reports of the Special Rapporteur on FOE[15]in which he clarified the scope of legitimate restrictions on different types of expression online.[16]He identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;

- expression that is not criminally punishable but may justify a restriction and a civil suit; and

- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[17]

In particular, the Special Rapporteur on FOE clarified that the only exceptional types of expression that States are required to prohibit under international law are: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; and (d) incitement to terrorism. He further made clear that even legislation criminalizing these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[18] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

The Special Rapporteur on FOE also highlighted his concern that a large number of domestic provisions seeking to outlaw hate speech are unduly vague, in breach of international standards for the protection of freedom of expression. This includes expression such as combating "incitement to religious unrest," "promoting division between religious believers and non-believers," "defamation of religion," "inciting to violation," "instigating hatred and disrespect

[14] See Report of the Special Rapporteur on FOE, A/HRC/38/35, 6 April 2018.
[15] See the May 2011 and August 2011 Reports of the Special Rapporteur on FOE, *op.cit*.
[16] *Ibid.*, August 2011 Report, para 18.
[17] *Ibid.*, paras 20-36.
[18] *Ibid*, para 22.

against the ruling regime," "inciting subversion of state power" and "offences that damage public tranquillity."

The protection of the right to privacy and anonymity online

Guaranteeing the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. The right of private communications is strongly protected in international law through Article 17 of the ICCPR.

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test.[19] In 2017, the HRC confirmed this in Resolution 34/7.

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. In his 2011 report, the Special Rapporteur on FOE expressed his concerns that:

> [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individual's communications and activities on the Internet. Such practices can constitute a violation of the Internet user's right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.[20]

In particular, the Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[21]

In his May 2015 report on encryption and anonymity in the digital age, the Special Rapporteur on FOE concluded:

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. (…)
>
> States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access

[19] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.
[20] The May 2011 Report of the Special Rapporteur on FOE, *op.cit.,* para 53.
[21] *Ibid.*, para 84.

> to digital communications and online services and requiring SIM card registration for mobile users (...)[22]

The findings of this report confirmed the earlier findings of the 2013 report of the Special Rapporteur on FOE, which observed that restrictions to anonymity facilitates States' communications surveillance and have a chilling effect on the free expression of information and ideas.[23]

Cybercrime

ARTICLE 19 notes that there is no international standard on cybercrime. From comparative perspective, we note that the Council of Europe Convention on Cybercrime CETS (Cybercrime Convention)[24]provides a helpful guidance on how to draft cybercrime legislation in accordance with human rights standards. In particular, it contains basic definitions, including a definition of computer data, computer system, traffic data and service provider.

The Convention further requires its signatory parties to create offences against the confidentiality, integrity and availability of computer systems and computer data, computer-related offences such as forgery and content-related offences such as the criminalisation of child pornography. In addition, the Convention mandates the adoption of a number of procedural measures to investigate and prosecute cybercrimes, including preservation orders, production orders and search and seizure of computer data.

Finally, and importantly, the Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights consistent with the Contracting parties' obligations under the European Convention on Human Rights and the ICCPR. Tunisia has requested to accede to the Cybercrime Convention.[25]

[22] Report of the Special Rapporteur on FOE, A/HRC/29/32, 22 May 2015, paras 56 and 60 respectively.
[23] *Ibid.*, paras 48-49.
[24] The Council of Europe Convention on Cybercrime, CETS No. 185, adopted on 23 November 2001 in force since July 2004. The Convention and has been ratified also by countries outside of the Council of Europe, including Philippines, Japan or Australia.
[25] For the record of Tunisia's request, see here.

Analysis of the Draft Code

The Draft Digital Code is made up of 251 articles. It is divided into six Chapters. Chapter 1 deals with General Provisions, Chapter 2 concerns Infrastructure and Communication Resources, Chapter 3 deals with Digital Trust and the Protection of the National Digital Space, Chapter 4 sets out key provisions on Rights and Liberties in the Digital Space, Chapter 5 is concerned with Economic and Social Development and Chapter 6 sets out Offences, Violations and Penalties.

For the purposes of this analysis, ARTICLE 19 focuses on key definitions in Chapter 1 and sets out our key concerns for the protection of freedom of expression in Chapter 4 and 6.

Chapter 1, Article 2 – The protection of human rights

ARTICLE 19 welcomes the adoption of specific provisions in the Draft Code guaranteeing the protection of freedom of expression by electronic communications operators (Article 9) and equal access to the Internet (Article 8). Nonetheless, ARTICLE 19 regrets that the protection of human rights, especially the rights to freedom of expression, privacy and non-discrimination, is not given more prominence as a key objective of the legislation in Article 2. In our view, this suggests that the protection of human rights is not a government priority in this sector.

We also note that Article 8 of the Draft Code potentially delegates the responsibility to protect certain human rights to the private sector. While we generally support the responsibility of non-state actors to respect human rights, we stress that this should never be equated with an abdication of responsibility on the part of the State. We further note that delegating the responsibility to protect freedom of expression and related freedoms to the private sector could potentially raise issues of privatisation of censorship.

Recommendations:

- The protection of human rights, especially the rights to freedom of expression, privacy and non-discrimination, should be explicitly mentioned as a key objective of the legislation in Article 2 of the Draft Code.

Chapter 1, Article 3 - Definitions of key terms and concepts

ARTICLE 19 notes that Article 3 of the Draft Code sets out the definition of series of key terms, such as "electronic communications," "electric communications service,, "radio and television broadcasting services," "Internet access service," "Internet services," "electronic communication network," "public electronic communication network," "private electronic communication network," "public electronic communication network operator," "Online platform operator," "electronic communication service provider,, "Internet Service Provider" and "Internet Access Service Provider," among others.

At the outset, we note that given the large number of definitions contained in Article 3, it might be helpful to number them for ease of reference.

Secondly, we are concerned that some key concepts lack definition or are too broadly defined. In particular:

- **Digital economy:** a definition of 'digital economy' or 'digital economy activities' is currently missing from the Draft Code. In our view, it would be helpful to define these terms in order to clarify the scope of the Draft Code and therefore bring greater legal certainty to economic actors in this area. This is particularly important given that the concept of 'digital economy' appears to be central to the Draft Code.

- **Digital safety:** 'digital safety' is defined as "measures and procedures aimed at protecting information systems, networks, and digital data from attacks, intrusions and other incidents that hinder their exploitation." We note that various regulatory instruments around the world make reference to the concept of 'security' and in particular to the security of networks and services. In practice, this means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services. Because the security of networks and services is a public objective that implies certain obligations from both government and private actors owning and managing the networks and providing the service, a more precise definition, in line with international best practice, would be helpful to the entire sector. It would also benefit end-users, who would be better protected from the risk of arbitrary intrusion in their communications on the basis of vaguely defined 'digital safety'.

Thirdly, ARTICLE 19 is concerned that Article 3 provides for a number of overlapping and vague definitions, which are likely to fail the legality test under international human rights law. In particular:

- **Electronic communications service**: the Draft Code defines an electronic communications service as "a service that secures communications between two or more parties whether partially or entirely." This definition is extremely broad. It encompasses both the conveyance of signals on electronic communications networks (traditional telephone), Voice over Internet Protocol services (VoIP) such as Skype or instant messaging services. It also includes social media services. This is a problem because Article 12 provides that the provision of "electronic communications services" is subject to a pre-authorisation or a permit system. In other words, this could potentially mean that services such as instant messaging or social media are subject to licensing requirements. If so, this would be a severe restriction of the right to freedom of expression and in breach of international human rights law.

  It is true that under Article 13 some activities "that adopt electronic communications are not subject to the system of authorisation or pre-authorisation" and can be "freely practiced." However, it is unclear what activities fall within the ambit of Article 13.

  Equally, Articles 14-18 of the Draft Code suggest that the licensing system would primarily apply to telecommunications operators in practice. However, this is not clear from the definition outlined above, read in conjunction with Article 12. By contrast, we note that under the EU Framework Directive, for instance, 'electronic communications service' means "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information

society services (…)." The Framework Directive effectively applies to telecommunications services whilst another regime is applicable to information society providers and providers of content or exercising editorial control over content.

In our view, different types of communications services, e.g. telecommunications services on the one hand and other digital services on the other hand, call for different regulatory approaches. These differences should be reflected in the way in which these services are defined. We urge the drafters to clarify and narrow the definition 'electronic communication service' to enable a distinction between telecommunications services and other types of digital services, such as social media. For the purposes of the Draft Code, this would also enable a distinction to be drawn between electronic communication providers and online platform operators (see below).

- **'Online platform operator'**: the definition of 'online platform operator' makes reference to "the classification or preparation of references, through computer algorithms, for the content, goods or services provided or put online by others; or in the form of connecting multiple parties with the aim of selling something, providing a service, exchanging, or sharing a content, an object or a service." First, it is worth noting that this definition seems to leave out services like WhatsApp or similar instant messaging platforms. Secondly, online platform operators, as defined, also fall in the definition of electronic communication providers. This is likely to have implications for the regulatory regime applicable to them and could potentially lead to significant legal uncertainty unless these terms are defined more narrowly and used consistently throughout the Draft Code;

- **'Internet services' and 'Internet access service'**: the distinction between "Internet services" or "Internet Access service" is unclear and for all intents and purposes, both definitions appear to be the same. If the applicable regime to Internet services and Internet Access Service providers is different, it is likely to lead to confusion as to what requirements providers are meant to fulfil;

- **Other examples**: other examples of unclear terminology include: the lack of definition of 'electronic communications activities' in Article 3 despite its use in Article 13 and 15, the lack of definition of 'public operator of electronic communications and the related service provider' under Article 3 despite reference being made to such an operator in Article 16;

- **'Comprehensive/full electronic communication services':** the definition of "comprehensive/full electronic communication services" would benefit from a stricter reliance on the commonly understood concept of universal service;

- **'Vital and sensitive infrastructures'**: the Draft Code explains that vital and sensitive infrastructures are considered 'vital when damaging them, leaking or losing the data hosted in them compromises activities of vital importance.' However, this definition does not provide any meaningful indication of what should be considered 'of vital importance'. This broad and vague definition therefore leaves the door open to abuse.

In ARTICLE 19's view, it is vital for these definitions to be carefully reviewed and narrowed according to the types of services provided and therefore the regulatory framework applicable to them. We also urge lawmakers to ensure consistency in the terminology being used throughout the Draft Code in order to avoid legal uncertainty for actors in this sector and prevent the risk of arbitrariness and abuse of power in the application of the rules by the regulator.

Recommendations:

- Definitions in Article 3 should be numbered;

- Several definitions, including electronic communications service, online platform operator, Internet services, Internet Access service, and vital and sensitive infrastructure, must be narrowed or clarified in accordance with international standards or best practice.

Chapter 1, Articles 13-19–General provisions on licensing regime

ARTICLE 19 has three key concerns in relation to the licensing regime.

Lack of clear structure of the licensing regime

ARTICLE 19 notes at the outset that the licensing regime is not readily apparent from the proposed structure of the Draft Code. We therefore strongly suggest revising the Draft Code's structure to make the licensing regime more apparent and easier to follow.[26]

Lack of clarity of the rules and processes

ARICLE 19 further observes that the licensing regime itself is unclear with some actors required to obtain a licence (Article 14) and others a pre-authorisation (Article 15). However, the difference between the two regimes is unclear.

Moreover, the proposed licensing regime is lacking in detail. For instance, we note that under Article 15, "the conditions and procedures related to the pre-authorisation system are defined by government order." In our view, this is deeply inappropriate as it gives broad discretionary power to the executive to come up with whatever rules it likes. For instance, the government could set out content conditions as a pre-requisite for obtaining a licence in breach of international standards on freedom of expression.

This lack of detail also applies to the notification system applicable to some undefined 'electronic communications' activities. Under Article 13, these activities can be practiced freely but still have to comply with undefined obligations related to "health, environmental protection and the requirements of public security, national defence and the respect of regulations in force and the decisions of National Authority for Electronic Communications."

Licensing regime administered by the executive

Most importantly, ARTICLE 19 is concerned that the licensing regime proposed under the Draft Code grants the Ministry in charge of electronic communications the power to issue licences (Articles 14 and 19) or pre-authorisations to operators (Article 15). While the National Authority for Electronic Communications and the National Frequency Agency would be consulted for pre-authorisations, the decision to award pre-authorisations would ultimately rest with the executive.

This is in breach of international standards and best practice in this area. ARTICLE 19 recalls that all formal powers in the areas of electronic communications regulation should be exercised by independent public authorities, i.e. protected from political or economic interference. Independence should be secured, among other things, by an appointment process for members which is open, transparent, involves the participation of civil society, and is not controlled by any particular political party. In other words, licences should not.

[26] *C.f.* ARTICLE 19, Access to the Airwaves, Principles on Freedom of Expression and Broadcast Regulation, 2002.

Content obligations

Additionally, ARTICLE 19 notes that under Article 16 the public operator of electronic communications and the related service provider would be required to protect intellectual property. It is entirely unclear why this obligation has been singled out in the context of licensing obligations. In our experience, intellectual property rights holders have been strongly lobbying for mandatory filters so that content that they claim to be in breach of copyright can be blocked. In the EU, however, the Court of Justice of the European Union has found that the types of filters demanded by copyright holders would involve the systemic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. As such, the contested filters could be in breach of the data protection rights of Internet users as we well as their right to freedom of information since the filters may not distinguish adequately between lawful and unlawful content.[27] We would therefore strongly recommend deleting the protection of intellectual property from the list of conditions that telecommunications operators must meet.

We also observe that under Article 16, the public operator of electronic communications would be further mandated to "taking the necessary measures to protect users, minors and children over the network." Again, it is entirely unclear how operators are supposed to comply with this obligation. In practice, it could give great latitude to the government or a regulator to decide that this involves mandatory filtering or age verification systems in breach of international standards on freedom of expression or privacy. In our view, if telecommunications operators must take measures to protect children, these measures should be spelled out with more specificity, be compliant with international standards on freedom of expression and privacy and be subject to parliamentary scrutiny.

Recommendations:

- The Draft Code should be restructured to make the licensing regime more apparent and easier to follow;
- The Draft Code should set out the licensing and notification regime in more detail rather than leave it to statutory instruments in order to prevent the arbitrary exercise of unduly wide discretionary powers;
- Licences or pre-authorisations should be awarded by an independent public authority, not the government;
- The protection of intellectual property should be deleted from the list of conditions that telecommunications operators must meet;
- Any mandatory measures necessary for the protection of children should be spelled out in the law, compliant with international standards on the protection of freedom of expression and privacy and subject to parliamentary scrutiny.

Chapter 2, Section 7–National Electronic Communications Agency

ARTICLE 19 welcomes the proposal to have a National Authority dealing with the electronic communications sector. Nonetheless, we have a number of concerns with Section 7.

[27] See CJEU, *SABAM v Scarlet Extended*, Case C-70/10, 24 November 2011.

Lack of independence

ARTICLE 19 recalls that the Authority dealing with electronic communications must operate autonomously, with independence of judgment, and in the service of the public interest. It must be impartial and must perform its functions without fear, favour or prejudice. The Authority must enjoy functional and administrative independence from any other person or entity, including the government and any of its agencies, and no person or entity must seek to influence the Authority's members or staff in the discharge of their duties, or to interfere with the activities of the Authority. This autonomy must be respected at all times.

However, we note that Section 7 contains a number of provisions that undermine the independence of the Authority. In particular:

- Article 92 provides that the administrative and financial organisation as well as the methods of running the Authority are to be prescribed in a governmental order. The choice of this instrument, rather than a regulatory framework, exposes the Authority to the exercise of discretionary power by the government.

- Article 102 gives the government a key role in the selection and appointment of the Authority's President and of the Board members. Instead, the power to appoint them should be granted to a multi-stakeholder group that includes the government, the National Assembly, civil society and other relevant stakeholders, such as academia and sector experts, in order to guarantee the independence of these roles.

- Article 103 provides that the chair and the members of the Authorities' wages, privileges and allowances are determined by governmental order. In other words, members of the Authority are once again subject to governmental discretion. Furthermore, Article 109 provides that the Authority prepares an annual report on its activities to be submitted to the Prime Minister and the Minister in charge of electronic communications and publishes it for the general public. Instead, an independent Authority should report to the National Assembly, not to the government, as its accountability is towards the public, not the government.

Transparency and accountability

In addition to being independent, the Authority has to guarantee the highest standards of transparency and accountability. With this in mind, ARTICLE 19 warns against the provision in Article 109, which establishes that meetings and deliberations of the council shall not be public. On the contrary, we strongly recommend that all deliberations should be made public and accessible to the general public via appropriate channels, such as their publication on the Authority's website.

Powers and Tasks

Article 94 lists the Authority's powers and tasks. ARTICLE 19 recommends adding an obligation for the Authority to exercise its powers and execute its tasks based on the principles established in the first section of this Code, and in particular: freedom of expression and information; freedom of media; freedom of publication and communication on the internet; free, transparent and non-discriminatory access to the Internet.

We further note that the language in Article 94 is often vague and imprecise. For example, a number of tasks have to be undertaken 'in cooperation with the concerned public structures'.

It is not clear who the 'concerned public structures' are nor what the 'cooperation' implies. Another example is the task 'Setting the rules for organizing and monitoring the integrity of the fairness and transparency of the activities that it has under consideration and setting the mechanisms for their implementation'. The provision should better define the concepts of 'organising and monitoring' and of 'the activities (...) under consideration', which in this formulation are overbroad and undefined.

Decisions

Article 96 makes reference to 'judicial' decisions. However, the Authority is an independent regulatory body, not a judicial authority, and therefore it is not in a position to issue judicial decisions. ARTICLE 19 recommends amending the wording of Article 96 so that 'judicial' decisions is replaced by 'administrative' decisions.

ARTICLE 19 generally welcomes the introduction of the possibility of appeal against the decisions of the Authority. We strongly believe that for the Authority to be fully transparent and accountable, all its decisions issued in the discharge of its functions and which affect individual rights should be public, be accompanied by written reasons and be subject to a right of appeal before the relevant courts.

Sanctions

ARTICLE 19 is fully aware that sanctioning powers are necessary to regulate a sector of economy activity properly. However, for those powers to comply with international standards on human rights, they should be narrowly defined, pursue a legitimate aim and be necessary and proportionate. In addition, a right of appeal or judicial review against sanctions should be available to affected parties.

Under Article 124, however, the Authority has the power to impose on operators that have breached the relevant rules 'special conditions' when carrying out the activity. In our view, this wording is overbroad and does not provide economic operators with sufficient certainty about the possible consequences of their actions. With regard to the procedure, we note that Article 123 should also include the possibility for the actors given a cease and desist warning to provide their reasons and arguments about the allegations, which should be duly assessed by the Authority before imposing any sanctions or enforcing any obligations.

Finally, operators should have a right of appeal to the competent courts for review of the Authority's decisions imposing the penalties.

Recommendations:

- The independence of the National Electronic Communications Agency must be guaranteed in law, including through provisions on funding arrangements and membership. The Agency must be accountable to Parliament, not the Executive;

- The meetings and deliberations of Authority Council should be made public;

- Article 94 should clearly state the Authority must exercise its powers with a view to upholding the right to freedom of expression;
- Sanctions must be more narrowly defined, including Article 124. Economic actors should be given a right to be heard before any sanction is imposed and have a right of appeal or judicial review against decisions made by the Authority.

Chapter 4– Rights and Liberties in the digital space

At the outset, ARTICLE 19 would like to point to some generally positive features in Section 4 on Rights and Liberties in the digital space:

- We welcome Article 200 that gives a **right to users of electronic communication services to file individual or group cases** before the courts for violations by public network operators or providers of electronic communication services of their obligations under section 4 of the Code.

- We also commend the approach to **the protection of minors** in Article 201 that focuses on warnings about inappropriate content and giving the ability to consumers to download filtering software as a matter of choice. We reiterate that the protection of children or minors should not be used as a pretext to impose filtering obligations or age-verification systems in breach of the rights to freedom of expression and privacy.

- While we generally welcome the stated goal of Article 187, i.e. **guaranteeing the right to free, transparency and non-discriminatory access to the Internet**, we believe that it should use more decisive language. Instead of promising to 'work to guarantee' this right, the State should simply guarantee it. Moreover, the subclause about the 'requirements of public security and national defence" is nebulous and potentially provides a blank cheque to the government to restrict this right without sufficient justification. It should be clarified or better still, removed entirely.

- Similarly, we welcome the **protection of users' personal data and privacy rights** in both Article 195 and 196.

However, we are concerned that the obligations of electronic communication network operators and service providers towards their users are made subject to the 'requirements of public security and national defence' without clearly spelling out the circumstances in which these exceptions might apply. This is particularly concerning given that these exceptions are mentioned separately from circumstances in which operators might be required to disclose their users' personal data subject to 'the powers of the judiciary'. It therefore suggests that operators may be required to handover the personal data or private information of their users to law enforcement or intelligence agencies without a court order and merely on the ground that it is for 'public security' or 'national defence' purposes.

In our view, this is contrary to international standards on freedom of expression and privacy.

- First, while the right to privacy and personal data may be restricted for law enforcement or national security purposes, this can only be justified if the restriction is set out in law with sufficient precision so that people can foresee its effects.

  For instance, from comparative perspective, we note that the European Court of Human rights has found that it was "essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public

authorities are empowered to resort to any such measures."[28] The Court further noted that "since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[29]

- Secondly, international standards are clear that surveillance measures should in principle be entrusted to the supervisory control of a judge because judicial control offers the best guarantees of independence, impartiality and a proper procedure.[30] In our view, the reference to the requirements of public security and national defence is too vague and should be removed from Article 195. At the very least, reference should be made to the appropriate legislation setting out the circumstances in which law enforcement or national intelligences agencies may be granted access to users' personal data.

Additionally, ARTICLE 19 is concerned by a number of provisions in Chapter 4 that are either unclear or concerning from a human rights perspective:

- **Codes of Conduct**: Article 194 provides that the Authority "urges electronic communication network operators and service providers to formulate and adopt codes of conduct that guarantee the rights of service users". The Authority approves these Codes and can ask the concerned operator to change some of its provisions in observance of these rights. ARTICLE 19 is concerned that the Codes of Conduct could be used to codify restrictions on online content in the absence of parliamentary scrutiny. We have seen proposals along those lines in the United Kingdom with the Online Harm White Paper.[31] If used for this purpose, Codes of Conduct are deeply undesirable, particularly in relation to social media platforms.[32]

- **Identification of users and data registry:** Article 202 of the Draft Code providers that operators of public networks for electronic communications and the providers of services exploited through them must obtain from their users "all data specified for their identity before they are allowed to use the service." They must also take undefined 'necessary precautions' to ensure that their service distributors and 'dealers' obtain their clients' identity data. The data necessary to identify users, as well as the conditions and procedures for obtaining them, are determined by a decision of the Minister in charge of electronic communications. Article 203 further provides that the operators of public electronic networks and electronic service providers must maintain a registry containing the data specified for the identity of the service user and the documents supporting them.

  ARTICLE 19 is deeply concerned by these provisions. In our view, this constitutes an unnecessary and disproportionate interference with the rights to privacy, data protection and freedom of expression. In particular, we note that for the collection of their users' personal data to be lawful, telecommunications operators should only be able to collect the

[28] See European Court, *Roman Zakharov v Russia*, App. No. 47143/06, [GC], 4 December 2015, para 229.
[29] *Ibid.*, para 230.
[30] *Ibid.* para 233.
[31] ARTICLE 19, Response to the Consultations on the White Paper on Online Harms, June 2019.
[32] This is without prejudice to content rules developed in a broadcasting context, see ARTICLE 19's Access to the Airwaves, *op.cit.*, Principle 23.

personal information of their users that are necessary for the delivery of the service and billing purposes. As such, it should not require the use of identification documents such as ID cards, passports or driving licences. However, the language of Article 202 is so broadly drafted that it allows for the widespread collection of user data beyond what is necessary for the purposes of delivery of the service. Moreover, it grants the government unchecked power to make up the rules requiring the collection users' personal data. We further note that the mandatory creation and maintenance by telecommunications operators of a user database under Article 203 is unnecessary. Telecommunication operators would normally create a client database. It is unclear why such a database should be mandated by law.

Recommendations:

- Article 187 and 195 should be amended so that reference to the 'requirements of public security and national defence" is removed. In the alternative, these requirements should be clarified in the draft Code or in other legislation and be brought in line with international standards on freedom of expression and privacy;

- Article 194 should be deleted. In the alternative, the purpose and scope of application of Article 194 should be clarified and brought in line with international standards in this area. Codes of Conduct entrenching unduly restrictive content rules online should not be applicable to online social media platforms;

- Article 202 should be amended to bring it line with international standards on privacy and freedom of expression. In particular, references to the Minister deciding the rules of collection of user data should be deleted;

- Article 203 should be deleted.

Chapter 4 – Liability of intermediaries

At the outset, ARTICLE 19 notes that Article 207 appears to reproduce the definition of online platform service operators already outlined in Article 3. In our view, this is confusing. Definitions should be set out at the beginning of the Draft Code and used consistently thereafter. We would recommend removing Article 207.

ARTICLE 19 otherwise generally welcomes the liability provisions in the Draft Code (Articles 204-206). These appear to be largely drawn from the conditional liability model under EU law. In particular, we note that:

- Article 204 provides that an intermediary is immune from liability as a 'mere conduit' unless it initiates the transmission, it selects the receiver of the transmission, it actively selects or modifies the content being transmitted;

- Article 205 provides a natural or legal person hosting content or providing navigation tools is not responsible for that content unless it has failed to remove or restrict access to it upon notification of its illegality;

- Article 206 makes clear that natural or legal persons engaging in the transmission of communications as 'mere conduit/ or 'host' are not subject to a general monitoring obligation.

In addition, we note that under Article 208, hosting providers have a duty of loyalty towards their users so that they must provide fair, clear and transparent information about the criteria they use for labelling, promoting or demoting content, as well as any contractual relationships that would affect the ranking or publication of content.

While these are all generally positive features of intermediary liability laws, we note that Article 205 could be improved in the following ways:

- Reference should be made to obtaining 'actual knowledge' of illegality.

- In addition, it should be made clear that such knowledge can only be obtained by a court order. In other words, the only valid form of notification of illegality should be a court order.

- A potential alternative would beto set out a clear notice-and-notice procedure but only for content involving private disputes (or that should be private such as copyright infringement, privacy or defamation claims).

- For criminal content, an order of a court should be sought with allowance being made for exceptional circumstances where law enforcement may have the power to order the removal of content when e.g. someone's life is at risk. In all cases, such an order should be confirmed by a court within a short period of time, e.g. 48 hours.

Our proposal for a notice and action system are set out in more detail in ARTICLE 19 policy in intermediary liability[33] and the Manila Principles on Intermediary liability[34] and should be used for guidance. In our view, this is very important in order to prevent legal uncertainty as to how knowledge of illegality is obtained and in order to protect freedom of expression from spurious claims made by private parties with little evidence that content is unlawful. It is also very important in order for allegations of illegality to be decided by the court.

Recommendations:

- Article 205 should be amended to be brought in line with the Manila Principles on Intermediary Liability. In particular, Article 205 should clarify that hosts and other similar intermediaries must obtain 'actual' knowledge of illegality and such knowledge should be obtained by a court order;
- Notice-and-notice procedures could be considered for private disputes.

Chapter 6 – Offences

ARTICLE 19 believes that the offences set out in Articles 250 and 251 of the Draft Code are in breach of international standards on freedom of expression:

- Article 250 criminalises whoever intentionally offends others or disturbs their comfort through public electronic communications networks. In our view, this offence is drafted in overly broad and subjective terms, such as 'offend', 'disturb' or 'comfort'. Whilst the need to prove intent is welcome, it is insufficient. Offense or disturbance of someone's comfort are highly subjective concepts. It could also be used to crackdown on journalists who 'intentionally' ask probing questions to politicians who may feel that their 'comfort' is

[33] ARTICLE 19, Intermediaries: Dilemma of Liability, 2013.
[34] Manila Principles on Intermediary Liability, March 2015.

'disturbed'. We also note that similar provisions, contained in the current Code of Telecommunications is frequently used to prosecute bloggers and users of social media.

- Article 251 criminalises, among other things, whoever uses, makes, imports, exports or acquires for sale or free distribution encryption software or services without observing legislative and regulatory provisions related to encryption. In our view, this is problematic as individuals should be free to use encryption services available to them on the Internet. To begin with, encryption services should not be required to comply with government prescriptions as to what good encryption might look like. In our experience, governments frequently try to bypass encryption in ways which undermine information security of all Internet users. As such, they should not be making prescriptions about encryption standards and equally, they should not criminalise those who use different, potentially better, encryption standards. In our view, Article 215 is both unnecessary and disproportionate. As such, it should be deleted.

Recommendations:

- Articles 250 and 251 should be deleted in their entirety.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, freedom of expression and equality, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org.

For more information about the ARTICLE 19's work in Tunisia, please contact, Saloua Ghazouani Oualesti, Regional Director for Tunisia and MENA of ARTICLE 19, at saloua@article19.org.