Egyptian Parliament approves Cybercrime Law legalizing the blocking of websites and full surveillance of Egyptians – مؤسسة حرية الفكر والتعبير

The Association for Freedom of Thought and Expression (AFTE) and Access Now condemn the Egyptian Parliament's approval of the *Law on Combating Cybercrimes* ("Cybercrime Law"), which provides new authority for online surveillance, blocking of websites, and monitoring of internet users and the use of communications services in Egypt. Approval of this draft is in line with a series of rights-harming laws the Parliament has approved since its election in 2015, most notably the Law of Civil Associations (1, 2), the Law of Institutional Regulation of the Press and Media, and the Protest Law. These laws serve to close space for civil society and deprive citizens of their rights, especially the right to freedom of expression and of association.

Background

The Cybercrime Law has a total of 45 articles. The final draft for the law was submitted by the government and approved by Parliament on 5 June 2018. The law had been discussed in the Communications and Information Technology Committee, which approved it in principle on 5 March 2018. Debate of the law had been preceded by several attempts at passage over the past three years, including a draft prepared by the Ministry of Justice in March 2015 and another draft submitted by MP Tamer Chehawi in May 2016. The law, after passing in parliament, requires the President's signature to enter into force. However, if the president fails to sign it within 30 days, it is automatically entered into force.

What's in the law

Article 7: Censorship

This law legalizes broad censorship of the internet and enables executive authorities to block websites, a practice that Egyptian authorities have been employing since 24 May 2017. To date, the number of blocked sites in Egypt has reached at least 500. Article 7 of the Cybercrime Law gives the investigative authority the power to order a website blocked whenever it deems the content to constitute a crime or a threat to security, or a danger to national security or the economy. The investigative authority submits its blocking order to a competent court within 24 hours, and the court issues its decision within a period not exceeding 72 hours, either accepting or rejecting the order. Article 7 effectively legalizes the blocking of websites. After the passage of this law, authorities can safely rely on Article 7 to censor content online.

In addition to authorizing investigatory authorities to order the blocking of websites, Article 7 also grants security authorities this power, with the ability to order the National Telecom Regulatory Agency (NTRA) to implement the decision by telling internet service providers (ISPs) to block a website, link, or specific content. Article 7 obliges ISPs to execute an order as soon as it is received, in "an urgent manner due to imminent danger or damage." This is at the discretion of the security authority, not subject to any criteria that would prevent arbitrary abuse of this power. The security investigators ordering a block must then, within 48 hours,

present the decision — after it has already been implemented — to competent investigative authorities, who in turn present it to a competent judicial authority within 24 hours. The court then issues its decision within 72 hours, either approving or rejecting the decision.

This means that intelligence bodies have greater authority than the investigative authorities, whose decisions are neither valid nor executed except upon a judicial decision by the competent court.

Broad and vague provisions, open to abuse

The reasons articulated in the Cybercrime Law for blocking websites are vague and broad. For example, the law defines national security as "all that is related to the independence, stability, and security of the homeland and its unity and territorial integrity," and all affairs "related to the Presidency of the Republic, the Defense Council, the National Security Council, the armed forces, military production, the Ministry of Interior, the General Intelligence, the Administrative Oversight Authority, and the organs affiliated with those bodies." Investigative bodies have used these same broad, vague grounds for launching cases against demonstrators and activists (accusing them of calling for demonstrations, publishing crimes, such as in Case 173 against civil society organizations). The failure to clearly define the terms for violating the law means that authorities could misuse or abuse the law to censor what they see as contrary to their policies, justifying censorship as a way to protect national security.

Article 2: Data retention and surveillance

In addition to authorizing broad censorship, this law facilitates comprehensive surveillance of communications. Article 2 requires telecommunications companies to retain and store users' data for 180 days. This includes data that enables the identification of users, "metadata" about the content of their communications, the computer "IP" address, and the devices they use. This means that telecom providers could be asked to turn over to authorities detailed information about users' communications, including information on voice calls, text messages, website visits, and the use of apps on computers and smartphones. The same article requires that telecommunications companies comply with regulations for any "other data decided by the NTRA board," which means that companies could be forced to collect and retain data not provided for in the law, based on a decision by the NTRA. The article also expands the legality of telecommunications service providers to collect user data, extending it to the agents and distributors responsible for marketing their services.

In addition, Article 2 gives national security authorities the right to access these data, and telecommunications service providers are obliged to offer the technical assistance necessary to facilitate such access. The law states, "service providers and their subordinates shall, when requested by the national security authorities and in accordance with their needs, provide them with all available technical facilities that allow them to exercise their powers in accordance with the law."

In other words, instead of linking the monitoring of communications to permission by investigating bodies in specific crimes and for a specific period, the law provides security services with extensive powers to obtain user data, without limitation or standards.

This article violates the provisions of the Egyptian Constitution, which prohibits the monitoring of the means of communication without a specific judicial order and without a specified period of time. Article 57 of the Constitution stipulates that, "The right to privacy may not be violated, shall be protected and may not be

infringed upon. The State shall protect citizens' right to use all forms of public means of communications. Interrupting or disconnecting them, or depriving the citizens from using them, arbitrarily, is impermissible. This shall be regulated by Law."

AFTE and Access Now stress our rejection of this large-scale, comprehensive collection of the personal data of citizens. Already, Egyptians are suffering from having to disclose their personal data in their normal daily practices. Over the past year, AFTE has monitored several cases, in which some distributors have used the personal data of users without their knowledge, including in the sale of mobile phone lines, which resulted in many cases of hacking personal social media and email accounts. Due to the growing use of ICT in business and financial transactions, all related services are thus endangered, as well as subjecting users to prosecution in case any telecommunication service is used to commit a crime punishable by law.

Article 4: Access to personal data by other governments

The law also enables violations of the right to privacy of Egyptians by other governments. Article 4 of the law addresses the exchange of data and information between Egypt and foreign countries through the Ministries of Foreign Affairs and International Cooperation within the framework of international, regional, and bilateral agreements or the application of the principle of reciprocity. The article does not include any requirements for the exchange of such information, such as the existence of data protection laws in the requesting country or requirements regarding the scope, duration of retention, or processing of information.

General vagueness in definitions and purpose

The provisions of the law are characterized by vagueness, which allows the possibility of extending the penalties of the law to any ordinary act that is perceived to be contrary to the policies of Egyptian authorities. For example, the first article of the law defines the terms contained therein, most of which are quite broad and vague. The term "national security" is defined as "all that relates to the independence, stability, security, unity and territorial integrity of the homeland, including those that are not defined, such as endangering the security of the country and its national economy, as mentioned in Article 7 of the law."

Similarly, the law does not specify what is meant by "public morals," mentioned in Article 27. In the same vein, Article 35 — which introduces charges that are often used as the basis for accusations against political protesters and activists, in investigations or trials — aggravates the penalty if the crime "is committed for the purpose of disturbing public order, endangers the safety and security of society, prevents or obstructs the exercise by public authorities of their mandates, disrupts the provisions of the Constitution, laws or regulations, or harms national unity and social peace." None of these terms are defined in the law, and as such, authorities have leeway to prosecute legal speech using obscure terms that have no specific meaning. The terms "family principles or values" is also used in Article 25, without specifying what these principles and values are; these are again the same terms authorities have previously used to censor advertisements, delete scenes from series and movies, and ban television programs.

Media and publications law is also dangerous

Another law approved by the Egyptian Parliament increases the threat to free expression. On 10 June 2018 the parliament approved a law regulating the press and the media , Article 19 of which stipulates that the Supreme Council for Media Regulation shall impose sanctions on those with a personal website, blog or online

account, with 5,000 or more followers, for the publication or dissemination of false news, incitement to or violation of the law, violence or hatred, discrimination against citizens, racism, intolerance or defamation of individuals, or insult to divine religions or religious beliefs. This article makes it evident that the parliament is attempting to establish a system for comprehensive monitoring of online accounts, blogs, and personal sites, and to enable the Supreme Media Council — whose bylaws do not include this authority — to prosecute citizens who express their views using the internet.

The Cybercrime Law must be withdrawn

Access Now and AFTE call for the immediate withdrawal of the *Law on Combating Cybercrimes* in order to preserve the rights of Egyptian citizens in online expression, privacy, and access to information. The law will increase the frequency of curtailing of freedom of expression in the digital space and expose internet users to the dangers of imprisonment due to normal use of means of communication. The law also restricts media freedom, as the internet has become the primary medium for news circulation. We also call on Egyptian authorities to cease any practice that restricts digital rights, to lift the block on hundreds of websites, and immediately release detainees who have been incarcerated for online expression of their views.