December 13, 2023

LEGAL ALERT

National Congress approves the Bill that establishes a Framework Law on Cybersecurity

On December 12th, 2023, the Chamber of Deputies approved in the second constitutional procedure the bill that "Establishes a Framework Law on Cybersecurity and Critical Information Infrastructure" (the "Bill"). On the same date, the Bill was sent to the Senate and advanced to the third constitutional stage, with all the amendments of the reviewing chamber being approved. Thus, the Bill will be sent to the President of the Republic for its promulgation, without prejudice to the preventive control to be carried out by the Constitutional Court.

The main objectives of the Bill are to establish the institutionality, principles and general regulations to structure, regulate and coordinate the cybersecurity actions of State bodies and between them and individuals, as well as to establish the requirements for the prevention, containment, resolution and response to cybersecurity incidents and cyberattacks.

The Bill involves a series of relevant aspects and changes in cybersecurity matters. Some of these are highlighted below:

It creates a new institutionality

The Bill contemplates the creation of new institutions in cybersecurity matters, providing for the creation of the National Cybersecurity Agency ("ANCI"), the Multisectoral Council on Cybersecurity, the Interministerial Committee on Cybersecurity and different Computer Security Incident Response Teams ("CSIRT")"), including the National Computer Security Incident Response Team, the National Defense Computer Security Incident Response Team and the other CSIRTs belonging to State Administration Bodies.

Regarding to the ANCI, this authority will be responsible, among other things, for advising the President of the Republic on cybersecurity matters, collaborating in the protection of national interests in cyberspace, coordinating the actions of the institutions with competence in cybersecurity

matters, ensuring the protection, promotion and respect for the right to computer security, and coordinating and supervising the actions of State Administration Bodies in cybersecurity matters. To fulfil its functions, the ANCI will have regulatory, supervisory and sanctioning powers.

As an example, among other attributions, the ANCI is given the competence to "dictate the protocols and standards set forth in article 7" and "the general and particular instructions, of a mandatory nature, for both public and private institutions bound by this law" (regulatory powers); the power to "oversee compliance with the provisions of this law, its regulations, protocols, technical standards and the general and particular instructions issued by the Agency [...]" (supervisory powers); and the power to "instruct the initiation of sanctioning procedures and sanction infractions and non-compliances incurred by the institutions bound by the present law [...]".

The Bill also provides for regulatory coordination mechanisms between the ANCI and sectoral entities in the event that the protocols, technical standards or general instructions it issues in the exercise of its functions have effects in the areas of competence of such sectoral entities. Sectoral authorities may also issue general regulations, technical standards and instructions necessary to strengthen cybersecurity of institutions of their sector, in accordance with the respective regulation and in coordination with ANCI.

It establishes principles in cybersecurity matters

The Bill introduces several principles that obligated institutions must observe in their conduct. Among the principles included in the Bill, it is possible to highlight the following:

- Principle of damage control. This principle requires that, in the event of a cyberattack, or cybersecurity incident, coordinated and diligent action must be taken, adopting the necessary measures to prevent the escalation of the cyberattack or cybersecurity incident and its possible spread to other computer systems.
- Principle of cooperation with authority. In application of this principle, cybersecurity incidents should be resolved through appropriate cooperation with the competent authority and, if necessary, cooperation between different sectors, taking into account the interconnectedness and interdependence of systems and services.
- Principle of responsible response. Under this principle, the implementation of measures to respond to cybersecurity incidents or cyberattacks shall in no case involve the conduct of, or support for, offensive operations.
- Principle of computer security. This principle requires that everyone has

the right to adopt the technical measures of computer security that deems necessary, including encryption.

- Principle of reasonableness. In application of this principle, measures for cybersecurity incidents management, cybersecurity obligations and the exercise of the ANCI powers should be necessary and proportionate to the degree of exposure to risk, as well as to the social and economic impact it wou|ld have.
- Principle of security and privacy by default. Under this principle, IT systems, applications, and information technologies must be designed, implemented, and managed with the security and privacy of the personal data they process in mind.

Scope of application: providers of essential services and operators of vital importance

The Bill will apply to institutions providing services qualified as "essential" and those that qualified as "operators of vital importance".

The Bill establishes that essential services are:

- Those that are provided by the State Administration Bodies and by the National Electricity Coordinator, as well as those that are provided under a public service concession; and
- Those that are provided by private institutions that carry out the following activities:
  - Generation, transmission or distribution of electricity;
  - Transport, storage or distribution of fuels; supply of drinking water or sanitation;
  - Telecommunications;
  - Digital infrastructure;
  - Digital services, information technology services managed by third parties;
  - Land, air, rail or maritime transport, as well as the operation of their respective infrastructure;
  - Banking, financial services and means of payment;
  - Administration of social security benefits;
  - Postal and courier services;
  - Institutional provision of health care by entities such as hospitals, clinics, doctors' offices and medical centers;
  - Production and/or research of pharmaceutical products.

The ANCI may qualify other services as essential by means of a reasoned decision of the National Director when their affectation may cause serious damage to the life or physical integrity of the population or its supply, to relevant sectors of the economic activities, to the environment, to the normal functioning of society, of the State Administration, to the national defense, or to the security and public order.

For its part, ANCI will be responsible for determining the providers of essential services that are qualified as operators of vital importance by means of a reasoned decision, that complies with the following requirements: (i) that the provision of such service depends on the networks and information systems; and (ii) that the affectation, interception, interruption or destruction of its services has a significant impact on security and public order; on the continuous and regular provision of essential services; on the effective fulfillment of the functions of the State; or, in general, of the services that the State must provide or guarantee.

Likewise, ANCI shall have the power to qualify private institutions that, although they do not have the quality of providers of essential services, also meet the requirements set forth in the preceding paragraph under certain assumptions.

Security obligations

The Bill distinguishes between duties and obligations of a general nature and those of a specific nature that must be complied with by the entities that are qualified as vital operators.

- General duties for providers of essential services and operators of vital importance.
  - **Obligation to report.** On the one hand, it is provided that all providers of essential services and operators of vital importance will have the obligation to report to the National CSIRT within a maximum period of 3 hours cyber-attacks and cybersecurity incidents that may have significant effects, in accordance with the criteria established by the Bill.
  - **Other obligations.** On the other hand, the Bill also establishes that all obliged institutions must permanently apply measures to prevent, report and resolve cybersecurity incidents, adding that these measures may be of a technological, organizational, physical or informational nature, as the case may be. In addition, it should be noted that compliance with

these obligations requires the due implementation of the protocols and standards established by ANCI, as well as the particular cybersecurity standards dictated in accordance with the respective sectorial regulation, to prevent and manage the risks associated with cybersecurity, containment and mitigation of the impact that the incidents may have on the operational continuity of the service provided or the confidentiality and integrity of the information or of the networks or computer systems.It should be noted that the precise content of these obligations is not fully determined in the Bill and is likely to be specified only by rules issued by ANCI in the future and the respective sectoral authorities, as appropriate.

- Specific Duties for Operators of Vital Importance:

  The Project provides that critical operators are subject to specific duties, among which is the obligation to implement continuous information security management systems; to prepare and maintain operational continuity and cybersecurity plans, which must be certified and subject to periodic reviews; to continuously carry out review operations, exercises, drills and analysis of networks, computer systems and systems; to inform those potentially affected about the occurrence of incidents or cyber-attacks that could seriously compromise their information or computer networks and systems; to appoint a cybersecurity delegate, among other specific duties.

It establishes infractions and associated penalties

The Bill establishes a series of sanctions for infringement of the provisions of the future law. The ANCI will be in charge of sanctioning such infringements, without prejudice to the powers of the respective sectorial authority to know and sanction the infringements, as well as to execute the sanctions, to the regulations on cybersecurity that it has issued and whose effects are at least equivalent to those of the regulations issued by the ANCI.

It should be noted that the Bill classifies infringements into minor, serious and very serious infringements, in addition to establishing specific infringements for operators of vital importance. The following are some of the infringements contemplated in the Bill:

- The following are considered minor infractions: (i) late delivery of the information required when it is not necessary for the management of a cybersecurity incident; (ii) failure to comply with the general or specific instructions issued by ANCI in cases that are not sanctioned as a serious or very serious infraction; and (iii) any infraction of the obligations of the

future law that do not have a special sanction.

- The following are considered serious infractions: (i) failure to implement the protocols and standards established by ANCI to prevent, report and resolve cybersecurity incidents; (ii) failure to implement the particular cybersecurity standards; (iii) late delivery of the information required when necessary for the management of a cybersecurity incident; (iv) delivery to ANCI of information that is manifestly false or erroneous; (v) failure to comply with the reporting obligation; (vi) unjustifiably refusing to comply with an instruction of ANCI or hindering ANCI in the management of a cybersecurity incident; (iv) providing ANCI with manifestly false or erroneous information; (v) failing to comply with the reporting obligation; (vi) unjustifiably refusing to comply with an instruction from ANCI or deliberately hindering the exercise of ANCI's attributions during the management of a cybersecurity incident, provided that the attribution does not have a special sanction; and (vii) the repeated commission of the same minor infraction within a year.
- The following are considered very serious infractions: (i) providing ANCI with manifestly false or erroneous information, when it is necessary for the management of a cybersecurity incident; (ii) failing to comply with general or specific instructions given by ANCI during the management of a significant impact incident; (iii) failing to provide the information required when it is necessary for the management of a significant impact incident; and (iv) the repeated commission of a serious infraction within one year.

As for the amounts, minor infractions will be sanctioned with a fine of up to 5,000 Monthly Tax Units ("UTM"), which can reach up to 10,000 UTM if the offender is an operator of vital importance; serious infractions will be punished with a fine of up to 10,000 UTM, which may reach 20,000 UTM if the offender is an operator of vital importance; and, finally, very serious infractions will be punished with a fine of up to 20,000 UTM, which can reach 40,000 UTM if the offender is an operator of vital importance. As a result, the penalties could amount to almost USD 3,000,000.

Effective Date

The President of the Republic must issue, within one year of the publication of the future law, one or more executive law decrees to determine a period for the entry into force of the rules of the future law, which may not be less than six months from the publication of the future law, the date of initiation of the activities of ANCI, among other matters.

Authors: Guillermo Carey; José Ignacio Mercado; Iván Meleda; Jorge Gatica