LEY N°21.459

On June 20, 2022, Law N°21,459 that "ESTABLISHES RULES ON COMPUTER CRIMES, REPEALS LAW N°19,223 AND AMENDSS OTHER LEGAL BODIES WITH THE OBJECTIVE OF ADAPT THEM TO THE BUDAPEST CONVENTION", which typifies a number of criminal offenses related to the security of information that is being handled by computer systems.

In particular, the new law sets out the following catalog of crimes:

1. Attack to a computer system's integrity: It punishes anyone who hinders or impedes the normal operation of a computer system through the introduction, transmission, damages, deterioration, alteration or deletion of computer data.

2. Illegal access: It punishes the unauthorized access to a computer system or exceeding the granted authorization, overcoming technical barriers or technological security measures, and holding, using or disclosing the computer data gathered through such means.

3. Illegal interception: It punishes the undue interception, interruption or interference, through technical means, of a non-public transmission in a computer system or between two or more computer systems, and picking up the contents of computer systems through the electromagnetic waves emitted by them.

4. Attack on the integrity of computer data: It punishes the alteration, damages or deletion of computer data, provided that it causes a severe damage to the owner of such data.

5. Computer forgery: It punishes anyone who unduly introduces, alters, damages or deletes computer data with the purpose that such data is believed to be authentic or to be used for the creation of authentic documents.

6. Illegal reception of computer data: It punishes anyone who knowingly or who cannot not know the origin of computer data originated through the commission of some of the crimes described in this law (namely, illegal access, illegal interception and computer forgery), commercializes, transfers or storages such data with the same purpose or for other illegal ends.

7. Computer fraud: It punishes anyone who, causing damages to another and with the purpose of obtaining monetary gain for him or herself or a third party, manipulates a computer system through the introduction, alteration, damage or deletion of computer data or through any other interference in a computer system's operation.

8. Device Abuse: It punishes delivering or obtaining, importing, marketing or any other manner to make available any device, computer program, security code, access code or any other similar data, that have been created or adapted with the main objective of allowing an attack to a computer system's integrity, illegal access, illegal interception, attack on the integrity of computer data and the fraudulent use of payment cards and electronic transactions[1].

The new law adds these crimes to the list of illegal conducts for which a legal person can be held criminally responsible. Therefore, an entity could be responsible of such crimes when these are committed, whether directly or indirectly, in its favor and the commission of the conduct is a consequence of the entity's non-compliance of its direction and supervision duties.

In this sense, entities should undertake the necessary measures to avoid the commission of these crimes, such as setting or reviewing their information security policies in order to give clear guidelines regarding the management of computer data and systems, and implementing technical and organizational mechanisms that

[1] Article 7, Law N°20,009

allows to ensure the security, confidentiality and control of the stored or transmitted information, both within and outside the entity.

We hope this information is useful to you and remain available to clarify or supplement any aspect of it.

María José Henríquez
Partner | Competition / Antitrust
mjhenriquez@moralesybesa.cl

Juan José Prieto
Associate | Data Protection
jjprieto@moralesybesa.cl