Chile: The implications and pending challenges of recent cybersecurity regulations in Chile

Monday 24 July 2023

Felipe Bravo

Carey, Santiago

fbravor@carey.cl

Sebastián Gómez

Carey, Santiago

sgomez@carey.cl

Alfonso Silva

Carey, Santiago

asilva@carey.cl

Introduction

Only a few years ago, we entered the era of the hyperconnected world. This reality has put cybersecurity breaches at the centre of the discussion. They can occur in fractions of seconds, over great distances, and without the need to carry tools or weapons. Today, suffering a cybersecurity attack seems to be only a matter of time.

The cybersecurity phenomenon has been particularly intense worldwide and especially in Chile, which has suffered several publicly known cyberattacks against strategic entities.[1] According to the latest threat report released by cybersecurity company Fortinet's FortiGuard Labs, a data intelligence lab, Chile suffered 14 billion cyberattack attempts in 2022, which represents a 50 per cent increase compared to 2021.

With a view to preventing this scenario, as early as 2017, the Chilean government launched the National Cybersecurity Policy,[2] which set the guidelines of the policies of the State of Chile on cybersecurity matters to work towards a free, open, secure and resilient cyberspace by 2022. Following years of analysis and contributions from the public and private sectors on these guidelines, on 12 March 2022, the President of Chile presented to the National Congress of Chile the 'Framework Law on Cybersecurity and Critical Information Infrastructure' (LCCII).[3]

The purpose of the LCCII is to establish the necessary institutional framework to enhance cybersecurity, expand and strengthen preventive work, create a public culture of digital security, address contingencies in the public and private sectors, and safeguard the security of people in the cyberspace. The LCCII is still under discussion by Congress. Once approved, it would be the main cybersecurity legislation in Chile, establishing general obligations for public and private entities and providing a common legal framework for both existing and new sectoral laws and regulations.

New developments in the LCCII

Under its current status, the LCCII incorporates a series of novel developments in the Chilean legal framework, the most significant ones being the following:

stitutional framework

CCII introduces the creation of new public entities to strengthen the Chilean institutional security framework:

lational Cybersecurity Agency (the 'Cybersecurity Agency') – This Agency would advise the Chilean dent on cybersecurity matters, coordinate the actions of public entities with cybersecurity orities, and organise and oversee the actions of the State Administration's public entities ding cybersecurity matters. In addition, the Cybersecurity Agency will have regulatory, supervisory and sanctioning powers, not only over public entities, but also private entities.

(ii) National Computer Security Incident Response Team (CSIRT) – This entity would integrate the Cybersecurity Agency and would be in charge of responding and preparing for cyberattacks, in coordination with Sectoral CSIRTs, with the aim of contributing to capacity development and the confidence and security of IT networks and systems, as well as providing assistance for cybersecurity management in the respective sectors.

(iii) Multisectoral Council on Cybersecurity – this Council would act as an advisory board of the Cybersecurity Agency, being comprised of the Cybersecurity Agency's Director and six advisers who shall come from the commercial, academic and social sectors.

(iv) Inter-ministerial Committee on Cybersecurity – this Committee would be composed of the Undersecretaries of the most relevant Ministries related to cybersecurity, the Director of the National Intelligence Agency and the Director of the Cybersecurity Agency. Its main function would be to advise the President of the Republic on cybersecurity matters relevant to the functioning of the country.

2. Operators of Vital Importance

Public and private entities providing essential services, determined by the Minister in charge of national security, which meet the following requirements: (i) the operator must provide a service qualified as essential under the LCCII; (ii) the relevant services must depend on networks and computer systems; and (iii) a cybersecurity incident relating to such services would have a disruptive impact on their provision.

The main obligations of Operators of Vital Importance are to:

(i) implement protocols and standards set forth by the Cybersecurity Agency;

(ii) implement an information security management system;

(iii) keep a record of the actions performed in the context of the information security management system;

(iv) continually conduct review operations, drills, exercises, simulations and the analysis of networks and computer systems to detect actions that may compromise cybersecurity;

(v) take expeditious actions to reduce the impact and extent of a cybersecurity incident;

(vi) obtain the corresponding certifications for their information security management systems and processes, as determined by the relevant regulations;

(vii) inform the community of any cyberattacks that could seriously compromise their networks and computer systems;

(viii) provide training and education programs to their employees and collaborators, including cybersecurity campaigns; and

(ix) appoint a cybersecurity delegate.

3. Sanctions

The LCCII sets forth different types of sanctions depending on the entity that infringes the obligations established thereunder. If the infringements are made by a private entity, the entity would be fined in an amount depending on the seriousness of the infraction (up to 20,000 Monthly Tax Units, approximately USD $1,607,700). As for public entities, sanctions would not be applied directly to the entity, but rather to the public officer deemed responsible for the infringement in accordance with its statute of liability.

Pending challenges of the Chilean legal framework on cybersecurity

ugh the LCCII is currently under discussion in Congress and could still suffer modifications, it nts the following challenges, which we believe should be addressed in the pending discussions in ress:

entives to join the Cybersecurity Agency

ybersecurity Agency, along with the National CSIRT and Sectoral CSIRTs, will need to hire the qualified IT experts to comply with its legal mandate. Therefore, the Congress should analyse the possibility of creating incentive mechanisms that would help promote the finding and retaining of talent for these purposes.

Classification of significant incidents

The LCCII establishes which cybersecurity incidents should be considered as relevant for report and for the Cybersecurity Agency and corresponding CSIRTs to take action. However, it does not set forth a classification of significant incidents in accordance with their severity, only providing general criteria to determine their significance.

In this regard, we note that other regulations currently in force in our jurisdiction already classify the severity and impact of threats to cybersecurity. For example, Resolution No 1.328/2020 establishes the general cybersecurity fundamentals for the design, installation and operation of networks and systems used for the provision of telecommunications services, classifying the risks of cybersecurity incidents as Critical, Very High, High, Medium, or Low. This Regulation also establishes a classification of the levels of penetration of such cybersecurity incidents in terms of Critical, Very High, High, Medium, Low, or Without Impact. Accordingly, the obligations that shall be applicable in case of a cybersecurity incident vary depending on the level of risk and penetration of the incident.

Considering the above, we believe that the Chilean Congress should analyse precisions in this regard or establish an express mandate for the LCCII regulation to develop a classification of significant incidents in accordance with the relevant factors.

Issuance of regulations complementary to the LCCII

In Chile, by legislative technique, when a new law is enacted, it contains references to complementary regulations to be issued in the future by specialised government agencies. Thus, the LCCII refers on several occasions to regulations that will be issued in the future by the Ministry of the Interior and Public Safety and by the Ministry of Defence.

However, there have been recent cases in which the referred legislative technique has generated an excessive delay in the application of laws, especially when it comes to highly specialised matters. We believe that this could be one of those cases and, therefore, that the Congress needs to reevaluate which public entities should participate in the elaboration of the complementary regulations to ensure the application of the LCCII. The eruption of new technologies such as artificial intelligence (AI) will require the expertise and efforts of specialised entities such as the Ministry of Transport and Telecommunications (MTT) and the Ministry of Science and Technology (MST).

Ethical hacking

The LCCII introduces an amendment to the law establishing cybercrimes that exempts from criminal responsibility individuals who – in the context of a cybersecurity investigation – access computer systems without the corresponding authorisations and overcoming technical or technological barriers. This is often referred to as 'ethical hacking'.

In order to be exempted from criminal responsibility, such individuals must meet the following three requirements established by the LCCII: (1) they must report the access and security vulnerabilities detected in their investigation to the person responsible for the affected networks and computer systems; (2) they must have complied with the other conditions on responsible communication of vulnerabilities issued by the Cybersecurity Agency; and (3) the access must have been made with no intention of seizing or using the information contained in the computer system, nor with the purpose of attempting fraud.

However, it has been widely discussed whether ethical hacking requires the previous consent of the accessed entity. The latest regulation of the European Union[4] in this regard establishes that previous consent is not required, but that entities should adopt vulnerability disclosure protocols for third parties to provide the necessary information on how to report any vulnerabilities discovered.

The LCCII does not establish the need to previously obtain the accessed entity's consent, nor does it establish protocols or standards on how this access should be handled. The three requirements tioned above, which are needed to practice ethical hacking, seem insufficient to prevent ill- ded individuals from using this exemption to camouflage their intent to test computer systems iminal purposes.

nclusion

ventual approval of the LCCII would place Chile at the forefront of cybersecurity regulations in America. Notwithstanding the above, there are still several topics that require definition, such as s relating to significant incidents or delicate topics like ethical hacking, as well as the paths that the country will follow to provide the necessary training to people involved in the cybersecurity framework.

In addition, even if the LCCII becomes a law in a relatively short term, it will be essential that the relevant authorities and agencies set forth the complementary regulations that the LCCII establishes for its entry into force, and effectively harmonise the current regulations on cybersecurity related to the LCCII. For these purposes, we believe that all the sectors involved should reinforce their resources and efforts by continuing to build public-private partnerships and, especially regarding public entities, by allowing the participation of the MTT and the MST.

Notes

[1] These include: (1) Banco de Chile, which suffered losses in excess of USD $10m in 2018; (2) Banco Estado, which was forced to close its offices; (3) the Armed Forces Joint Command (EMCO), where 400,000 confidential emails were released; and (4) the Chilean Army, which, on 26 May 2023, detected that its institutional networks had been victims of a ransomware attack.

[2] Please note that the Chilean Government has recently launched the new 2023–2028 National Cybersecurity Policy.

[3] Related regulations on cybersecurity matters have been issued, including: (1) Law No 21,180 in 2019, with the aim of promoting that the administrative procedures of all bodies of the Chilean State Administration be carried out by electronic means; (2) Law No 21.459 establishing rules on computer crimes and amending other legal bodies to adapt them to the Budapest Convention; and (3) Resolution No 1,318, of 10 August 2020, issued by the Undersecretary of Telecommunications, establishing the general cybersecurity fundamentals for the design, installation and operation of networks and systems used for the provision of telecommunications services.

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

Similar topics

- Cybersecurity
- essential services
- cybersecurity incidents
- National Cybersecurity Policy.