Summary of the Military's Changes to the Electronic Transactions Act on 15 February 2021

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

May 2021

On 15 February 2021, the military introduced new amendments to the Electronic Transactions Act (ETA). This Summary explains the amendments and highlights why they do not comply with international human rights standards.

Protection of Personal Information

New Provisions:

- Persons managing personal information now have obligations to protect such information. However, there are major exceptions to these requirements:
    - When agencies are preventing, investigating or submitting evidence about cybersecurity, cyberattacks and other cyber incidents
    - When agencies are investigating or prosecuting a criminal case
    - For any investigations, data collection and coordination about cybersecurity or cybercrime issues related to state sovereignty, public order or national security
- Personal information managers who fail to manage personal data properly commit a criminal offence. *Anyone* who obtains, discloses, uses, destroys, modifies or disseminates the personal data of another without approval also commits an offence.
    - The penalty for both offences is 1-3 years in prison and/or a fine.

International Human Rights Law: Proper data protection regimes are important for guaranteeing the right to privacy, the right to freedom of expression and the rights of criminal defendants. These new provisions do not constitute a proper data protection law:

- The obligations are vague and unlikely to be implemented without specifics. Crucial elements, such as an independent oversight system, are absent.
- The exceptions are sweeping. They may offer legal cover for problematic surveillance, such as collecting data about civil society, journalists and activists.
- The crime of disclosing personal information without consent is too broad. It could punish those who accidently share private information, or be used to target journalists who disclose information about members of the military or other public figures.

Misinformation and Disinformation

New Provisions: Creating misinformation or disinformation with the intent to cause public panic, loss of trust or social division on a cyber space is a crime. The penalty is 1-3 years imprisonment and/or a fine.

International Human Rights Law: Laws prohibiting disinformation restrict freedom of expression. Restrictions on freedom of expression can only aim to protect one of the following: national security, public order, the rights or reputations of others, or public health and morality. False information should only be prohibited when it may cause a specific harm to one of these aims. This harm needs to be clearly and precisely defined: a vague reference to "national security" is not specific enough. Such laws should also only punish those who know the information is false and share it with the intent to cause harm.

The ETA does not comply with these standards. It lacks definitions of "misinformation" or "disinformation" and does not target a specific harm. While it requires an intent to cause public panic, loss of trust or social division, these concepts are too vague. They do not require a specific intent to cause harm by creating information which the person knows is false.

Cyberattacks and Cyber Violence

New Provisions: Two new provisions criminalise certain cyber offences:

- "Cyber violence" is not defined, but includes acts "such as" restricting access to a website and accessing more information than one is permitted to access.
    - There must be an intent to threaten or disturb national sovereignty, security, peace and stability, rule of law and national solidarity.
    - The crime is punished by 2-5 years in prison and/or a fine.
- Cyberattacks are defined as online actions to threaten national sovereignty, security, peace and stability, rule of law and national solidarity. They include acts "such as" unauthorised access to confidential information or using more access than allowed.
    - There must be an intent to harm foreign relations or support foreign interests.
    - The punishment is 3-7 years in prison and/or a fine.

International Human Rights Law: Cybercrime laws should clearly define what acts they prohibit and establish precise intent requirements. They should focus on attacks to computer systems or misuse of computer systems, not on policing online speech.

Cyber violence and cyberattacks under the ETA are highly unclear. Only examples of such acts are given, not a clear list of prohibited acts. The intent requirements are far too general, focused on ambiguous concepts like disturbing national solidarity. Such vagueness does not meet criminal justice standards. It also risks criminalising behaviour that should be protected by human rights law, such as reporting on sensitive information or online speech deemed to constitute "cyber violence".