RECIPE
Recentering The Civic Internet
Through Partner Engagement

Policy Paper on the Legal Framework on Cybercrime in Tunisia

OXFAM

Alkhatt

Policy Paper on the Legal Framework on Cybercrime in Tunisia

Introduction 3

Part I: Digital rights in the light of international standards 7

1. Freedom of expression 7
2. The right to privacy 9
Encryption 9
Protection of communications 9
The right to encryption 11

Part II: Weakness of legal safeguards related to digital rights in Tunisian legislation 12

1. Conflicts of Article 24 with the Tunisian constitution and international conventions 12
2.Risks of Chapters 9 and 10 of decree N° 54 to journalists' right to protect the confidentiality of their sources 15
3. Weak safeguards concerning the interception of communications 17
4. The danger of the right to privacy of requiring telecommunications service providers to store data in advance 18

Part III: Cybercrime in comparative systems 20

Recommendations 24

This policy paper provides an in-depth analysis of Decree No. 54 in relation to other Tunisian legislation as well as international standards related to digital rights. This analysis, carried out by Oxfam and AL KHATT Association, seeks to come up with a number of recommendations to be submitted to the parties directly related, with the aim of developing the current legislation and improving its response to its original objectives, which is to protect cybersecurity from piracy and the destruction of national digital infrastructures, without going beyond that i.e. serve as a tool to strike at civil and political rights.

Introduction

The rapid development of information and communication technologies has enhanced the capacity of individuals to access and exercise rights thanks to the spread of the Internet, the ease of use of smartphones, and the ability to reach individuals and groups at the national and international levels. Technological developments have clearly had a positive impact in terms of the right to knowledge, learning and freedom of expression, as individuals are now able to collect, disseminate and access all kinds of opinions and information regardless of geographical boundaries.

On the other hand, technological developments have also contributed to the development of the means adopted by organized crime groups and the emergence of new forms of crime aimed at encroaching on private spaces and information, hacking information and communication systems, and destroying or altering databases to harm states, economic institutions or individuals.

Among the recent global crimes, for example, is the cyberattack on Colonial Pipeline, the largest fuel pipeline in the United States, which supplies the East Coast with about 45 % of its gasoline, diesel and jet fuel needs, by a hacker group called DarkSide, which gained access to the company's systems through a password hole and encrypted sensitive data, but they also stole internal files related to the operation of the line, shutting down oil pipelines and causing chaos large until a ransom of $4 million is paid in Bitcoin.[1]

In this context, many countries have enacted legislation aimed at addressing cybercrime in order to protect their cybersecurity and the rights of individuals in the digital space. In 2001, the Budapest Convention aimed at strengthening international efforts to address cybercrime, which can only be effectively addressed through bilateral and multilateral cooperation due to the global nature of cyberspace and the overlap of several government and private entities at the level of infrastructure and communication systems.[2]

[1] For more details, see:
https://www.state.gov/darkside-ransomware-as-a-service-raas
Also: https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[2] The European Convention on Cybercrime entered into force on July 1, 2004. It can be viewed via the following link:
https://rm.coe.int/budapest-convention-in-arabic/1680739173

At the UN level, the United Nations General Assembly has established a special committee to prepare a draft international convention on combating the use of information and communication technologies for criminal purposes. Important discussions have taken place among States regarding the content and scope of the international convention, which should not deviate from its primary purposes of strengthening international cooperation to combat cybercrime without extending to threaten the gains made by international human rights instruments.[3]

On August 8, 2024, after two years of negotiations, the aforementioned committee reached agreement on the final version of the draft convention, which will open for accession in October 2025 in Thailand.

The definition of cybercrime has been the focus of debate among specialists and experts, especially since the distinction between cybercrime and non-cybercrime has a profound impact on the fundamental rights and procedural safeguards of individuals, institutions and governments alike.

Although there is no uniform definition of cybercrime, it can be recognized that there are fundamental concepts in the definition, such as the use of information and communication systems to commit a crime or damage to information and communication systems or the data stored therein. Several classifications have emerged, the most important of which is the classification between pure cybercrime and cyber-enabled crime.[4]

Pure cybercrimes are new crimes that have emerged and spread with the spread of information and communication technologies, and that can only be committed through information and communication systems, such as disrupting information and communication systems, illegally accessing them, or illegally intercepting communications. On the other hand, there are cyber-enabled crimes, that can be committed within the digital space, such as infringement of intellectual property or digital fraud and extortion, and other crimes that can be practiced outside cyberspace.

Referring to the laws in the Arab and African region, we note that in most of the legislations, crimes related to cyber-enabled crimes surpass provisions related to pure cybercrimes, which is contrary to the content of the Budapest Convention on Cybercrime or the UN Convention against Cybercrime, as the crimes of defamation, insult and fake news are not mentioned in these two conventions.[5]

[3]For more details on the International Convention against Cybercrime and the entire negotiation process that preceded it, please see the following link: https://www.unodc.org/unodc/cybercrime/convention/home.html

[4] On the definitions of cybercrime, see:
Kirsty Phillips, Julia C. Davidson,Ruby R. Farr,Christine Burkhardt,Stefano Caneppele and Mary P. Aiken, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies, https://www.mdpi.com/2673-6756/2/2/28

[5] Access Now, Cybercrime Law Policy Paper in the Arab Region: Protecting the Digital Space or Suppression of Freedoms?, 2024. Available via the following link:
https://www.accessnow.org/wp-content/uploads/2024/11/Cybercrime-Laws-in-Arab_Region_Protecting_Digital-Space-Omitten-Suppression-of-Freedoms-1.pdf

For its part, Tunisia has embarked since 2015 on a legislative process to enact a law related to cybercrime[6], which was approved by the Council of Ministers on June 1, 2018, but it was not submitted to the Assembly of People's Representatives for deliberation and approval.[7] In 2022, the President of the Republic issued Decree No. 54 of 2022 dated September 13, 2022 on combating crimes related to information and communication systems.[8]

While the issuance of a legal text related to cybercrime was natural and important to protect cybersecurity and address cybercrime, several legal provisions were added to Decree No. 54 that are not related to the original purpose of such legislation aimed at combating crimes that seek to damage or hack information and communication systems in order to obtain, alter, destroy, or use data for fraud or ransom. This led to the violation of several constitutional rights, primarily the right to freedom of expression and the right to private life.[9]

It is not an exaggeration to say that Decree No. 54 was reduced to Article 24, which included a wide range of expression offences that are already criminalized under other national legislations, such as Decree No. 115/2011 dated 2 November 2011 on freedom of the press, printing and publishing, the penal code or the communication code.

Accordingly, the implementation of Decree No. 54 in Tunisia has narrowed the digital public space and created a state of fear stifling the expression of opinions on matters of public interest due to the fear of severe penalties stipulated in the aforementioned decree. Many lawyers, politicians, journalists, and ordinary citizens have been subjected[10] to judicial consequences, often leading to imprisonment on charges brought against them on the basis of Decree No. 54. As a matter of fact, they have not committed cybercrimes with the aim of destroying information and communication systems, unlawful interception of communications, data theft, or other crimes stipulated in international conventions related to cybercrime.

As a result of diverting Decree No. 54, which laid the foundation for combating cybercrime, voices came up calling for its repeal or amendment so that it would not continue to be used to violate basic rights and force individuals to refrain from participating in public affairs.[11]

---

[6] The first version of the project can be viewed via the following link: https://cdn.nawaat.org/wp-content/uploads/2014/08/A2T_Projetdeloi.pdf

[7] Access Now, Tunisia's 'cybercrime' law: an unsolved mystery, 8 August 2018. Available via the following link: https://www.accessnow.org/Cybercrime-Law-in-Tunisia/

[8] The text of the decree can be viewed through the following link: https://legislation-securite.tn/ar/latest-laws/Decree-No-54-of-2022-Date-on-13-September-2022-Related/

[9] For the full legal analysis of Decree No. 54, please refer to the legal paper published by ARTICLE 19 via the following link: https://pamt2.org/ressources_post/Legal-Analysis-of Decree-No-54-2022-Dated/

[10] Human Rights Watch, Authorities Escalate Crackdown on Media and Freedom of Expression, May 30, 2024. Available via the following link: https://www.amnesty.org/ar/latest/news/2024/05/tunisia-authorities-escalate-clampdown-on-media-freedom-of-expression/
Also: Enkfada, «The danger is not limited to journalists»: Why is it time to amend Decree 54?, 31 January 2025. Available via the following link: https://inkyfada.com/ar/2025/01/31/Decree-54-Tunisia-Threat-Freedom-Press/

[11] Nawat, Revision of Decree 54, Late Awakening or a Maneuver to Absorb Anger, 4 July 2025. Available via the following link: https://nawaat.org/2025/07/04/ Revision-Decree-54, Late-Awakening-Um-Manawa/

On February 20, 2024, forty members of the Assembly of People's Representatives submitted a draft Basic Law No. 17/2024 to amend Decree No. 54, mainly repealing Article 24, which represents almost the only chapter adopted on «freedom of expression» cases, with the addition of several guarantees related to wiretapping of individuals, as will be clarified later, or some of the crimes mentioned in the decree.[12]

Subsequently, the Bureau of the Assembly of People's Representatives, in its session held on April 10, 2025, decided to refer the proposal to the General Legislation Committee, which held its first session on July 2, 2025, to hear the initiative.[13]

Results of the thorough reading and analysis

This paper is divided into **three** parts:

- First, digital rights in the light of international standards
- Second, the weakness of legal guarantees related to digital rights in Tunisian legislation
- Third, recommendations for a legal framework on digital security that is compatible with constitutional principles and international standards on human rights.

[12] The Draft Basic Law on the Revision of Decree No. 54 can be viewed at the following link: https://www.arp.tn/ar_SY/loi/project/4139

[13] For more details, please see the official website of the Assembly of People's Representatives: https://www.arp.tn/ar_SY/loi/project/4139

Part I: Digital Rights in the Light of International Standards

The focus of this section will be on the right to freedom of expression and the right to privacy in the digital age in view of the serious threats posed by Decree No. 54 to these two fundamental rights. These threats can be reduced to two main reasons: the first is offences related to content (slander, insult, hate speech, and dissemination of fake news) mentioned in Article 24, despite the fact that the Budapest Convention, which Tunisia has ratified, does not contain such crimes which are already criminalized under other national legislation such as Decree No. 115 related to the freedom of the press, printing and publishing. The second reason is the weak legal guarantees on the right to privacy.[14]

1. Freedom of expression

The right to freedom of expression is one of the rights most affected by technological development, as the universal nature of the Internet has allowed this right to be embodied in all its dimensions, i.e. the freedom to publish, receive, and have access to all types of information and opinions, regardless of geographical boundaries. This right has been embedded in the Tunisian legal system in many texts, such as articles 37 and 38 of the Tunisian Constitution.[15]

Tunisia has also ratified the International Covenant on Civil and Political Rights (ICCPR), article 19 of which enshrines the right to freedom of opinion and expression, to obtain and receive information without regard to geographical boundaries. A number of controls related to legitimate restrictions on the right to freedom of expression have been adopted, namely the fact that they must be stipulated in a legal text and are necessary to respect the rights or reputation of others, or to protect national security, public order, public health or public morals[16].

Decree No. 115 on the freedom of the press, printing and publication also includes in its first chapter the right to freedom of expression in accordance with the provisions of the ICCPR and other relevant international conventions ratified by the Republic of Tunisia. It stipulates that this right includes the freedom to circulate, publish and receive news, opinions and ideas of any kind, and that expression may not be restricted except by virtue of a legislative provision whose purpose is to achieve a legitimate interest in respect for the rights and dignity of others, the maintenance of public order or the protection of national defence and security; the measures taken must be necessary and proportionate to the measures required in a democratic society without endangering the very essence of the right to freedom of expression and information.[17]

---

[14] For the full legal analysis of Decree No. 54, please refer to the legal paper published by ARTICLE 19 via the following link: https://pamt2.org/ressources_post/Legal-Analysis-of Decree-No-54-2022-Dated/

[15] The constitution can be viewed through the following link: https://legislation-securite.tn/ar/latest-laws/PresidentialOrder-No-691-of-2022-Date-on-17-August-2022-Related/

[16] The International Covenant on Civil and Political Rights (ICCPR) is available at the following link: https://www.ohchr.org/ar/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[17] Decree No. 115 of 2011 of 2 November 2011 on Freedom of the Press, Printing and Publication, available via the following link: https://legislation-securite.tn/ar/latest-laws/Decree-No-115-of-2011-Date-on-2-November-2011-Off/

The right to freedom of expression is governed by a set of controls set out in article 19, paragraph 3, of the ICCPR. The Human Rights Committee interpreted it in its 2011 General Comment No. 34, which emphasized that such controls must be *"prescribed by law and imposed only for one of the reasons set out in paragraph 3, paragraphs (a) and (b); they must be consistent with rigorous tests of necessity and proportionality. Limitations may not be imposed on grounds other than those set out in paragraph 3, even if those grounds justify restrictions on other rights under the protection of the Covenant. The restrictions may apply only for the purposes for which they were made and must relate directly to the specific purpose for which they were established."*[18]

Article 55 of the Tunisian Constitution stipulates that «*restrictions on the rights and freedoms guaranteed by this constitution shall be placed only by virtue of a law and by necessity required by a democratic system, with a view to protecting the rights of others or for the purposes of public security, national defence or public health. Such restrictions must not prejudice the substance of the rights and freedoms guaranteed by this Constitution and must be justified by their objectives, proportionate to their reasons. No revision shall prejudice the gains of human rights and freedoms guaranteed in this Constitution."*

"All judicial bodies must protect these rights and freedoms from any violation."

With regard to international standards, States may restrict the right to freedom of expression in accordance with the provisions of **article 19, paragraph II** of the ICCPR, provided that the restriction complies with the requirements of the triple test:

- **Condition of Legitimacy:**

That is, stipulating the restriction within a law and drafting it in a clear and precise manner that allows individuals to regulate their behaviour and anticipate sanctions that may be imposed on them if they violate the legal text. Therefore, any use of inaccurate and broad concepts and phrases is contrary to the requirements of clarity and accuracy and thus the element of legitimacy.

- **Condition of Legality:**

That is, the achievement of a legitimate purpose under international human rights law, which is to respect the rights or reputations of others, or to protect national security or public order, public health or morals.

- **Condition of Necessity and Proportionality in a Democratic Society:**

Necessity means that recourse to the procedure is necessary to protect the legitimate interest, while proportionality is to choose the measure that will deter the offender according to the gravity of the act committed.[19] In this context, the Human Rights Committee, in its General Comment No. 34/2011, stressed that the deprivation

[18] Paragraph 22 of the Human Rights Committee's general comment No. 34 on article 19 on the right to freedom of opinion and expression. It can be viewed via the following link: https://digitallibrary.un.org/record/715606?ln=ar

[19] For more details on the controls of the right to freedom of expression and their applications in Tunisia, see: Ayman Zaghdoudi, Freedom of Expression in Tunisia, PhD thesis in Public Law, Faculty of Law and Political Science in Sousse, 2016.

of liberty is incompatible with the principle of proportionality.[20] This means that the prison sentence for blasphemy and insult and the attribution of illegal matters to a public official are all contrary to the principle of proportionality enshrined not only in article 19 of the ICCPR but also in article 55 of the Tunisian Constitution.

With regard to Article 24 of Decree No. 54, to which we will return in depth later, we conclude that the right to freedom of expression is targeted at by very severe penalties that contradict the requirements of necessity and proportionality, in addition to doubling the punishment whenever the target is a public official or similar, which is also contrary to international standards.

2. The right to privacy

In light of the rapid development of information and communication technologies and the emergence of sophisticated and complex tools used in hacking, intercepting communications and stealing data, States must pay close attention to the right to privacy by enacting legislation that protects personal data, criminalizes all forms of attacks on the confidentiality of communications, and establishes legal safeguards to limit the powers of public authorities to resort to private investigative methods while allowing individuals to protect their private lives through appropriate technical tools, including encryption.

Protection of Communications:

The right to privacy includes the right to the confidentiality of correspondence and communications. Article 17 of the ICCPR stipulates that *"no person shall be subjected, arbitrarily or unlawfully, to the intrusion into his privacy, family, home or correspondence, or to any unlawful campaign against his honor or reputation. Everyone has the right to be protected by law from such interference or infringement."*

It is worth noting that the importance of the right to privacy lies in the fact that it is a fundamental guarantee for the enjoyment of human rights in the digital age, and any restriction of this right would prevent individuals from exercising their rights. In this regard, the Supreme Court of India has affirmed that *"privacy is the highest expression of the inviolability of the individual. It is a constitutional value that extends across a wide range of fundamental rights and provides the individual with a space for choice and self-determination."*[21]

In its report on the right to privacy in the digital age, OHCHR stressed the importance of States providing all necessary safeguards to prevent any violation. One of the most important safeguards is to establish independent oversight structures to monitor oversight carried out by States or other parties.[22]

---

[20] General comment No. 34 of the Human Rights Committee on article 19 on the right to freedom of opinion and expression. It can be viewed via the following link: https://digitallibrary.un.org/record/715606?ln=ar

[21] See: Report of the Special Rapporteur on the right to privacy presented at the 37th Session of the Human Rights Council.
https://www.ohchr.org/ar/documents/reports/report-special-rapporteur-right-privacy-0

[22] Report of the Office of the United Nations High Commissioner for Human Rights, Right to Privacy in the Digital Age, 30 June 2014, A/HRC/27/37.
https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F27%2F37&Language=E&DeviceType=Desktop

For its part, the European Court of Human Rights has considered in several decisions that any process of phone-tapping and censoring the communications of individuals must be consistent with the triple test of legitimacy, legality, and necessity/proportionality. A number of controls have been put in place to help strike a balance between the right to privacy on the one hand and other legitimate objectives that can justify the interception of communications by public authorities in certain situations. These controls are:

1. Grounds for censorship and interception of communications that should be serious and related to serious crimes against the lives of individuals or national security and defence;

2. Circumstances under which communications made by individuals can be intercepted, i.e. the need to determine with precision the exact times when the suspect's communications can be intercepted and the list of individuals who can be exempted from interception when contacted by the suspect (e.g., minor children);

3. The procedures adopted to obtain an interception permit, which should always go through the judiciary to ensure that the Administration's agents do not resort to this procedure;

4. Procedures for the selection, examination and use of intercepted content;

5. Precautions to be taken into account when delivering intercepted content to third parties;

6. Restrictions related to the duration of the interception operation and the security of the interception's results and their destruction, which means that the interception period cannot be extended arbitrarily or indefinitely, in addition to the need for the judicial authority to supervise the storage of the intercepted data and its destruction after the need for it has ceased to exist.

7. Procedures to monitor this action by an independent structure and its deterrent powers in the event of a breach of the above-mentioned safeguards;

8. Ex-post control procedures and safeguards that enable the appropriate punishment to be arranged, especially by informing the suspect that he was subject to the wiretapping operation, especially in the event that no evidence incriminating him was found, which enables him to track down those involved in the wiretapping process if the reasons are not serious or the legal procedures related to the interception of communications are not respected.

We will see later the opposition (or contradictions) of Decree No. 54 , and in particular Chapters 9 and 10 thereof, to these standards by failing to specify methods to renew the judicial authorization to intercept communications or by not providing for the exhaustion of ordinary investigation methods before resorting to this exceptional measure.

[23] The decision can be viewed via the following link: https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2258170/13%22,%2262322/14%22,%2224960/15%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-210280%22
In this context, see also the European Court of Human Rights' Guide on the Applications of Chapter VIII of the European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/guide_art_8_eng

The right to encryption:

Many countries are trying to restrict the right to encryption for a number of reasons, including protecting public security and addressing crimes that could harm individuals. Despite the relevance of these considerations, any restriction on the right to encryption should be necessary and proportionate and laws on these issues should be developed in a participatory and open manner.[24]

Encryption can be defined as *"the mathematical process of converting messages, information, or data into a form that can only be read by the target recipient."* Thus, encryption ensures the confidentiality and integrity of the content from any interception or surveillance by third parties.[25]

For his part, the Special Rapporteur on the promotion and protection of the right to freedom of expression stressed the role of encryption in ensuring that individuals enjoy the right to freedom of expression, as it allows them to express their opinions and disseminate information without fear of judicial consequences that may arise against them for criticizing public authorities or exposing abuses.[26]

Encryption is increasingly important for journalists as it allows them to protect the information they hold and ensure that their sources are not revealed. Encryption is also considered a fundamental guarantee for the protection of the right to privacy, as the OECD has stressed that the confidentiality of communications and information and communication systems cannot be protected without ensuring encryption and that every violation of it is considered a serious threat to the protection of personal data.[27]

[24] ARTICLE 19, Right to Anonymity in Cyberspace, 2015, p. 11. https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

[25] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the use of encryption and anonymity in digital communications, 22 May 2015, A/HRC/29/32, para. 7.

[26] Ibid.

[27] ARTICLE 19, Right to Anonymity in Cyberspace, 2015, p. 15. https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

Part II: Weakness of Legal Safeguards Related to Digital Rights in Tunisian Legislation

While it is necessary to enact laws related to cybercrime, the legitimate purpose of protecting information and communication systems and the data stored in them cannot justify the violation of digital rights by adding crimes that are not cyber in origin or reducing the legal safeguards necessary to protect digital rights.

1. Conflicts of Article 24 with the Tunisian Constitution and International Conventions

Article 24 of Decree No. 54 stipulates that *"Anyone who deliberately uses information and communication networks and systems to produce, promote, publish, transmit, or prepare false news, data, rumours, or documents that are artificial, forged, or falsely attributed to others with the aim of infringing on the rights of others, harming public security or national defence, or spreading terror among the population, shall be punished by imprisonment for a period of five years and a fine of fifty thousand dinars.*

Anyone who deliberately uses information systems to publish, disseminate news, artificial or forged documents, or data containing personal data or attribution of false matters with the aim of slandering or defaming others, harming them financially or morally, inciting attacks or inciting hate speech shall be punished with the same penalties as prescribed in the first paragraph.

The penalties prescribed are doubled if the targeted person is a public official or equivalent."

This chapter raises several legal problems, the most important of which is the lack of clarity of its wording, the disproportionality of the penalties stipulated therein, and its contradiction with other legal texts in force.

Regarding the first issue, Article 24 criminalizes a wide range of acts that include not only the publication of content, but even the preparation, production and transmission of prohibited content. In this context, criminal liability can arise for a person whose computer contains a text, which is still being prepared and checked, even though that text may be produced by AI which can in some cases generate inaccurate text or include dangerous speech. The overbroad nature of Article 24 makes it possible to track individuals even if the content is not published, and even if it is in the form of an informational file, such as a draft text whose authenticity is being investigated and verified.

The aforementioned chapter also included a new and unique crime of «incitement to hate speech», which is strange, since the scope of the crime is not based on hate speech per se, but on the act of incitement itself, which necessarily leads to the exclusion of hate speech from the scope of application of this chapter as long as it does not include incitement.[28]

[28] See the legal paper published by ARTICLE 19 via the following link: https://pamt2.org/ressources_post/Legal-Analysis-of Decree-No-54-2022-Dated/

Returning to the (ICCPR), article 20, paragraph 2, obliges States to prohibit hate speech on the basis of race, religion or nationality that constitutes incitement to discrimination, hostility or violence. Consequently, the offence of incitement to hate speech is not in accordance with international standards, since it does not criminalize incitement to violence against individuals and groups because of their characteristics protected under international law, such as colour, sex, religion, race and other characteristics.

The use of broad language is contrary to international standards on freedom of expression, as the Human Rights Committee calls for laws to be drafted *"with sufficient precision so that an individual can control his or her behaviour in accordance with them and must be made available to the general public. The law may not give the persons responsible for its implementation absolute discretion to restrict freedom of expression. The law must provide adequate guidance to those in charge of implementing it to enable them to properly verify which types of expression are subject to the restriction and those that are not."*[29]

On the other hand, the penalties provided for in Article 24 are inconsistent with the requirements of necessity and proportionality, since a penalty of five years is provided for multiple types of expression, without taking into account the degree of harm that each of them may cause. Whether the content is to harm the reputation of individuals or to harm national defence, both are subject to the same punishment, which is contrary to the principle of gradual punishment according to the seriousness of the act committed.

Furthermore, the penalties for deprivation of liberty for defamation offences are disproportionate, with the Human Rights Committee, in its General Comment No. 34 of 2011, calling for consideration of decriminalizing, emphasizing in particular the incompatibility of deprivation of liberty with the principle of proportionality.[30]

The last paragraph of Article 24 is also contrary to the principle of equality because it provides for doubling of punishment in the event that the object of the illegal expression is a public official or similar. The Human Rights Committee went in the same direction when it recognized that *"laws should not provide for the imposition of harsher penalties solely on the basis of the identity of the person being challenged."*[31]

Finally, Article 24 contradicts other legal provisions in force that criminalize the same acts, such as but not limited to Decree No. 115 on freedom of the press, printing and publication criminalizing the dissemination of fake news, hate speech, slander, and insults under articles 53 and onwards. The Penal Code also included, in articles 128, 245 and others, crimes related to content that contain damage to the reputation of individuals or false news that would harm public security. Article 86 of the Communications Code criminalized offences towards others through public communication networks.

[29] General comment No. 34 of the Human Rights Committee on article 19 on the right to freedom of opinion and expression. It can be viewed via the following link: https://digitallibrary.un.org/record/715606?ln=ar

[30] General comment No. 34 of the Human Rights Committee on article 19 on the right to freedom of opinion and expression. It can be viewed via the following link: https://digitallibrary.un.org/record/715606?ln=ar

[31] General comment No. 34 of the Human Rights Committee on article 19 on the right to freedom of opinion and expression. It can be viewed via the following link: https://digitallibrary.un.org/record/715606?ln=ar

For example, in the case of an individual who publishes a post that contains incorrect things that may harm the reputation of a public official, there are several legal texts that would apply to this content, such as article 128 of the Penal Code, which stipulates the crime of attributing illegal acts or facts to a public official, article 55 of Decree No. 115, which stipulates the crime of defamation (defamation is attributing incorrect matters that may harm the reputation of individuals), or article 86 of the Telecommunications Code, which includes the crime of offending others through public communication networks, as well as article 24 of Decree No. 54 and other legal chapters that criminalize the same act. The main problem in this context is the clear contrast between the penalties, ranging from financial sanctions in Decree No. 115 to 10-year imprisonment according to Decree No. 54.

It is also unacceptable to accept any approach aimed at applying Decree No. 115 to journalists and anyone who expresses his opinion in the media, and to apply the Telecommunications Code, the Penal Code, or Decree No. 54 to others, because this violates the principle of equality and would lead to the emergence of unfair situations, such as the application of Decree No. 115 to journalists who publish false content and punish them with sanctions, while Decree No. 54, the Communications Code or the Penal Code are applied in other cases, hence imprisoning anyone who reshares the same content on social media sites or in the public space.

Accordingly, the judicial system must deal with all these conflicting legal texts, which leads to a violation of the principle of legal safety, as it is difficult to predict a judge's position on a particular expression, as this expression can be interpreted as a crime or may not be interpreted as such. This confusion was reflected in the decisions of the Court of Cassation, which tried to exclude Article 24 from application and thus resorted to either Decree No. 115 or Article 86 of the Communications Code. However, the Court's jurisprudence lacked consistency since it ruled out the application of Article 24 to posts critical of the President of the Republic that were published on a social media site on the grounds that Decree No. 54 and the Budapest Convention related to cybercrimes without highlighting the outcome of this article. Considering that it was not contrary to the Constitution or international conventions, the Court of Cassation did not do more but ruling it out, considering that *"Blogs and posts published by people on social media are not subject to the provisions of Decree No. 54, as the violations and crimes that may be committed by their owners through such posts are not considered electronic crimes as described above, but are traditional crimes governed by the Penal Code as the general law or some injunctive texts contained in other codes or special laws, as the case may be."*[32]

In another decision, the Court of Cassation confirmed that Decree No. 54 did not abrogate Decree No. 115 on Freedom of the Press, Printing and Publishing, which remains applicable to crimes committed in the media, and that it does not apply to the opinions of journalists and media professionals that they express, as the first chapter of Decree No. 54 *"does not include crimes that may be committed by a journalist, media professionals, or any intervenor in the public sphere when expressing their opinion on a matter, commenting on a news or giving a position on issues of public interest."*

[32] Court of Cassation, Decision No. 56798 of December 22, 2024, unpublished.

In these two decisions, the Court of Cassation found itself in embarrassment, mainly represented by the disproportionality of the penalties stipulated in Decree No. 54, whose original purpose is to combat cybercrime and not freedom of expression, and the possibility of applying other legal texts that have been applied in similar cases. Although the exclusion of Article 24 remains commendable, its legal structure remains weak due to the court's failure to decide upon, despite its clear contradiction with the Constitution and international conventions.

In the light of many other such examples, the repeal of Article 24 of Decree No. 54 is essential not only to protect freedom of expression in the digital space, but also to avoid conflicts of jurisprudence that would harm the principles of legitimate trust in institutions and legal integrity.

2. Risks of Chapters 9 and 10 of Decree No. 54 to Journalists' Right to Protect the Confidentiality of Their Sources

The right to protect the confidentiality of journalistic sources is a fundamental pillar of journalistic work. In the absence of such a right, the source will not trust the journalist and will hesitate to provide them with important information for investigative reporting, such as information that would expose corruption, for fear of repercussions should the journalist be forced to reveal the identity of the source.

In its interpretation of article 19 of the ICCPR, the Human Rights Committee called on States to *"recognize and respect that one of the elements of the right to freedom of expression includes the privilege of journalists to anonymize and protect their sources of information."*

Tunisia has enshrined this right in accordance with the last paragraph of article 11 of Decree No. 115 on Freedom of the Press, Printing and Publication, which stipulates that *"a journalist shall not be subjected to any pressure from any authority, nor shall any journalist or person contributing to the preparation of the media material be required to disclose the sources of their information except with the permission of the competent judicial judge, provided that such information is related to crimes that pose a grave danger to the physical integrity of others and that the access to such information is necessary to avoid the commission of these crimes and when information cannot be obtained in any other way."*

In light of the provisions of the aforementioned article, we conclude that a journalist's right to protect their sources can only be infringed upon when three conditions are met:

- Presence of a judicial authorization

- The purpose of the disclosure of the source should be to avoid crimes that pose a serious danger to the physical safety of others, and that obtaining them is necessary to avoid committing such crimes.

- Information must be such that it cannot be obtained in any other way, i.e. all available legal means of obtaining such information have been exhausted before resorting to the request for source disclosure.

With reference to provisions of Articles 9[33] and 10[34] of the Decree, we note that the Prosecutor of the Republic, the investigating judge or the officers of the judicial police are authorized in writing to seize the entire or part of an information system or carrier, including the data stored therein, which would help to uncover the truth. In cases where the need for an investigation is necessary, they may also resort to intercepting the communications of suspects.

The application of this chapter necessarily violates the right to confidentiality of sources enshrined in Chapter 11 of Decree No. 115 since all three conditions are not met. While the first condition of judicial authorization is respected, journalists' phones, cameras, computers or communications may however still be confiscated or intercepted in order to detect crimes that do not pose a threat to the physical safety of others (the second condition) and without exhausting all legal means available to obtain this information before resorting to a source disclosure request (the third condition).

This regression in protecting the right of journalists to protect their sources contradicts provisions of article 55 of the Constitution, which states that «no revision shall prejudice the gains of human rights and freedoms guaranteed in this Constitution.» It also contradicts the General Comment No. 34 of the Human Rights Committee, which called on states to protect this fundamental right.

What makes Articles 9 and 10 even more dangerous is the existence of offences of expression in Article 24, which, by virtue of their existence in Decree No. 54, permit the use of the seizure of electronic equipment and the interception of communications

[33] Article 9 states that "the Prosecutor of the Republic, the investigating judge or the officers of the judicial police authorized in writing may order:

• Enabling them to access information data stored in a system, an information carrier, or related to a telecommunications transaction, its users, or other data that would help to uncover the truth.
• Seizure of the whole or part of an information system or an information drive, including the data stored therein, which would help uncover the truth. If the seizure of the information system is not necessary or cannot be made, the data related to the crime and the data that are readable and understood shall be copied to an information drive in a manner that ensures the correctness and integrity of its content.
• Collect or record telecommunications flows data immediately using appropriate technical means.

They can also access any system or information drive directly or with the help of experts they see and conduct an inspection of the drives in order to obtain stored data that would help uncover the truth.

The competent departments of the Ministry of National Defense and the Ministry of Interior shall ensure the seizure process, its location, and the process of accessing information systems, data, stored data, software and all their disks and drives related to the two ministries, each according to its field."

[34] Article 10 stipulates that: "In cases where the investigation necessitates the interception of suspect's communications by virtue of a reasoned written decision issued by the Public Prosecutor or the investigating judge, and in the same cases, and on the basis of a reasoned report by the judicial police officer in charge of examining crimes, the interception of the communications of the suspects may be resorted to by virtue of a reasoned written decision by the Public Prosecutor or the investigating judge.

Interception of communications includes obtaining traffic data, wiretapping or accessing the content of communications, as well as copying or recording them using appropriate technical means and, where appropriate, the use of competent structures, each according to the type of service provided.

Traffic data is the data that allows the identification of the type of service, the source of the connection, the destination or recipients, the network through which it passes, its time, date, size and duration."

made by journalists, thereby exposing them and endangering their work. Therefore, we believe that it is necessary to exclude journalists from the scope of application of this chapter wherever their journalistic duties are concerned, in order to ensure harmony between Decree No. 54 and Decree No. 115 on freedom of the press, printing and publishing.

3. Weak safeguards concerning the interception of communications

Technological development has contributed to the development of communication methods between individuals and the promotion of civil and political action thanks to the ease of communication with the public and the ability to coordinate between various actors in the public space through digital communication channels. On the other hand, the methods of censorship and interception of communications have evolved to keep pace with the digital transformation, which should be surrounded by a great deal of safeguards so that they are not abused and thus the private life of individuals is compromised, especially the right to confidentiality of communications, which is enshrined in article 30 of the Tunisian Constitution.

In view of their impact on the right to private life, communications interceptions must be subject to specific safeguards in view of the terrifying and intimidating effects that can be felt on individuals under legislation that frees the hands of public authorities without any clear conditions and adequate safeguards. The Special Rapporteur on the promotion and protection of the right to freedom of expression has recommended that this procedure be subject to the supervision of an independent judiciary that is limited to the detection of serious crimes, or that other less severe measures be put in place to achieve the same end. The period of time for the wiretapping should also be specified and the person concerned should be informed following the conclusion of the investigation that he or she was subject to such action and his right to litigate in the event of damage caused to him as a result of the process.[35]

In order to balance between the State's efforts to combat cybercrime with respect for the right to confidentiality of communications, Article 10 of Decree No. 54 stipulates that *"in cases where the investigation necessitates the interception of suspect's communications by virtue of a reasoned written decision issued by the Public Prosecutor or the investigating judge, it is also possible similar cases on the basis of a reasoned report by the judicial police officer in charge of examining crimes, to intercept suspects' communications by virtue of a reasoned written decision by The prosecutor of the republic or the investigative judge. Interception of communications includes obtaining traffic data, wiretapping or accessing the content of communications, as well as copying or recording them using appropriate technical means and, where appropriate, the use of competent structures, each according to the type of service provided. Traffic data is the data that allows the identification of the type of service, the source of the connection, the destination or recipients, the network through which it passes, time, date, size and duration."*

[35] The report can be viewed via the following link: https://digitallibrary.un.org/record/3814512?ln=en

This chapter makes two basic observations. The first is that it is used only in cases of cybercrime, and therefore it cannot be used to investigate other crimes unless it contains a special provision, such as human trafficking and terrorist crimes. Second, while this chapter requires the existence of judicial authorization prior to the interception process, it lacks several other safeguards included in international standards as in national legislation; such as, to intercept communications only after all the least intrusive measures have been met and to inform the person concerned after the conclusion of the investigation that he or she was subject to such action so that he or she can sue the parties that authorized the interception without respecting legal safeguards.[36] The non-requirement of specifying the length of time in which the wiretapping will take place and the cases of extensions in the wiretapping period is contrary to the principle of necessity and proportionality, because this means that it is possible to wiretap not only the targeted person for an indefinite period, but also his or her colleagues, friends and family members, which would infringe on the rights of others as well.[37]

At the national level, Articles 54 of Basic Law No. 26/2015 dated 7 August 2015 on the Prevention of Terrorism and Money Laundering[38] and Article 32 of the Organic Law No.61/2016 dated 3 August 2016 on the Prevention and Combating of Trafficking in Persons[39] stipulate that *"The interception period cannot exceed four months from the date of the decision, which may be extended once for the same period by virtue of a reasoned decision."*

4. The danger of the right to privacy of requiring telecommunications service providers to store data in advance

The Tunisian Constitution enshrines the right to private life at the heart of the first paragraph of Article 30, which stipulates that *"the State shall protect private life, the inviolability of the residence, and the confidentiality of correspondence, communications and personal data."*

International human rights law also enshrines the right to privacy at the heart of article 17 of the ICCPR, which states that *"1. No person shall be subjected, arbitrarily or unlawfully, to interfere with his or her privacy, family, home or correspondence, or to any unlawful campaigns that affect his/her honour or reputation. 2. Everyone has the right to be protected by law from such interference or infringement."*

With regard to provisions of chapter 6 of Decree No. 54, we conclude that there is a conflict with the Constitution and international standards relating to the right to privacy, as telecommunication service providers are obliged to keep data stored in an information system for a period of at least two years from the date of data registration.

---

[36] On the legal principles related to telecommunications censorship, see: EFF and ARTICLE 19, International principles on the application of human rights law to communications surveillance, available online: https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

[37] Cf. Report of the Special Rapporteur on the Promotion of the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, 23 September 2014, A/69/397, para. 66.

[38] Available via the following link: https://legislation-securite.tn/ar/latest-laws/Statute-No-26-2015-Date-on-7-Aug-2015-Text/#:~:text=Chapter%2030%20-%2020%20Commits%20 of a crime, 20%20 of an act%20 or %20%20 of abstinence%20

[39] Available via the following link: https://legislation-securite.tn/ar/latest-laws/Bylaw-No-61-2016-Date-on-3-Aug-2016-Date/

The data to be saved are:

- Data that enables the identification of users of the service.
- Data related to communication traffic flows.
- Data related to communication peripherals.
- Data related to the user's geographical location.
- Data related to the availability and exploitation of protected value-added content.

While Decree No. 54 does not oblige telecommunications service providers to store data on the content of communications and messages exchanged between people, the data contained in chapter 6 clearly infringes on the right to private life, since it allows for detailed conclusions about the daily behaviours, mobility routes and social relationships of individuals. This is done by identifying the place where the call was made, the type of device, and by collecting data on the traffic of all people, it is possible to identify their whereabouts and when meetings took place and other information related to private life.[40] For these reasons, we consider that the prior and public storage of such data (i.e., involving all individuals present in Tunisian territory) violates the right to private life, the right to protection of personal data and a disproportionate procedure.

The Court of Justice of the European Union has issued several decisions in which it has considered that obliging telecom service providers to store traffic data for all users in advance and automatically without any suspicion of committing a particular crime constitutes a violation of the right to the protection of personal data and private life, as it is contrary to the Charter due to the failure to respect the requirements of necessity and proportionality.[41]

This action cannot be justified by the fight against crime and the need for such data to be consulted whenever required by the investigation. In the same logic, the State would justify placing surveillance cameras inside homes, recording what is going on inside, and using them in investigations whenever a crime is committed inside a home. Proportionality in this context requires favouring the presumption of innocence for individuals at the expense of finding the truth in the case of crimes.

For these reasons, it is advisable to amend Article 6 in order to limit the obligation to store and preserve data in cases related to the existence of crimes, provided that the competent judge authorizes this to ensure judicial control over the balance between the right to private life on the one hand and the legitimate objective of guaranteeing the rights of others and public security on the other.

[40] The OSCE Guide on Ensuring Respect for Human Rights in Conducting Cybercrime Investigations Reviews: Organization for Security and Co-operation in Europe, Ensuring Human Rights Compliance in Cybercrime Investigations, 13 October 2023. Available online: https://www.osce.org/secretariat/554901

[41] See: The decision dated December 21, 2016, is available via the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203
The decision dated 6 October 2020 is available via the following link: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62017CJ0623

Part III: Cybercrime in Comparative Systems

Ninety percent of countries have passed laws related to cybercrime either in separate laws or through amendments to penal laws.[42] For example, Australia,[43] Germany[44], Morocco[45], and Canada[46] have amended their penal codes and added cybercrimes. Other countries such as Tunisia, Egypt,[47] Jordan,[48] Botswana,[49] Malaysia,[50] Kenya,[51] and South Africa[52] have envisioned enacting laws on cybercrime.

Regarding comparative legislation, we note that several authoritarian countries have added content crimes to the core of cybercrime laws, which constitutes a violation of the right to freedom of expression. Article 23 of Kenyan law,[53] article 28 of Syrian law,[54] article 22 of the UAE law,[55] article 16 of Tanzanian law,[56] and article 24 of Sudanese law[57] criminalize anyone who publishes false news, all of which are crimes similar to those stipulated in Article 24 of Decree 54.

---

[42] https://unctad.org/page/cybercrime-legislation-worldwide

[43] https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/wM2oCWukY7tM/content/australia?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_assetEntryId=64860673&_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3Dcom_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_cur%3D0%26p_r_p_resetCur%3Dfalse%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_assetEntryId%3D64860673%23p_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM#p_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM

[44] https://www.coe.int/en/web/octopus/-/germany

[45] http://site.eastlaws.com/GeneralSearch/Home/ArticlesTDetails?MasterID=336365#:~:text=%D9%88%D9%8A%D8%B9%D8%A7%D9%82%D8%A8%20%D8%A8%D9%86%D9%81%D8%B3%20%D8%A7%D9%84%D8%B9%D9%82%D9%88%D8%A8%D8%A9%20%D9%85%D9%86%20%D8%A8%D9%82%D9%8A,%D9%84%D9%84%D9%85%D8%B9%D8%B7%D9%8A%D8%A7%D8%AA%20%D8%A3%D9%88%20%D8%A7%D8%B6%D8%B7%D8%B1%D8%A7%D8%A8%20%D9%81%D9%8A%20%D8%B3%D9%8A%D8%B1%D9%87

[46] https://laws-lois.justice.gc.ca/eng/acts/c-46/

[47] https://www.coe.int/en/web/octopus/-/egypt

[48] https://www.coe.int/en/web/octopus/-/jordan

[49] https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/wM2oCWukY7tM/content/botswana?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_assetEntryId=64859800&_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3Dcom_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_cur%3D0%26p_r_p_resetCur%3Dfalse%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_assetEntryId%3D64859800%23p_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM#p_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM

[50] https://www.coe.int/en/web/octopus/-/malaysia

[51] https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf https://www.article19.org/resources/kenya-withdraw-computer-misuse-and-cybercrimes-bill-and-protect-freedom-of-expression/

[52] https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

[53] https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

[54] https://moct.gov.sy/news-0015

[55] https://u.ae/ar-ae/resources/laws

[56] https://www.nps.go.tz/uploads/documents/sw-1751202044-The%20Cybercrimes%20Act.pdf

[57] https://drive.google.com/file/d/1IFMoDS6o31hKS7jgg-sq1yHbCUo-djEF/view

It should also be noted that States Parties to the Budapest Convention have multiple pieces of legislation, as countries such as Tunisia or Costa Rica[58] have added crimes related to digital content, which would disrupt bilateral cooperation between States Parties. If a country such as Tunisia submits a request for information related to a non-cybercrime such as phishing or spreading fake news online, its request will be rejected by several States Parties because they do not consider such crimes to be cybercrimes. In contrast, there are countries that have largely respected the Budapest Convention, such as Switzerland[59] or Belgium[60].

In order to ensure effective international cooperation, the focus should be on the real risk of crimes targeting information and communication systems or using technological means to steal and destroy evidence and intercept communications, all of which require States to work together. Crimes of expression should be addressed by special laws that take into account international standards on freedom of expression as set out in article 19 of the ICCPR and General Comment No. 34 of 2011 issued by the Human Rights Committee.

58 https://www.coe.int/en/web/octopus/-/costa-rica

59 https://www.coe.int/en/web/octopus/-/switzerland

60 https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/wM2oCWukY7tM/content/belgium?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_assetEntryId=64858902&_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3Dcom_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_cur%3D0%26p_r_p_resetCur%3Dfalse%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM_assetEntryId%3D64858902%23p_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM#p_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_wM2oCWukY7tM

Comparison between Tunisian Cybercrime Legislation and Comparative Legislation[61]

	UN Convention on Combating Cybercrime	Budapest Agreement	Tunisia	Egypt	South Africa	Croatia	Monaco
Obliging telecom service providers to comprehensively store traffic data	Non-existent	Non-existent	Exists	Exists	Non-existent	Non-existent	Non-existent
The crime of spreading fake news	Non-existent	Non-existent	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)[62]	Non-existent	Non-existent	Non-existent
The crime of incitement to violence	Non-existent	Non-existent	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)	Exists	Non-existent	Exists
The crime of defamation (attributing incorrect matters that would harm the dignity and reputation of persons)	Non-existent	Non-existent	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)	Non-existent	Non-existent	Non-existent
Hate speech crime	Non-existent	Non-existent[63]	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)	Non-existent	Exists	Exists

[61] We selected these four countries on the basis of two main criteria: on the one hand, the extent to which there is independent legislation on cybercrime (Egypt and South Africa) and on the other hand, the criteria for accession to the Convention on Cybercrime (Croatia and Monaco).

[62] This article stipulates that anyone who "establishes, manages or uses a private website or account on an information network with the aim of committing or facilitating the commission of a crime punishable by law."

[63] are not included in the Budapest Convention, which Tunisia has ratified, but has been added under the Additional Protocol on the Criminalization of Acts of a Racist and Xenophobic Nature, Committed by Computer Systems, which entered into force on March 1, 2006, and is not binding on the Tunisian State as long as it does not adhere to it.

	UN Convention on Combating Cybercrime	Budapest Agreement	Tunisia	Egypt	South Africa	Croatia	Monaco
The crime of slandering a civil servant	Non-existent	Non-existent	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)	Non-existent	Non-existent	Exists
The crime of unlawful interception of communi-cations	Exists	Exists	Exists	Exists	Exists	Exists	Exists
The crime of illegal access to informa-tion and communica-tion systems	Exists	Exists	Exists	Exists	Exists	Exists	Exists
Data Interference Crime	Exists	Exists	Exists	Exists	Exists	Exists	Exists
Misuse of devices	Exists	Exists	Exists	Exists	Exists	Exists	Exists
Cyber Forgery Crime	Exists	Exists	Exists	Exists	Exists	Exists	Exists
Cyber Fraud Crime	Exists	Exists	Exists	Exists	Exists	Exists	Exists
Child pornography offences	Exists	Exists	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)	Non-existent	Exists	Exists
Crimes related to copyright infringement	Non-existent	Exists	Exists	Exist (indirectly, as stipulated in Article 27 of the Law on Combating Information Technology Crimes)	Non-existent	Exists	Exists

Recommendations

According to the in-depth analysis of provisions of Decree No. 54 aimed at contributing to improve the Tunisian legislation related to digital rights to be more compatible with other laws and regulations in force in the Republic of Tunisia as well as with international human rights standards, the following recommendations are made:

For members of the House of People's Representatives:

- Define a precise definition of cybercrime in Decree No. 54 in order to avoid any interpretation that would expand the scope of criminalization of digital behaviours and reduce it to acts that deliberately target the confidentiality, integrity and continuity of the information and communication systems and data stored therein.

- Avoid repressive censorship of content by ensuring communication service providers do not monitor content in advance, but rather ensure that any censorship follows a judicial authorization from the competent court and respects procedures related to the rights of defence and the principle of confrontation. Amend Chapter 6 of Decree No. 54 in order not to oblige telecommunication service providers to store contact data comprehensively and pre-emptively because this obligation is contrary to international standards related to the protection of personal data, and to oblige telecommunication service providers to store data related to communication traffic only in the event of a judicial authorization in the framework of criminal investigations related to specific individuals; the permission should be time-limited, with the need to inform those concerned after the conclusion of the investigations, regardless of their outcome.

- In line with the Budapest Convention on Cybercrime and the United Nations Convention to Combat Cybercrime, repeal Article 24 of Decree No. 54 since speech crimes are not considered cybercrimes, and limit Decree No. 115 on freedom of the press, printing and publication to the crimes of defamation, insult, incitement and dissemination of fake news.

- Offer sufficient safeguards to ensure that special investigative methods are not abused, including the limitation of the time period for the interception of communications and the conditions for their renewal, in addition to the fact that they shall be used only after all normal investigative mechanisms have been exhausted, and that the individual whose communications have been intercepted shall be notified after the conclusion of the operation, even if no evidence has been found to incriminate him or her.

For the Executive Branch:

- Exert all efforts to popularize digital education and raise awareness about its positive and negative effects by supporting stakeholders' programs, such as digital rights trainings and awareness raising campaigns by trade unions and civil society organizations, and allocate sufficient school time to educate young people on dealing with electronic platforms and the importance of digital security, and to support the media to produce programs related to media and digital literacy.

- Spread awareness and enhance knowledge using data and statistics concerning issues related to Decree No. 54 and publish judicial decisions to enable researchers to analyse them and publish scientific studies in the field of cybercrimes.

For the Judiciary:

- Exclude the application of Article 24 of Decree No. 54 and Enforce Decree No. 115 only in all cases related to freedom of expression.

- Rely on Article 55 of the Tunisian Constitution in matters of expression and establish a balance between freedom of expression and other legitimate interests, while ensuring that the conditions of necessity and proportionality are respected whenever punishment and sanctions are enforced.