

June 20, 2022

LEGAL ALERT

New Cybercrime Law: Criminal and Compliance Aspects

On June 20th, 2022, Law No. 21,459 (hereinafter, the "New Law") was enacted, repealing Law No. 19,223 (which formerly regulated cybercrime offenses). The New Law includes several new rules which address the needs of modern society and adapt Chilean legislation to the Cybercrime Convention of the European Council, known as the "Budapest Convention".

One of the main innovations of the New Law is the modernization of the criminal offenses to include modern cybercrimes, and address developments in technology, as well as relevant legal assets that were not included in the former legislation.

The New Law allows for the prosecution of criminal offences such as illegally accessing an information system without requiring a specific purpose (Section 2); an attack on a computer system as well as the integrity of its data (Section 1 and 4); the illegal interception of information (Section 3); and computer-related forgery (Section 5). Additionally, computer-related fraud is expressly regulated (Section 7), which previously was only partially punishable under the general offenses of fraud of the Chilean Criminal Code.

The New Law also sanctions anyone who sells, transfers, or stores -in any way- computer data, they know was obtained illicitly, i.e., obtained through any of the crimes described in the New Law. Additionally, the misuse of devices is addressed. (Section 8).

All of the cybercrimes established in the New Law will be added to the list of predicate offenses to commit money laundering according to the Anti-Money Laundering Law (Law No. 19,913).

Furthermore, the New Law expressly regulates so-called "ethical hacking", which exempts from criminal liability those who, within the framework of vulnerability investigations or to improve computer security, access a computer system with the express authorization of its owner (Section. 16).

In addition, the concept of “effective cooperation” is included as a mitigating factor of criminal liability, i.e., which allows the judge to reduce the penalty imposed -up to one degree of the sanction regulated in the law- to those who provide information helpful to solve the case, identify those responsible or prevent the perpetration of any of these crimes. On the other hand, special investigative measures are also included, such as the use of undercover agents (Section 12).

The New Law also establishes some requirements for communications service providers when the Public Prosecutor's Office requests that they provide information. Companies are now required to preserve information for a specific period and adhere to confidentiality requirements. Breaching confidentiality may be punishable according to the offense included in Section 36 B of Law No. 18,168, General Telecommunications Law, which only applies to natural persons.

Please consider that the cybercrimes described above may generate criminal liability for legal entities, as they are included in the list of crimes of Law No. 20,393 (“Corporate Criminal Liability Law”). Thus, companies and legal entities must identify the activities or procedures in which, whether habitual or sporadic, the risk of committing cybercrimes is generated or increased, and implement specific protocols, policies, and procedures, to prevent such crimes. For these purposes, they will have to carry out a risk survey and update their respective risk matrices and controls of their Crime Prevention Models.

Finally, please note that the New Law establishes a deferred enforcement. Regarding the new rules of the Procedure Criminal Code, the New Law states that it will come into force six months after the publication in the Official Gazette of a regulation that must be issued by the Ministry of Transportation and Telecommunications, and also signed by the Minister of the Interior and Public Security. Regarding the new money laundering regulation and new crimes that are incorporated into the catalog of the Corporate Criminal Liability Law, the New Law states that it will become effective six months after the publication of the present law in the Official Gazette. Regarding the new cybercrime offenses, the New Law will enter into force once the promulgating decree is published in the Official Gazette.

Authors: Rodrigo Aldoney; Eduardo Alcaíno