www.amnesty.org

AMNESTY INTERNATIONAL PUBLIC STATEMENT

12 December 2022 MDE 30/6290/2022

REPEAL DRACONIAN CYBERCRIME DECREE

Tunisia must repeal a new cybercrime decree issued by President Kais Saied that severely threatens the rights to freedom of expression and privacy, Amnesty International said today. The decree-law is among the latest legislative attacks by the president on human rights safeguards since he carried out a power grab in July 2021.

President Saied has held sole legislative power since he suspended parliament on 25 July 2021. Decree-law 2022-54, issued on 13 September 2022, imposes heavy prison sentences for the wilful and malicious spread of false information via digital networks based on ambiguous terms such as "fake news," and empowers authorities to shut down entities such as media outlets and civil society groups for offenses under its provisions.[1]

It also grants authorities sweeping powers to monitor how people use the internet, collect personal data, and intercept private communications based on vaguely defined criteria – such as the possibility that such information "might help reveal the truth" about suspected crimes - that allow for widespread surveillance.

Already, authorities have opened criminal investigations under Decree-Law 2022-54, including for public criticism of top government officials.[2] Regardless of how authorities seek to use the decree-law, the menace it poses to freedom of expression and privacy risks creating a chilling effect on both public and private use of the internet.

Since the 2011 ouster of dictator Zine El Abidine Ben Ali, authorities have regularly relied on longstanding repressive laws, including articles of the penal code that criminalize "outrage" and defamation of public officials, to prosecute people for exercising their right to freedom of expression. However, Decree-Law 2022-54 introduces some of the harshest new measures in over a decade to enable authorities to punish the exchange of information and ideas.

International human rights law guarantees the rights to freedom of expression and to privacy.[3] Any restrictions imposed on them must be exceptional, provided by law, and strictly necessary and proportionate to achieving a legitimate aim.[4] Core provisions of Decree-Law 2022-54 fail to meet those requirements.

Decree-Law 2022-54 contains some provisions that are in line with human rights protections. These include, for example, the criminalization of unauthorized disclosure or use of personal data collected in criminal investigations, and of wilfully accessing, producing, or spreading child sexual abuse material.[5] However, it fails to provide for adequate human rights safeguards including effective independent oversight mechanisms.

While the prevention of crimes committed online is a legitimate concern, governments must never use legislation to fight crime of any kind as a license to violate the rights to privacy or freedom of expression as protected by international law.

---

[1] The full name of decree-law is "Decree-Law 2022-54 of 13 September 2022 relating to the fight against offenses in connection with systems of information and communication". Available in Arabic and French via the website of Tunisia's official gazette: http://www.iort.gov.tn

[2] These include investigations under Decree-Law 2022-54 against Nizar Bahloul, editor of the online news outlet *Business News*, for an article criticizing Prime Minister Najla Bouden, and lawyer Mehdi Zagrouba, for a Facebook post he wrote criticizing Justice Minister Leila Jaffel, and an investigation ordered by the justice minister against lawyer and politician Ghazi Chaouachi for remarks to media. A Tunis court is investigating Ahmed Hamada, a university student whose Facebook page came under police scrutiny, under the decree-law plus articles 131 and 132 of the penal code relating to organized violence, according to his lawyers.

[3] Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 9 of the African Covenant on Human and Peoples' Rights (ACHPR), both of which Tunisia has ratified.

[4] ICCPR, Article 19, Paragraph 3; Human Rights Committee, General Comment 34, in particular Sections 21, 22; Human Rights Committee, General Comment 16, in particular Sections 1, 3, 4, and 8

[5] Decree-Law 2022-54, Articles 31 and 26, respectively.

Harsh penalties for "fake news" and defamation

Article 24 of Decree-Law 2022-54 mandates five years in jail and a fine of 50,000 Dinars (around 15,500 USD / 14,900 Euros) for using telecommunications networks to produce, send, or disseminate "fake news," "false data," "false rumours," or "fake, falsified, or falsely attributed documents" to harm, defame, or incite violence against others, or to undermine public safety or national defence, spread fear, or incite hatred. The penalties are doubled if the victim is a public official.

Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which Tunisia has ratified, guarantees the right to freedom of expression. Official guidance on implementing Article 19 by the United Nations' Human Rights Committee (HRC) states that to meet the requirement of being provided by law, any restrictions on freedom of expression "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly…."[6]

Restrictions based on ambiguous terms such as "fake news," which the decree-law fails to define, fail to meet that requirement, and could grant authorities leeway to prosecute people for exercising their right to freedom of expression as protected by international law.[7]

The HRC has noted that leaders and public officials should not be protected from criticism, and that defamation laws should not provide for more severe penalties "solely on the basis of the identity of the person that may have been impugned."[8] Defamation should always be treated as a civil, not criminal, offence, and should never be punished with time in prison.[9]

Article 32 of Decree-Law 2022-54 allows authorities to penalize groups of people whom they deem a single legal entity for crimes under Decree-Law 2022-54 that were committed to benefit that entity or that represent its purpose. In such instances, courts may fine an entity up to five times the amount mandated for a single person, ban it from operating for up to five years, or dissolve it. This could allow authorities to disrupt the work of entities such as businesses, civil society groups, and news media, or even shut them down entirely.

Article 34 allows authorities to prosecute Tunisian citizens abroad for crimes under Decree-Law 2022-54, as well as foreign nationals abroad who are accused of crimes under the Decree-Law that "were committed against Tunisian parties or interests."[10] Thus, for example, a tweet by a Tunisian living abroad or a news report by a foreign journalist could trigger prosecution on the charge of spreading "fake news" as set out in Article 24 of the Decree-Law.[11]

Broad powers to track internet use and eavesdrop on communications

Decree-Law 2022-54 grants authorities overly broad powers to monitor people's use of digital networks, collect personal data, and share that information with foreign governments. It also forces telecommunications providers - such as internet and phone companies - to store customers' personal data en masse so that authorities may access them. Sweeping

---

[6] Human Rights Committee, General Comment 34, Sections 24, 25.

[7] "Joint Declaration on Freedom of Expression and 'Fake News', Disinformation, and Propaganda", by the UN Special Rapporteur on Freedom of Expression and Opinion, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, *FOM.GAL/3/17*, Section 2a. 3 March 2017, available at: https://www.osce.org/fom/302796

[8] Human Rights Committee, General Comment 34, Section 38.

[9] "Joint Declaration on Freedom of Expression and 'Fake News', Disinformation, and Propaganda", *FOM.GAL/3/17*, Section 2a. 3 March 2017, available at: https://www.osce.org/fom/302796

[10] Decree-Law 2022-54, Article 34

[11] Article 34 also cites the possible extradition to Tunisia of people abroad who are accused of crimes under Decree-Law 2022-54, stating that "[e]xtradition will take place according to the procedures in force, in accordance with the Code of Criminal Procedure and taking into account conventions concluded to that end."

powers of surveillance such as these threaten the right to privacy and risk undermining the exercise of freedom of expression.[12]

State surveillance powers make it harder for journalists, human rights defenders, and whistle-blowers to keep their communications confidential.[13] Fear of surveillance may also dissuade people from using telecommunications networks to communicate or seek news and information.[14]

Article 9 empowers prosecutors, investigate judges, and certain members of judicial police to order government agents to collect data from telecommunications providers showing records of their customers' online activity, seize and analyse computer systems and other devices, and monitor telecommunications use in real-time, all on the grounds that such actions "might help to reveal the truth" about suspected crimes.

Article 10 allows judicial authorities overseeing a criminal investigation to authorize the interception of communications of "suspects" that they deem "necessary to the investigation."[15]

Article 17 of the ICCPR guarantees protection from "arbitrary or unlawful interference" in personal privacy. According to official guidance on Article 17 by the HRC, any state interference in personal privacy must be provided by law "specify[ing] in detail the precise circumstances in which such interferences may be permitted."[16] The UN High Commissioner for Human Rights (OHCHR) has stated that "vague and overbroad justifications" for digital surveillance fail to satisfy that requirement, and that "[s]urveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted."[17]

Article 6 of the Decree-Law states that telecommunications providers must store the personal data of their customers, including data showing their customers' identities, network traffic, devices, and physical locations, for at least two years. Providers who fail to do so face a year in prison and fine of 10,000 Tunisian Dinars (around 3,000 USD / 3,000 Euros), under Article 27. Article 11 compels providers to let authorities access customer data as authorized by judicial orders.

According to the OHCHR, laws forcing telecommunications providers to store customers' personal data indiscriminately "for extended periods of time" and hand it over to authorities "exceed the limits of what can be considered necessary and proportionate."[18]

---

[12] In particular, Articles 6, 9, 10, and 35 of Decree-Law 2022-54.

[13] UN Special Rapporteur on freedom of opinion and expression, "Reinforcing media freedom and the safety of journalists in the digital age," *A/HRC/50/29,* 20 April 2022, Sections 47 and 53, available at: https://www.digitallibrary.un.org/record/3973716?ln=en

See also: La Rue, Frank, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," *A/HRC/23/40*, Sections 52, 79, 17 April 2013, available at: https://www.digitallibrary.un.org/record/756267?ln=en

[14] The UN Special Rapporteur on freedom of opinion and expression has noted that restrictions on anonymity in using digital networks "have a chilling effect, dissuading the free expression of information and ideas." See La Rue, Frank, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," *A/HRC/23/40,* Sections 47 - 49, 17 April 2013, available at: https://www.digitallibrary.un.org/record/756267?ln=en

See also: UN High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," *A/HRC/27/*37, Sections 18 – 20, 30 June 2014, available at: https://www.digitallibrary.un.org/record/777869?ln=en

[15] Article 10 of Decree-Law 2022-54. Under Tunisian law, investigative judges have wide authority to direct investigations by police into alleged or suspected crimes.

[16] Human Rights Committee, General Comment 16, Sections 3, 8

[17] UN High Commissioner for Human Rights, "The right to privacy in the digital age," *A/HRC/39/*29, Section 35. 3 August 2018, available at: https://digitallibrary.un.org/record/1640588?ln=en

[18] UN High Commissioner for Human Rights, "The right to privacy in the digital age," *A/HRC/39/*29, Sections 18, 61. 3 August 2018, available at: https://digitallibrary.un.org/record/1640588?ln=en

Moreover, such laws increase the risk of human rights abuses simply by allowing for more state surveillance, while leaving personal data in danger of theft or leaking by accident.[19] The UN General Assembly has called on governments "[t]o refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way."[20]

Article 35 of the Decree-Law allows unspecified "specialized authorities" to share personal data they collect with "their counterparts in other countries…." The article states that such data sharing is based on commitments by foreign governments to keep data confidential and to use it only to combat crimes identified by the decree-law. However, the decree-law fails to set clear conditions on data-sharing to ensure that it complies with international human rights law.

The OHCHR has noted that multiple threats to human rights may arise when governments share digital surveillance data with one another. Governments might help one another evade their own national laws by spying on one another's citizens, or share information obtained in violation of international law.[21] The OHCHR has called for agreements between governments on combating cybercrime to include strong provisions to ensure that they cannot be abused to violate human rights.[22]

Inadequate Human Rights Safeguards and Oversight Mechanisms

Any law that allows authorities to impose restrictions on human rights must contain provisions to ensure that such restrictions are themselves provided by law, and that they are strictly necessary and proportionate to achieve a legitimate end.

In light of this, surveillance practices must be governed by adequate safeguards to prevent abuse and ensure that they remain lawful. These safeguards should include a human rights-compliant legislative framework that provides for effective independent oversight.[23] It is well-established that where such safeguards are lacking, the mere threat of surveillance may create a chilling effect on the exercise of human rights even amongst those who may not themselves have been targeted.[24]

---

[19] LaRue, Frank, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," *A/HRC/23/40,* Section 67. 17 April 2013, available at: https://digitallibrary.un.org/record/756267?ln=en

[20] United Nations General Assembly, "The right to privacy in the digital age," *A/RES/75/176*, Section 7, para-M. 28 December 2020, available at: https://www.digitallibrary.un.org/record/3896430?ln=en

[21] UN High Commissioner for Human Rights, "The right to privacy in a digital age," *A/HRC/39/*29, Section 21. 3 August 2018, available at: https://www.digitallibrary.un.org/record/1640588?ln=en

[22] UN High Commissioner for Human Rights, "Key messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes," Section 4. 17 January 2022, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

[23] UN High Commissioner for Human Rights, "The right to privacy in a digital age," *A/HRC/39/*29, Sections 26 - 41. 3 August 2018, available at: https://www.digitallibrary.un.org/record/1640588?ln=en

In a 2020 resolution, the UN General Assembly called on governments to protect the right to privacy through measures including "independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms" for state surveillance of communications and personal data. See United Nations General Assembly, "The right to privacy in the digital age," *A/RES/75/176*, Section 7, paras C, D. 28 December 2020, available at: https://www.digitallibrary.un.org/record/3896430?ln=en

[24] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age, A/HRC/27/37*, para 20. 30 June 2014, available at: https://www.digitallibrary.un.org/record/777869?ln=en

See also: UN Special Rapporteur on freedom of expression and opinion, "Reinforcing media freedom and the safety of journalists in the digital age," *A/HRC/50/29*, paras. 47, 53. 20 April 2022, available at: https://www.digitallibrary.un.org/record/3973716?ln=en

Decree-Law 2022-54 provides for a degree of judicial control over its enforcement by mandating prosecutors and investigative judges to approve digital surveillance and data collection.[25] However, Article 9 also empowers certain members of the judicial police to order data collection, seizure of devices, and monitoring of internet traffic based on written authorization from an unspecified and thus ambiguous source.

In addition, the decree-law fails to set clear limits and conditions on why, when, and for how long those authorities may order digital surveillance and data collection to ensure that such measures do not violate human rights. It does not specify that such measures are permitted only when strictly necessary and proportionate to addressing a serious suspected crime or threat for which clear evidence exists. Nor does it provide for any mechanism of independent review and oversight.

While Article 3 of the decree-law states that the Code of Criminal Procedure and Military Code of Justice both apply, where relevant, to enforcement of Decree-Law 2022-54, those laws similarly grant judicial authorities overly broad leeway to authorize evidence gathering in criminal investigations.[26] Article 3 also states that Tunisia's penal code, child protection law, and unspecified "special penal texts" apply to the enforcement of the decree-law, where relevant.[27] Neither the penal code nor the child protection law addresses digital surveillance and data collection by authorities.

The OHCHR and UN Special Rapporteur on freedom of expression have stressed that laws governing digital surveillance must establish mechanisms for independent authorization and oversight, and require that surveillance meet standards of necessity and proportionality in line with international human rights law.[28] As the Special Rapporteur has noted, even judicial authorization of surveillance can become a "de facto arbitrary approval of law enforcement requests" in states where "the threshold required to be established by law enforcement is low."[29]

Background

On 25 July 2021, President Saied dismissed the prime minister and suspended parliament, claiming emergency powers he said were granted to him by the constitution. On 22 September 2021, he issued Presidential Decree 2021-117, suspending most of the constitution, granting himself the right to rule by decree, dissolving a body to vet the constitutionality of laws, and barring anyone from overturning decree-laws.

---

[25] Decree-Law 2022-54, Articles 4, 9, and 10. The Arabic version of Article 4 refers to "permissions" (أذون), while the official French version of the Article refers more explicitly to "judicial orders."

[26] Article 97 of the Code of Criminal Procedure empowers investigative judges to authorize the seizure of any papers or other effects that might help "reveal the truth" about a suspected crime. Similarly, Article 99 empowers them to authorize the seizure of any correspondence or other sent item that they believe might help "reveal the truth" about a suspected crime. These provisions also apply to investigative judges in military courts under Article 24 of the Military Code of Justice, as amended by Decree-Law 2011-69. And thanks to their overly broad terminology, they fail to impose adequate conditions of necessity and proportionality on digital surveillance and data collection under Decree-Law 2022-54.

[27] Decree-Law 2022-54 does not define the "special penal texts" cited in Article 3. In any case, it is worth noting that key laws relating to personal data and digital surveillance - specifically, Organic Law 2004-63 on the protection of personal data, Decree 2013-4506 creating the Agence Technique des Télécommunications, and Organic Law 2015-26 on fighting terrorism - do not sufficiently define and limit the nature, scope, and duration of surveillance and data collection carried out under their provisions to ensure that these measures do not violate international human rights law.

[28] UN High Commissioner for Human Rights, "The right to privacy in the digital age," *A/HRC/39/2*9, Sections 39, 40. 3 August 2018, available at: https://digitallibrary.un.org/record/1640588?ln=en

Examples of international standards on digital surveillance and data collection include authorizing such measures only against people reasonably suspected of committing or having committed a serious crime; subjecting authorization to independent oversight; and barring digital surveillance and data collection from violating the confidentially of certain privileged communications, notably between lawyers and their clients. See UN High Commissioner for Human Rights, "Key messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes," Section 3. 17 January 2022, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

[29] LaRue, Frank, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," *A/HRC/23/40*, Par 56. 17 April 2013, available at: https://digitallibrary.un.org/record/756267?ln=en

Since then, Saied has issued further decrees to dissolve the High Judicial Council, an independent judicial oversight body, and grant himself powers to intervene in the functioning of the judiciary, to dismiss judges summarily, to mandate prison terms ranging from ten years to life for the spread of "fake news" about the economy in certain circumstances, and to dissolve parliament.[30]

On 25 July 2022, voters approved a new constitution by referendum, following a drafting process carried out behind closed doors and overseen by the president. The new constitution, which went into effect on 17 August 2022, grants the president largely unchecked power to rule, and contains provisions threatening human rights.[31] It grants the president the final word on judicial appointments based on recommendations from judicial oversight bodies as yet to be created. That oversight role is currently filled by the Temporary High Judicial Council, a new judicial oversight body created by decree by President Saied, which is partly appointed by the president and in whose work he or she may intervene.[32]

Tunisian authorities have targeted high-profile critics and perceived enemies of President Saied with measures including arbitrary travel bans, arbitrary house arrest, and criminal investigations and prosecutions for publicly criticising of authorities - including of civilians by military courts.[33]

[30] Decree-Law 2022-11, Decree-Law 2022-35, Decree-Law 2022-14, and Presidential Decree 2022-309

[31] Notably, article 96 of the Constitution grants the President sweeping, open-ended emergency powers, devoid of any mechanism of independent review. Article 5 of the Constitution commits the state to "achieving the purposes of Islam in preserving life, honour, wealth, religion, and freedom." While the Article stipulates that it be carried out "within the framework of democracy," its ambiguous terminology could allow authorities to cite it as grounds for infringing on human rights.

[32] Constitution of Tunisia, 2022, Articles 119 and 120, and Decree-Law 2022-11, Articles 3, 4, 5, 6, 8, and 19

Moreover, the President also has final say over the appointments of judges and prosecutors to military courts, as stipulated by Article 2 of Decree-Law 2011-70, amending Tunisia's Military Code of Justice.

[33] Amnesty International, "Tunisia: A year of human rights regression since president's power-grab". 21 July 2022, available at: https://www.amnesty.org/en/documents/mde30/5876/2022/en/