



Briefing paper: New Anti-Cybercrime law in Libya exacerbates the phenomenon of impunity

Tunis, 16 November 2022 - The Libyan Anti-Torture Network (LAN) and the World Organisation Against Torture (OMCT) express their concern over the provisions of the new [Anti-Cybercrime law](#) which will significantly contribute to the exacerbation of impunity in Libya, and will put human rights defenders working in and on the country at further risk.

Law No.5/2022 on *combating cybercrime* issued on September 27th, enables the [National Information Security and Safety Authority](#) to impose full control over all data and information posted on the Internet and on all other electronic and technical systems. The law enables the Authority to conceal, withhold, and block what it described as “*strife*” or “*ideas that undermine society’s security, stability and social peace*” without specifying what these expressions in this ambiguous and interpretable legislation mean, leaving its interpretation to the members of the Authority and the House of Representatives.

Anti-Cybercrime law drafted without consultation and in violation of basic human rights

Libyan citizens became aware of this new Anti-Cybercrime law when a copy of the draft was accidentally leaked in October 2021 on social media. Throughout the whole process of its development, the legislators working on the draft law did not consult with any relevant actors of civil society or the legal community and did not give prior knowledge of it to the Libyan public. Additionally, the Government’s total disregard for the Libyan civil society during the process of introducing, passing, and ratifying the new law constitutes a violation of the most important human rights, namely the right to knowledge, the right to access information, and especially the right to equality among citizens by being aware of the draft law and taking the initiative to consult on their rights contained [therein](#).

This law restricts basic rights such as freedom of opinion and expression, the right to freedom of peaceful assembly and association, and the right to obtain, receive, and hold information relating to human rights as outlined in the UN [Declaration on Human Rights Defenders](#)’ provisions. Hence, based on this legislation, repressive security and government agencies in Libya, including the National Information Security and Safety Authority, are allowed to violate the privacy of vulnerable individuals and communities as well as to impede the work of human rights defenders who use the Internet and social media to monitor, collect and share information about human rights violations committed by state and non-state actors in the country.

Criminalisation of encryption and jeopardization of documentation in Libya

Law No.5/2022 challenges the principle of confidentiality in dealing with information concerning victims of violations of international law in Libya, especially considering the continuing political, security and military instability. Articles 9 and 39 of this law criminalise the possession and use of encryption methods, thus exposing victims of torture, ill-treatment, and all other forms of crimes that undermine the right to life, the right to liberty and the right to protection against the threat of surveillance, restriction, and prosecution to reprisals. In the absence of justice within Libya, safe digital communication is vital between victims of violations and those who report them, as well as between civil society organisations, human rights defenders and international mechanisms concerned with the documentation of human rights violations.



As emphasized by the 2020 [Joint Declaration on Challenges to Freedom of Expression](#) by the United Nations Special Rapporteur on Freedom of Opinion and Expression, States must "*refrain from using arbitrary or unlawful restrictions on the use of encryption and anonymity techniques*" in the next decade. Law No.5/2022 is therefore incompatible with the provisions of the Declaration as it restricts the use of all electronic platforms and websites by imposing unrealistic standards on their users such as obtaining licenses or permits from the National Information Security and Safety Authority to be able to use encryption methods.

Advocacy activities carried out by human rights defenders and CSOs including online publication and dissemination of reports, and online information sharing about human rights violations via websites, digital media, and social media, are the only option left to denounce the crimes committed in Libya in a context of total closure of the civic space. In this context, the authorities' monitoring of digital content and data as well as the threat of being blocked from using online platforms puts the right to defend human rights in Libya at further risk, and muzzles thousands of victims of human rights violations, who use the online space to seek accountability. The human rights holders and the human rights defenders will undoubtedly be silenced, intimidated, excluded and prosecuted, especially since many of the perpetrators belong to the government itself.

The principle of confidentiality which protects victims, witnesses, families, lawyers, human rights defenders, judges, forensic doctors, and others, on which the success of monitoring, documentation, case-building, and litigation is based, is challenged through this law. Suppressing the possibility of sharing data through safe and encrypted platforms exacerbates the lack of accountability and total impunity for serious human rights violations committed by state and non-state actors in Libya against Libyan citizens and migrant individuals.

Possibility of subjective interpretation of the text of the Law

The use of vague and ambiguous language opens the door to a broad interpretation of the law and allows the Authority and the government to which the Authority is affiliated to misuse the law, notably to target victims of human rights violations, and human rights defenders and organisations.

- Article 4 of the law states that "*the use of the World Wide Web and modern technology is legitimate unless it results in a violation of public order or public morals.*"
- Article 7 enables the National Information Security and Safety Authority to "*block everything that spreads strife or ideas that undermine society's security, stability and social peace*" without clearly defining the meaning of "*society's security, stability and social peace.*"
- Article 8 requires the same body to block websites or web pages that display "*immoral/indecent*" material.

The legislator left the interpretation of the meaning of these undefined terms such as "*public order*" or "*public morals*" to the Authority. Which in turn gives it freedom to interpret anything that is contrary to the ideas of its members and the ideologies and objectives of the Government heading it, leaving whatever action in conflict with this unclear loose interpretation of provisions a punishable crime. This will create a legal loophole allowing arbitrary unlawful practices of restraint, subversion, harassment, and prosecution against every citizen according to the law.

What may result from the application of this new legislation is the return of dictatorial, repressive and arbitrary government practices that breach international human rights standards relating to the restriction of the right to freedom of opinion and expression and the freedom from fear, as these provisions must be "*formulated precisely enough to enable an individual to control his or her conduct*"



accordingly", as stipulated in the Human Rights Council's [General comment No. 34 on article 19](#) of the [International Covenant on Civil and Political Rights](#) ratified by Libya since 15 May 1970. This legislation also contradicts Article 19 of the International Covenant on Civil and Political Rights in its second paragraph, which states that "*everyone has the right to freedom of expression. This right includes freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, whether in writing, in print, in artistic form or by any other means of his choice.*"

In conclusion, these measures raise the level of danger and vulnerability and increase the likelihood and possibility of targeting human rights defenders, journalists, media professionals and victims of human rights violations in Libya, who are victims of systematic arbitrary arrests, threats, and violence. In this environment, the new Anti-Cybercrime law may be instrumentalised by the authorities and armed groups affiliated with the government to further crackdown on civil society and make impunity chronic in the country. Law No.5/2022 represents a new tool that enables perpetrators to prevent rights defenders from carrying out their human rights work, including supporting victims and exposing violations and crimes committed by militias and state armed groups by making access to information impossible, creating a clear barrier to the disclosure of evidence and essential documents that are important for the rule of law, exacerbating impunity, and allowing a greater number of violations to be committed.

The Libyan Anti-Torture Network and the World Organisation Against Torture call on:

1. All concerned Libyan governmental authorities, led by the House of Representatives, to review the provisions of this law and amend it in a manner that guarantees the protection of the rights to freedom of opinion and expression offline and online, the freedom from fear, and the right to defend human rights, in accordance with international human rights standards. The law must ensure the confidentiality of digital interactions and users' privacy, especially since many Libyans who are subjected to violations can only report crimes through encrypted technical means due to insecurity and lack of access to justice inside Libya
2. The concerned Libyan authorities to strip the National Information Security and Safety Authority of any powers that give it the right to withhold or block access to information or give licenses and permits for digital encryption in all its forms to any parties.
3. The UN Special Rapporteurs on freedom of expression and human rights defenders, to demand the Libyan authorities to significantly amend the Anti-cybercrime law to ensure the right to freedom of expression offline and online, and the right to defend human rights are duly protected in accordance with international human rights standards; the international mechanisms concerned with monitoring the human rights and humanitarian situation in Libya, the United Nations Security Council, to demand that the Libyan governments and authorities retract the enforcement of this law and possibly propose a change to the law so that its provisions guarantee digital protection for citizens, victims, civil society, journalists, activists and the general public, and allows the secure use of encryption.

OMCT Libya

Khaled Salem

Head of OMCT Libyager

kms@omct.org

Sahar Ben Hazem

Communications & Advocacy Officer

sab@omct.org