Tunisia: Decree-law No 54 of 2022

January 2023

Legal analysis

Executive summary

This legal analysis reviews the Decree-law No. 2022-54 of 13 September 2022[1] (the Decree-law) for its compliance with international human rights and freedom of expression standards.

At present, there is no international standard on cybercrime, although efforts at the UN level to create a new international treaty on cybercrime are underway. However, when reviewing the Decree-law, its provisions are compared with those in the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) – the most relevant regional standard on cybercrime. Where useful, references are made to comparative domestic legislation.

While some of the provisions in the Decree-law appear to have been drawn partially from the Cybercrime Convention, most fail to meet international human rights standards (and violate the human rights protections in the Tunisian constitution), lack basic due process protections, and do not respect the principles of necessity and proportionality:

- **The Decree-law is incompatible with the principle of legal predictability.** Most of the offences in the Decree-law provide for prison sentences. The principle of legal predictability requires that sentences which can amount to imprisonment be regulated in the Criminal Code itself. Those subject to the law need to be able to regulate their conduct with certainty, which requires that they find any criminal provisions imposing prison penalties with ease.

- **Many of the offences in the Decree-law are already criminalised in other legal texts.** Crimes included in the Decree-law such as defamation, the dissemination of child sexual abuse material, or hate speech are already criminalised in other legal texts, namely the Criminal Code, Decree-law No. 115 of 2011 on Freedom of the Press, Printing and Publishing (the Decree-law No. 115) or the Telecommunications Code, with different penalties applicable to what are effectively the same offences. This is incompatible with legal certainty requirements and increases the possibility of arbitrary application of these provisions.

- **Several provisions criminalise protected online speech rather than cybercrime.** The Decree-law contains provisions such as the prohibition of the dissemination of false news that are not in line with international freedom of expression standards. For a number of offences, it is likely that the Decree-law could be used to prosecute journalists, human rights defenders, critics of government, and security researchers. Many of the provisions contain vague and broad wording which increases the likelihood of their arbitrary application. From a comparative perspective, the Decree-law introduces several offences that do not exist in instruments like the Cybercrime

[1] Decree Law No. 2022-54 of 13 September 2022 on combating offences relating to information and communication systems (*Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication*).

Convention. The offences in the Decree-law therefore go beyond those offences that are internationally recognised to constitute cybercrimes.

- **The penalties in the Decree-law are excessive and disproportionate.** The sentencing regime in the Decree-law is excessively harsh, including for content-based offences. International human rights law only allows for the sanction of imprisonment to be prescribed for the worst speech offences, such as incitement to genocide.

- **The Decree-law grants Tunisian authorities far-reaching investigatory powers and lacks procedural safeguards for human rights protections.** The Decree-law mandates general and indiscriminate data retention by telecommunication service providers and introduces overly broad data access and interception powers of government authorities. Procedural safeguards and human rights protections, such as a right to be notified of surveillance measures and a right to appeal, are markedly absent throughout the Decree-law, despite a general reference to human rights commitments in its Article 2.

Table of contents

Introduction **5**
International human rights standards **6**
The protection of freedom of expression under international law 6
Limitations on the right to freedom of expression 7
Prohibiting incitement to discrimination, hostility or violence 7
Online content regulation 8
Surveillance of communications 8
Anonymity and encryption 10
Cybercrime 11
Analysis of the Decree-law **13**
Nature of the Decree-law 13
Definitions 13
Content-based offences 14
Dissemination of false Information 14
Defamation, incitement to aggression and incitement to hate speech 16
Expression targeting public officials 18
Child exploitation and physical aggression 19
Copyright offences 19
Other cybercrime offenses 20
Illegal access 20
Misuse of devices 21
Illegal interception and data interference 21
System interference and misuse of data 22
Computer-related fraud and forgery 22
Procedures and investigations 22
Mandatory data retention and access to data by law enforcement 23
Interception of communication 24
Inadequate protection of journalistic sources 25
Penalties for failure to comply with obligations for the collection of electronic evidence 25
Extraterritorial jurisdiction and international cooperation 26

Introduction

The stated purpose of the Decree-law is to "to lay down provisions aimed at preventing and punishing offences relating to information and communication systems, as well as those relating to the collection of related electronic evidence, and to support international efforts in this field, within the framework of international, regional and bilateral agreements ratified by the Tunisian Republic."[2]

The Decree-law appeared for the first time in 2015 in a leaked version, sparking widespread opposition within Tunisian civil society. [3] Despite this opposition, the Tunisian Government approved the draft on 1 June 2018. However, for reasons that are not public, the text was not transferred to the Assembly of the Representatives of the People.

The Decree-law incorporates the majority of the provisions of the 2018 version of the text, while adding new criminal offences.

Following the elections in December 2022 and January 2023, the Decree-law will be subject to approval by the newly constituted Assembly of the Representatives of the People.[4]

[2] See Article 1 of the Decree-law.

[3] See Projet de loi relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication. See also Committee to Protect Journalists, En Tunisie, la liberté de la presse s'érode sur fond de craintes pour la sécurité, 27 octobre 2015

[4] See Article 80 of the Tunisian Constitution.

International human rights standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of legally binding international human rights instruments; in particular, Article 19 of the **Universal Declaration of Human Rights (UDHR)**[5] and Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).[6] Freedom of expression is further protected under Article 37 of the Tunisian Constitution. In addition, Article 38 of the Tunisian Constitution guarantees the right to information and access to information.

General Comment No 34,[7] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of dissemination, including all forms of electronic and internet-based modes of expression.[8] In other words, the protection of freedom of expression applies online in the same way as it applies offline. States Parties to the ICCPR are also required to consider the extent to which developments in information technology, such as internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[9] The legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[10]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the internet.[11] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

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 of the ICCPR as interpreted by the HR Committee and that they are in line with the special mandates' recommendations.

[5] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[6] UN General Assembly Resolution 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[7] UN Human Rights Committee (HR Committee), General comment No. 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34.
[8] *Ibid*, para 12.
[9] *Ibid*, para 17.
[10] *Ibid*, para 39.
[11] Joint Declaration on Freedom of Expression and the Internet, June 2011.

Limitations on the right to freedom of expression

The right to freedom of expression is not guaranteed in absolute terms, but restrictions on the right to freedom of expression and the right to information must be strictly and narrowly tailored and may not put the right itself in jeopardy. Determining whether a restriction is justified is often articulated as a three-part test under Article 19(3) of the ICCPR. Restrictions must:

- **Be prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate their conduct accordingly.[12] Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible;

- **Pursue a legitimate aim:** exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals;

- **Be necessary and proportionate:** necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[13]

The same principles apply to electronic forms of communication or expression disseminated over the internet.[14]

Article 55 of the Tunisian Constitution also provides that restrictions on freedom of expression must meet the test of legality, legitimacy, necessity, and proportionality.

Prohibiting incitement to discrimination, hostility or violence

It is also important to note that 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. At the same time, inciting violence is more than just expressing views that people disapprove of or find offensive.[15] It is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At the international level, the UN has developed the Rabat Plan of Action, an inter-regional multi-stakeholder process involving UN human rights bodies, NGOs and academia - which provides the closest definition of what constitutes incitement law under Article 20(2) ICCPR.[16]

[12] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[13] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[14] General Comment 34, *op.cit.*, para 43.
[15] *C.f.* European Court of Human Rights, *Handyside v the UK*, 6 July 1976, para. 56.
[16] See UN Rabat Plan of Action (2012). In particular, it clarifies that regard should be had to six part test in assessing whether speech should be criminalised by states as incitement.

Online content regulation

The above principles have been endorsed and further explained by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FoE) in two reports in 2011.[17]

The Special Rapporteur clarified the scope of legitimate restrictions on different types of expression online.[18] He also 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.[19]

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:

- child pornography[20];
- direct and public incitement to commit genocide;
- hate speech; and
- incitement to terrorism.

He further made clear that even legislation criminalising 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.[21] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child sexual abuse material on the internet through the use of blocking and filtering technologies is not immune from those requirements.

Surveillance of communications

[17] Reports of the UN Special Rapporteur on Freedom of Expression, A/HRC/17/27, 17 May 2011 and A/66/290, 10 August 2011.
[18] *Ibid*, para 18.
[19] *Ibid.*
[20] It is recommended to use the term "child sexual abuse images" to reflect the non-consensual and illegal nature of the content. Terminology such as "child pornography" is no longer acceptable since children cannot consent to their own abuse.
[21] *Ibid*, para 22.

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[22] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR that states, *inter alia*, that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, or correspondence. In **General Comment no. 16** on the right to privacy,[23] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims, and objectives the ICCPR. It further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[24]

The UN Special Rapporteur on the 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:

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[25]

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[26]

The Special Rapporteur on FoE has also observed that:

---

[22] *Ibid*, para 84.
[23] HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[24] *Ibid.*, para 8.
[25] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37, 28 December 2009, para 17.
[26] *Ibid.*, para 21.

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[27]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental feature enabling anonymity online is encryption.[28] Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FoE, published his report on encryption and anonymity in the digital age.[29] The report highlighted the following issues in particular:

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[30]

- Anonymous speech is necessary for human rights defenders, journalists, and protestors. He noted that any attempt to ban or intercept anonymous communications during protests was an unjustified restriction to the right to freedom of peaceful assembly under the UDHR and the ICCPR.[31] Legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications;

[27] Report of the Special Rapporteur on FoE, A17/27, 17 May 2011, para 59.
[28] Encryption is a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation; see e.g. SANS Institute, History of encryption, 2001.
[29] Report of the Special Rapporteur on FoE, A/HRC/29/32, 22 May 2015.
[30] *Ibid,* paras 12, 16 and 56.
[31] *Ibid,* para 53.

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[32] Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction.[33]

The May 2015 report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online".[34] The report stipulated that such orders should be:

- based on publicly accessible law;
- clearly limited in scope focused on a specific target;
- implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not available.[35]

Cybercrime

No international standard on cybercrime exists, although efforts at the UN level to create a new international treaty on cybercrime are underway. In December 2019, the UN General Assembly adopted a resolution on "countering the use of information and communications technologies for criminal purposes" and introducing an Ad Hoc Committee. The committee was announced to elaborate a comprehensive international convention.

Of the existing regional standards, the Cybercrime Convention of the Council of Europe has been the most relevant to analyse new cybercrime legislations.[36] Although Tunisia is not party to the Cybercrime Convention, the latter provides a helpful reference point against which to analyse Decree-Law 54.

The Cybercrime Convention provides definitions for relevant terms, including definitions for computer data, computer systems, traffic data, and service providers. It requires States Parties to create offences against the confidentiality, integrity, and availability of computer systems and computer data; computer-related offences including forgery and fraud; one content-related offence - the criminalisation of "child pornography"; and offences related to infringements of copyright and related rights. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes,

[32] *Ibid,* para 56.
[33] *Ibid,* paras 31-35.
[34] *Ibid*, para 45.
[35] *Ibid*.
[36] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004.

including preservation orders, production orders, and the search and seizure of computer data.

Finally, and importantly, the Cybercrime Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

Analysis of the Decree-law

The interim character of the Decree-law

The Decree-law, as a secondary legislation issued by the President (who is part of the executive branch of the Tunisian government) is envisioned as an interim regulation – as mentioned in the introduction, following the election in December 2022 and January 2023, the Decree-law will be subject to approval by the newly constituted Assembly of the Representatives of the People. International human rights law requires that restrictions of the nature contained in the Decree-law should be established by Parliament, not by the executive government. Only Parliaments have the legitimate power to regulate issues concerning human rights as the latter are designed to protect individuals from the government itself. It is the role of the executive government to regulate matters concerning public administration, yet the subject matter regulated by the measures in the Decree-law relate not to public administration but to criminal matters as well as to human rights and freedom of expression. Insofar as the purpose of the adoption of an interim regulation under the emergency regime is to provide a framework for the operation of the law enforcement authorities in the interim period, international law requires that the scope of application of such a provisional regulation should be limited to this aspect only.

As such, only issues that need immediate regulation should be addressed in secondary legislation.

The principle of legal predictability

The Decree-law is incompatible with the principle of legal predictability. Most of the offences in the Decree-law provide for prison sentences. The principle of legal predictability requires that sentences which can amount to imprisonment be regulated in the Criminal Code itself. Those subject to the law need to be able to regulate their conduct with certainty, which requires that they find any criminal provisions imposing prison penalties with ease.

In addition, many of the offences in the Decree-law are already criminalised in other legal texts. Crimes included in the Decree-law such as defamation, the dissemination of child sexual abuse material, or hate speech are already criminalised in other legal texts, namely the Criminal Code, Decree-law No. 115 of 2011 or the Telecommunications Code, with different penalties applicable to what are effectively the same offences. This is incompatible with legal certainty requirements and increases the possibility of arbitrary application of these provisions.

Definitions

Article 5 of the Decree-law defines a number of terms used throughout the Decree-law. The definitions of computer system, computer data, and traffic data are broadly consistent with

the definitions contained in the Cybercrime Convention.

However, the definition of "service providers" departs from the scope of Article 1 of the Cybercrime Convention.[37] Service provider under the Decree-law is defined as "any natural or legal person providing a telecommunication service to the public, including internet services". The inclusion of natural persons in the definition means that they also may be subject to the mandatory data retention under Article 6 of the Decree-law which may be impossible in practice for them to adhere to.

At the same time, the definition appears to be narrower than under Article 1 of the Cybercrime Convention. The latter encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems. The definition under the Cybercrime Convention also extends to those entities that store or otherwise process data on behalf of such communication service or users of such service. As specified in the commentary to the Cybercrime Convention, a service provider under Article 1 therefore includes services that provide hosting services (such as those provided by social media platforms), caching services, and services that provide a connection to a network.[38]

The Decree-law, on the other hand, appears to be limited to companies operating at the infrastructure level. However, it is not clear whether the notion of "*services d'internet*" also covers communication service providers and whether they are thus covered by the data retention obligation under Article 6 of the Decree-law.

Content-based offences

The Decree-law contains a number of content-based offences, namely in Article 24 (regarding the dissemination of false information) and Article 26 (regarding child exploitation and corporal aggression).

Article 24 is a highly complex article which itself contains several content-based offences. These will be discussed in turn.

Dissemination of false Information

As explained earlier, any interference with freedom of expression must meet three criteria under international human rights standards, namely (i) to be prescribed by law; (ii) to pursue a legitimate aim; and (iii) to be necessary in a democratic society and proportionate to the legitimate aim pursued.

Article 24(1) of the Decree-law contains several terms, such as "false news", "false

[37] Cybercrime Convention, *op.cit.* Under Article 1(c), "service provider" means: i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

[38] Commentary to the Cybercrime Convention, para. 27.

information", "rumours", which are very broad, vague, and open to different interpretations. To meet the legality requirement, definitions in criminal laws should provide as much clarity as possible by elaborating in detail exactly what is prohibited. The terms at issue, however, do not have an agreed definition in international or regional human rights law and it is questionable whether it is possible to define such concepts with a level of precision that would meet the requirements of legal certainty. This is coupled with the complexity of distinguishing between fact and opinion. It is also notable that the spreading of "rumour" – without such rumour having to be demonstrably false – can be sufficient to constitute a breach of Article 24. Similarly, "infringing on the rights of others" is a very broad concept and does not meet the legal certainty standards required, in particular for a criminal provision.

Beyond issues of legal clarity, the phrase "with the aim of infringing on the rights of others, harming public security or national defense, or spreading terror among the population" does not meet the criteria under international freedom of expression standards. Restrictions on freedom of expression on the basis of a mere falsity or a misleading nature of certain information will not meet the requirements of legitimate interest (which are listed in Article 19 ICCPR as respect of the rights or reputations of others; the protection of national security or of public order, or of public health or morals). Any restrictions will only be permissible when demonstrably connected to a particular legitimate aim. In addition, laws may only restrict material which can be shown to be harmful. However, Article 24(1) does not require any actual harm or even a concrete risk of harm to public order or national security or that the message did indeed spread terror among the population. Indeed, the commission of the crime is complete based on only the intention of the speaker –although the element of intent tends to be one of the most difficult to demonstrate in criminal proceedings. At the same time, the use of terms like "promote" suggest that a mere "like" on a social media platform may be sufficient to fall within the scope of Article 24(1).

The lack of legal clarity and the absence of a legitimate aim in Article 24(1) is exacerbated by the fact that it imposes severe penalties, namely imprisonment for five years and a fine of 50,000 dinars (the equivalent of approximately USD 17,000). The prescribed punishment is excessively harsh and disproportionate. It is generally recognised that the principle of proportionality mandates that criminalization of speech always be an exceptional and last resort and that restrictions on the right to freedom of expression "must be the least intrusive instrument amongst those which might achieve their protective function".[39] Specifically referring to the issue of disinformation, the Special Rapporteur on FoE observed that "[c]riminal law should be used only in very exceptional and most egregious circumstances of incitement to violence, hatred or discrimination"[40] – these sort of offences are, however, not the subject of Article 24(1).

There is an evident inherent risk in empowering government authorities to decide what the truth is, and experience shows that legislation on disinformation is often abused to silence dissent or critical voices in society.[41] There is also a significant risk that due to the broad

[39] See General Comment No. 34, *op. cit.*, para 34.
[40] *Ibid.*
[41] UN Special Rapporteur report on disinformation, para 55.

nature of Article 24(1), it will be used against journalists, political opponents, and human rights defenders in Tunisia.

To provide a comparative perspective, while the Cybercrime Convention contains one content-related offence, namely child pornography (as will be discussed in the context of Article 26 of the Decree-law), it does not require the criminalisation of disinformation, false news or similar concepts. While many regulators have passed laws to deal with disinformation this does not always mean that disinformation is criminalised. For example, in the European Union, the Digital Services Act requires very large online platforms and search engines to assess and mitigate the risks arising from their services, including the dissemination and amplification of disinformation.[42] Where countries have actually criminalised the spreading of false news or disinformation (the most recent example being the provision on "false or misleading information" that was introduced in the Turkish Penal Code), this has been widely criticised by human rights organisations as being incompatible with free speech principles and human rights online.[43]

Defamation, incitement to aggression and incitement to hate speech

Article 24(2) of Decree-law No. 54 suffers from many of the same shortcomings as its paragraph 1, in particular a lack of clarity.

For example, Article 24(2) contains very different actions such as "disseminating false news" or "disseminating information containing personal data" and then combines those acts with concepts as varied as defamation, incitement to aggression, or incitement to hate speech. This makes it extremely hard for individuals to predict which actions exactly are criminalised. This is further exacerbated by the fact that, like in paragraph 1, the aim or intention of defaming others to damage their reputation or discredit or harm them materially or morally is sufficient to constitute a crime, without any evidence of a specific action being likely to cause any actual harm.

In addition, while Article 24(1) makes reference to the usage of information and communication networks and systems (*systèmes et réseaux d'information et de communication*), Article 24(2) only makes reference to the usage of information systems (*systèmes d'information*). It is, however, unclear whether this distinction is intentional and if so, how it is supposed the impact the scope of application of the respective paragraphs.

<u>Criminal defamation</u>

Criminal defamation laws are generally recognised to be incompatible with international

[42] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[43] See Venice Commission (European Commission for Democracy through law), Urgent joint opinion of the Venice Commission and the Directorate General of Human rights and Rule of Law (DGI) of the Council of Europe on the Draft Amendments to the penal code regarding the provision on "false or misleading information", Opinion no. 1102 / 2022.

standards on freedom of expression.[44] The HR Committee has similarly urged all States Parties to the ICCPR to abolish criminal defamation laws, reflective of an international consensus among international organisations.[45] This is because it is considered that such laws rarely can be said to pursue a legitimate aim and be necessary and proportionate. The HR Committee has further held that "in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty".[46] Article 24(2), which requires imprisonment for defamation is therefore in clear breach of international freedom of expression standards.

It is also unclear to what extent the defamation offence can be distinguished from the offence to spread a message with the aim of "damag[ing] the reputation [of others], discrediting or harming them materially or morally".

In addition, this provision is now added to what is already a significant list of criminal provisions that have been applied by Tunisian authorities when prosecuting defamation and similar speech-related offences (including Article 86 of the Telecommunications Code, Articles 55 and 56 of the Decree-Law No. 115 of 2011, or several provisions of the Tunisian Criminal Code).

Incitement to aggression

There is a risk that the reference to "incitement to aggression" could be abused to criminalise any critical coverage of public figures or politicians considered to making the latter potential targets for attacks.

Also, it is not clear how these provisions relate to other prohibitions on incitement, such as those in Article 32 of the Tunisian Criminal Code or Articles 50 and 51 of the Decree-Law No. 115 of 2011.

Incitement to hate speech

Article 24 further criminalises the "incitement to hate speech".

There is no uniform definition of 'hate speech' under international human rights law. International law requires that States prohibit the most severe forms of hate speech. For instance Article 20(2) of the ICCPR requires States to prohibit advocacy of discriminatory hatred that constitutes incitement to discrimination, hostility, or violence.[47] To provide clarity on the application of these provisions, the UN Rabat Plan of Action outlines a six-part threshold test to assess whether a certain expression reaches the level of severity under Article 20(2) of the ICCPR. These include taking into account social and political context, the status of the speaker, intent to incite the audience against a target group, content and form

[44] ARTICLE 19, Defining Defamation: Principles on Freedom of Expression and Protection of Reputation, 2017.
[45] General Comment 34, *op.cit.*, para 47. HR Committee, Concluding observations on Italy, CCPR/C/ITA/CO/5; Concluding observations on the Former Yugoslav Republic of Macedonia, CCPR/C/MKD/CO/2.
[46] General Comment 34, *op.cit.*, para 47.
[47] See Article 20(2) of the ICCPR.

of the speech, extent of dissemination, and likelihood of harm, including imminence. The Rabat Plan holds that *all six* of these factors should be fulfilled in order for a statement to amount to a criminal offense.[48]

The main issue with the prohibition of the incitement to hate speech in the Decree-law is that a wide range of expression could potentially be criminalised as no definition is provided of what hate speech signifies precisely. It is also notable that the law does not criminalise hate speech but "incitement to hate speech", which – if the meaning can in any manner be considered to be in line with ICCPR – essentially means that it seeks to criminalise incitement to incitement. This may be a drafting error but it goes further to show the lack of legal clarity. In addition to that, Article 52 of Decree-law No. 115 of 2011 and Law No. 2018-50[49] already criminalise certain forms of hate speech; additional legislation increases the risk of arbitrary application of these legal provisions by the prosecuting authorities in an individual case.

Expression targeting public officials

Article 24(3) provides that the penalties prescribed shall be doubled if the targeted person is a public official or similar. This provision increases the risk that Article 24 will be used to silence criticism and political dissent and is incompatible with international freedom of expression standards which are particularly protective of political speech. In particular, the Human Rights Committee observed in its General Comment No. 34 that "in circumstances of public debate concerning public figures in the political domain and public institutions, the value placed by the Covenant upon uninhibited expression is particularly high". It stressed further that speech-related offences "should not provide for more severe penalties solely on the basis of the identity of the person that may have been impugned".[50]

It is also a well-established principle under international human rights law that political speech requires enhanced protection and that politicians and public officials are subject to wider limits of criticism than private individuals. Indeed, international human rights courts have consistently held that public officials should tolerate more, not less, criticism than ordinary citizens.[51] By choosing a profession involving public responsibilities, officials knowingly open themselves to scrutiny of their words and deeds by the media and the public at large.[52] However, Article 24(3) inverts the fundamental democratic principle that the government is subject to public scrutiny.

[48] See also ARTICLE 19, 'Hate Speech' Explained, A Toolkit, 2015.

[49] Organic Law No. 2018-50 of 23 October 2018, on the elimination of all forms of racial discrimination (*Loi organique n° 2018-50 du 23 octobre 2018, relative à l'élimination de toutes les formes de discrimination raciale*).

[50] See General Comment No. 34, *op.cit.*, para 38.

[51] See, among many other authorities, European Court of Human Rights, *Thoma v Luxembourg*, App. no. 38432/97, para 47; *Lingens v Austria*, App. no. 9815/82, para 42.

[52] European Court of Human Rights, *Bodrozoc and Vujin* v. Serbia, App. 38435/05, para 34.

Child exploitation and physical aggression

Article 26(1) contains offences related to "child pornography."

Child sexual abuse images are a type of expression that States are required to prohibit under international law. Tunisia ratified the Optional Protocol to the Convention on the Rights of the Child (CRC) on the sale of children, child prostitution, and child pornography in 2002.[53] Article 9 of the Cybercrime Convention also requires States Parties to criminalise various aspects of the electronic production, possession, and distribution of child pornography.

It is important to note that Article 60 of Decree-Law No. 115 of 2011 already criminalises the dissemination of child sexual abuse material, albeit with a lower penalty (1-3 years as opposed to 6 years under Article 26(2) of the Decree-Law 54). Therefore, once again, there could be several charges applied for the same conduct and it is unclear which provision would take priority in a concrete case.

Article 26(2) criminalises the publication or diffusion of images or videos of physical or sexual aggression. The provision does not contain an exception for reporting that serves to inform the public. It could therefore criminalise publishing evidence of human rights violations or general reporting on crimes. While other jurisdictions, for example France and Germany, similarly prohibit the dissemination of violent images, they do contain such exceptions. For example, Article 222-33-3 of the French Penal code which criminalises "recording and broadcasting of images of violence" (*l'enregistrement et de la diffusion d'images de violence*) states that "this article shall not apply where the recording or broadcasting results from the normal exercise of a profession whose purpose is to inform the public or is made in order to serve as evidence in court."[54]

Copyright offences

Article 25 of the Decree-law criminalises the intentional use of information and communication systems to violate copyright and related rights without obtaining an authorisation from the rightful owner(s) with the aim to make a profit or to damage the financial interests or rights of others. The penalty may be a fine or prison between one month and one year.

Copyright offences are also included in the Cybercrime Convention. In particular, Article 10 of the Cybercrime Convention requires State Parties to criminalise copyright infringement and related rights pursuant to a number of existing international instruments, with Parties able to reserve the right not to impose criminal liability if other remedies are available.

[53] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, resolution A/RES/54/263 at the 54th session of the UN General Assembly, 25 May 2000, Article 3(1)(c).
[54] See similarly Article 131(2) of the German Criminal Code.

There are two main issues with Article 25. First, offences for copyright infringement may only be compatible with the right to freedom of expression and information if they have a clear legal basis, each element of the offence is clearly defined and the range of sentences available is proportionate to the seriousness of the offence. Article 25 lacks such level of detail, given that it does not describe in sufficient detail the sort of conduct it criminalises (e.g. publishing a protected work; modifying a work; using a work under a false designation or a designation that differs from that decided by the author, etc.).

Second, Article 25 criminalises the intentional use of information and communication systems to violate copyright "*with the aim of infringing on the "financial interests or rights of others"*. Many copyright infringements – even if of a non-commercial nature - could arguably be considered to fulfil this requirement. However, international freedom of expression standards require that (i) law enforcement authorities should not initiate prosecutions in non-commercial copyright infringement cases due to a lack of public interest; and (ii) prison sentences and other harsh penalties should never be available as a sanction for non-commercial copyright infringement.[55]

In addition, Law 94-36[56] already sanctions copyright infringements, but in a much more detailed way. The relationship between Article 25 of the Decree-Law and Law 94-36 is not clear. There is again a risk that the authorities apply these provisions arbitrarily in an individual case.

Other cybercrime offenses

The Decree-law also contains a number of offences against the confidentiality, integrity, and availability of computer data and systems as well as computer-related fraud and forgery.

Illegal access

Article 16 of the Decree-law criminalises accessing or remaining in a computer system illegally. It generally reflects the provision in Article 2 of the Cybercrime Convention. It is, however, generally acknowledged that the use of the term "without right" instead of "illegal" is more protective of freedom of expression, as the former also excludes from criminal liability conduct that may be justified. This may be the case not only in cases where classic legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. As the Commentary to the Cybercrime Convention observes, "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised".[57]

[55] ARTICLE 19, The Right to Share – Principles on Freedom of Expression and Copyright in the Digital Age, 2013.
[56] Law No. 94-36 of 24 February 1994 on literary and artistic property, as amended and completed by Law No. 2009-33 of 23 June 2009 (*Loi n° 94-36 du 24 février 1994 relative à la propriété littéraire et artistique, telle que modifiée et complétée par la loi ° 2009-33 du 23 juin 2009*).
[57] Commentary to the Cybercrima Convention, para. 38.

In addition, Article 2 of the Cybercrime Convention suggests certain additional elements that increase the protective level of illegal access provisions, for instance for access measures to be circumvented or for dishonest intent in obtaining data.

Misuse of devices

Article 17 of the Decree-law punishes anyone who sells or disseminates, intentionally and illegally, devices or programs that are designed or adapted to commit offences under the Decree-law as well as computer passwords, access codes, or similar data by which the whole or any part of a computer system is capable of being accessed to commit offences under the Decree-law.

Article 17 excludes liability where the conduct is required for scientific research or information security. This offers important protection as technologies can be dual-use and it is in the nature of technology that it can be used both for legitimate and illegitimate purposes. Most companies would know that the software they manufacture or sell could be used for dual purposes, including for the purposes of unauthorised access to computer data and systems. A standard of intent, particularly a heightened standard, is required; otherwise the provision could punish legitimate activities such as security testing.

Without adequate safeguards, provisions proscribing dual-use technologies may be used to prosecute individuals or companies producing, distributing, selling, or otherwise circulating software used to break Digital Management Rights systems. DRM systems are a type of technology principally used by hardware manufacturers, publishers and copyright holders to control how digital content may be used after sale. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising in perpetuity absolute control over the sharing of information is strongly contested. For example, DRM systems prevent individuals from engaging in trivial and non-commercial acts of copyright infringement such as transferring data between their own electronic devices; they can also prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of “fair use”.

While the wording of Article 17 of the Decree-law thus offers some protection, the provision does not specify that it does not impose criminal liability where the device or program is not sold or disseminated for the purpose of committing one of the offenses under the Decree-law against the confidentiality, integrity, and availability of computer data and systems, and is therefore not completely in line with the wording of Article 6(2) of the Cybercrime Convention. In addition, Article 17 require that the incriminated conduct be “illegal” instead of “without right”.

Illegal interception and data interference

Article 18 of the Decree-law punishes intentional interception without right. The provision largely mirrors Article 3 of the Cybercrime Convention.

Article 19 of the Decree-law for its part punishes the damaging, alteration, suppression, deletion, or destruction of computer data without right and also criminalises the attempt to do so. Article 19 does not require that such data interference be committed intentionally and "without right". In addition, Article 19 does not require that the data interference result in serious harm, in line with Article 4 paragraph 2 of the Cybercrime Convention.

System interference and misuse of data

Article 20 of the Decree-law punishes the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. While the provision mirrors Article 5 of the Cybercrime Convention, it leaves out an important requirement, namely that the conduct be "without right".

Article 21 of the Decree-law further punishes a person deliberately misusing computer data belonging to others. This offense is not contained in the Cybercrime Convention. It is yet another provision that is incompatible with international freedom of expression standards, due to the severe penalty it imposes (5 years imprisonment and a fine) and due to its broad and ambiguous wording. It is unclear what specifically misusing computer data may mean, in particular in the absence of any harm required, and there is a risk that it could be applied to the work of investigative journalists. The provision further does not require that the conduct be "without right".

Computer-related fraud and forgery

Articles 22 and 23 of the Decree-law punish computer-related fraud and forgery, respectively. These definitions generally track the definitions contained in the Cybercrime Convention. However, they do not require the incriminated conduct to be done "without right" and with "fraudulent" or "dishonest" intent.

Procedures and investigations

It is generally recognised that the nature of certain cybercrimes may require special investigative tools and international cooperation to be adequately addressed, which is why provisions addressing these aspects feature in the Cybercrime Convention. Articles 6 to 15 of the Decree-law (Chapter II) comprise procedural provisions and set out the investigatory powers given to Tunisian authorities to investigate the crimes that are included in the Decree-law.

While some of these provisions bear certain similarities with Section 2 of the Cybercrime Convention (addressing procedural law), many of them do not contain due process and human rights guarantees. For instance, the Decree-law does not contain a key feature of the Cybercrime Convention: the acknowledgment of the necessity for safeguards and oversight. The Cybercrime Convention in its Article 15 explicitly requires signatories to "ensure that the

establishment, implementation and application of powers and procedures" are "subject to conditions and safeguards" which "shall provide for the adequate protection of human rights and liberties," naming the ICCPR among other instruments. Further, the Cybercrime Convention requires, in Article 15(2), "judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure".

Despite a general reference to international law and constitutional guarantees in Article 2 of the Decree-law, the investigatory powers conferred to Tunisian authorities by the Decree-law are much too broad and intrusive. This is aggravated by the fact that the offences included in the Decree-law are not limited to those in the Cybercrime Convention but also criminalise certain forms of online speech in a way that falls short of international freedom of expression standards.

Mandatory data retention and access to data by law enforcement

Article 6 of Decree-law obliges providers of telecommunication services to retain, generally and indiscriminately, data stored in an information system for at least two years – and potentially longer, subject to a joint decision by the Minister of national defense, Minister of the interior, Minister of justice and Minister in charge of telecommunication. The persons whose data are retained do not need to be, even indirectly, in a situation which is liable to give rise to criminal prosecutions.

The data that needs to be stored includes data about user identity, traffic, and location data (electronic communications metadata). It is generally recognised that the analysis of that type of data can allow precise conclusions to be drawn about the individuals involved, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons, and the social environments frequented by them.[58]

The mandatory data retention provided by the Decree-law goes beyond what is required by the Cybercrime Convention, which does in fact not mandate any data collection or retention by a service provider. In its Articles 16 and 17, the Cybercrime Convention only refers to data *preservation*, which needs to be distinguished from data retention. As explained in the Commentary to the Cybercrime Convention, "preservation measures apply to computer data that 'has been stored by means of a computer system', which presupposes that the data already exists, has already been collected and is stored".[59] In addition, any data retention order must be made in the context of specific criminal investigations or proceedings (Article 14 of the Cybercrime Convention).

[58] See, for instance, CJEU judgment of 6 October 2020, La Quadrature du Net and Others, C-511/118, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117.
[59] See Commentary to the Cybercrime Convention, para. 152.

The general and indiscriminate nature of the data retention as required by the Decree-Law can undermine anonymous speech as it facilitates surveillance.[60] To meet the test of constituting a necessary and proportionate interference with the right to privacy and freedom of expression, access to such data by law enforcement authorities needs to be subject to clear and precise rules which provide for sufficient safeguards.[61]

Access to data is governed by Article 9 of the Decree-law, which sets out the following procedural powers for production orders, search and seizure of computer data, and real-time collection of traffic data. Access to data under Article 9 may go beyond access to data retained in compliance with Article 6 of the Decree-law and the orders may address natural and legal persons other than telecommunication providers.

Article 9 does not contain the necessary safeguards to ensure that any interference with the right to privacy and freedom of expression be limited to what is necessary and proportionate. For instance, for traffic and location data that allows precise conclusions to be drawn, law enforcement access should always be confined to cases of serious crime or preventing serious threats to public security[62] - a limitation which does not apply under the Decree-law. Further, no notice needs to be given to the user being investigated after their data being accessed. Thus, it is possible that individuals may never receive notice of their data being subject to search. This will hamper their ability to appeal against the data search and to challenge its admissibility in court, undermining their right to an effective remedy.[63] Finally, the wording of Article 9 concerning the need for judicial authorisation for the different measures are not sufficiently clear.[64]

Interception of communication

Article 10 of the Decree-law allows for the interception of communications of the suspect "if required by the investigation." Ordinarily, interception of communications, which allows authorities to access its content, are only warranted under exceptional circumstances due to their intrusive nature and the significant concerns they raise for the rights to privacy and freedom of expression. Such surveillance must only be conducted on the basis of specific

[60] For the interconnectedness between anonymity and the right to privacy and freedom of expression see UN Human Rights Council (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, A/HRC/29/32, para 16.
[61] See *La Quadrature du Net and Others*, *op.cit.*, para 117.
[62] See CJEU judgement of 2 March 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18.
[63] See A/HRC/29/32, para. 16.
[64] The text states: "The public prosecutor, the investigating judge or officers of the judicial police authorised in writing are empowered to order." "*Le procureur de la République, le juge d'instruction ou les officiers de la police judiciaire autorisés par écrit, sont habilités à ordonner...*". It is unclear why the investigating judge would require written authorisation, just as the public prosecutor and the judicial police officers, which is why a possible reading of this paragraph is that only the police officers require judicial authorisation. While the wording in Article 7 referring to "ordonnances judiciaires" for the measures listed in Article 9 may provide some comfort, that wording for its part appears to contradict the requirements set out for authorisation of interception measures under Article 10 as described just below.

decisions by a state authority with adequate judicial safeguards and respect for the principle of proportionality.

The safeguards provided in the Decree-law are insufficient. For instance, it is unclear whether the interception is subject to mandatory judicial oversight. While the wording of Article 10 itself suggests that the interception can be ordered on the basis of a written and reasoned decision by either the public prosecutor or the investigating judge,[65] Article 7 of the Decree-law only makes reference to "judicial orders" regarding data access and interception. This type of surveillance measure, however, requires that prior judicial authorisation be clearly enshrined in the relevant legislative instrument without any ambiguity in its wording. Additional shortcomings in the Decree-law include the lack of a time limit to the surveillance measure, the lack of requirement that interception only be ordered for serious crimes; [66] the lack of requirement that interception measures only be ordered where less intrusive measures fail to achieve the same result, the lack of requirement to inform the targets of the interception in writing, and the inability to appeal the measure.

Inadequate protection of journalistic sources

Article 19 of the ICCPR also covers the protection of journalistic privilege. In its General Comment No. 34, the Human Rights Committee observed that "States parties should recognize and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose information sources."[67] In addition, Article 11 of Decree-law No. 115 protects the confidentiality of journalistic sources and establishes that journalistic privilege may not be overcome without judicial authorisation and only in strictly defined circumstances.

In addition, the Decree-Law contains no special provisions for the protection of journalistic sources.[68] Particularly investigative journalism, relying heavily on confidential sources, may be jeopardised by indiscriminate data retention, the effectively unlimited access by government authorities to the data collected and the exercise of interception powers in the Decree-law.

Penalties for failure to comply with obligations for the collection of electronic evidence

Articles 27 to 33 of the Decree-law establish a number of penalties for failure to comply with the obligations established under the Decree-law for the collection of electronic evidence,

[65] Certain police officers may also order interceptions of communications based on a written and reasoned decision of either the public prosecutor or the investigating judge ("on the basis of a reasoned report by the judicial police officer authorised to record offences, the interception of suspects' communications may also be carried out, by virtue of a written and reasoned decision by the public prosecutor or the investigating judge").

[66] The interception can be ordered for all crimes contained in the Decree-law, including those that may only give rise to a penalty of three months. See for instance Article 16 of the Decree-law.

[67] General Comment No. 34, *op.cit.*, para 45.

[68] Article 7 of the Decree-law prohibits individuals that are enforcing orders relating to data access and interception measures from breaching professional privilege. However, it is not clear what type of professional privilege is covered by Article 7. In any case, Article 7 does not offer effective protection, since the data retention in itself endangers the protection of journalistic sources.

including failure to comply with the data retention requirement or the knowing obstruction of an investigation. Article 32 establishes the criminal responsibility for legal entities and their directors for the offences in Articles 27 to 31.

These provisions do not contain sufficient guarantees. For instance, Article 27 which criminalises non-compliance with Article 6 of the Decree-law, does not require intent. In addition, the severity of the sanctions established for the different offences, namely imprisonment or the dissolution of a company, is disproportionate and may well be used by Tunisian authorities to exert undue pressure on individuals and legal entities to comply with its orders. Given the incompatibility of many of the criminal offences in the Decree-law with international human rights law, coupled with the broad investigatory powers lacking due process guarantees, it may well be that certain companies would for instance resist disclosure requests with reference to their human rights commitments.

How much pressure the Tunisian government will be able to effectively exercise through these criminal provisions may depend to a large extent on whether the respective entities have local representatives and staff within Tunisian territory. For instance, when it comes to social media companies, Tunisia has not yet established any obligation on them to appoint local representatives. The situation may well be different for telecommunication providers located within Tunisian territory.

Extraterritorial jurisdiction and international cooperation

Article 34 provides that under certain circumstances, Tunisian courts may prosecute and try offences criminalised by the Decree-law even if they were committed outside Tunisian territory. This is the case if:

- The offence is committed by a Tunisian citizen;
- The offence is committed against Tunisian parties or interests;
- The offense is committed against persons or foreign interests by a foreigner or a stateless person whose habitual residence is in Tunisia; or
- The offence is committed by a foreigner or a stateless person who is on Tunisian territory and does not meet the legal conditions for extradition.

Article 34 further provides that any extradition shall take place in accordance with the applicable provisions under the Tunisian code of criminal procedure and the relevant international agreements. Indeed, any extradition request will be based on either a bilateral or a multilateral treaty on extradition.

It is also worth briefly discussing the potential use of investigatory powers against individuals outside Tunisian territory. As a general principle in public international law, the enforcement jurisdiction of States to investigate, prosecute, or apprehend an offender extraterritorially is limited by the territorial sovereignty of the foreign State. This means that a State's law

enforcement officers may only exercise their functions in the territory of another State with the consent of the latter (and given by duly authorised officials of that State).[69]

Tunisia can therefore not intercept any communications on foreign territory without violating said State's sovereignty. The Decree-law does also not provide a basis for such interception.

Typically, investigations into alleged offences by individuals outside Tunisian territory will be handled through international mutual legal assistance channels on the basis of international treaties where the requested State assists in criminal investigations. The extent of the cooperation will depend on the terms of any potential treaty in question or the political willingness of the requested State to assist Tunisia in its investigation.[70]

It is also important to mention the principle of double criminality in this context, a requirement in the extradition law of many jurisdictions. The principle of double criminality is a rule that assistance in criminal matters – including extradition - depends on double criminality in terms of the act in question being punishable and prosecutable in both the demanding and requested States. The principle is more commonly applied in extradition cases, but some States also apply it to mutual legal assistance.[71]

Based on the national legislation and international treaties in question, some States might therefore refuse extradition; for example, if the request is based on an alleged breach of the "dissemination of false news" offence in Article 24(1) of the Decree-law if said conduct is not criminalised in the respective requested State.

[69] See International Law Commission, Report on the work of the fifty-eighth session (2006), Annex E, para. 22. This explains why the Committee of Ministers of the Council of Europe has adopted a Second Additional Protocol to the Convention on Cybercrime concerning the strengthening of co-operation and the disclosure of electronic evidence.

[70] For a list of mutual legal assistance and extradition treaties between Tunisia and European States, see Tunisian Ministry of Justice, Bilateral Agreements Judicial Agreements.

[71] United Nations Office on Drugs and Crime, Manual on Mutual Legal Assistance and Extradition, 2012, para. 158.