

11 2501 0475 Av. Brigadeiro Faria Lima, 1826 - cj. 906 01451-908 Jardim Paulistano São Paulo - SP



Karin Toscano Mielenhausen karin@ktmadvocacia.com.br

Possible Penalties in the Event of Data Leaks

In an effort to recognize and regulate cyber-legal relations, the Internet Civil Law Framework ("Marco Civil da Internet") – as it was entitled by Law nº. 12,965 (2014) – established certain principles, rights, and duties for the use of information superhighway in Brazil. Every user, Internet Service Provider (ISP), and online service provider is directly covered by the norm and, as a result, has had to adapt to its legal requirements over the course of recent years. Though the law in question dealt closely with questions related to privacy in the context of the World Wide Web¹, some aspects remained undefine, namely the protection of personal data, the core subject addressed by Law nº. 13,709 (2018), the new General Data Protection Act (GDPA) ("Lei Geral de Proteção de Dados" - LGPD).

With a vacatio legis in line with the degree of complexity of the modifications imposed on its adherents, the new law – which was designed to protect fundamental privacy and liberty rights and free personal development, dignity, and citizenship – will take effect only in 2020, sufficient time it is hoped to guarantee that companies and society in general will make the necessary adaptations to comply with the norm. However, civil, administrative, and – in the last analysis – criminal sanctions will be imposed on anyone who deliberately refuses to or in some manner neglects to adapt to the law's requirements.

It should be noted that, among the innovations contained in the text of the GDPA, subject to administrative sanctions, is that companies must begin to collect only the minimum of data necessary for their particular needs and eliminate any data collected after those purposes are served. They must also maintain detailed records of all of their data handling activities, as well as name a so-called Data Protection Officer, whose job it will be to act as a communications conduit between the owners of the data and the company, while also supervising and monitoring compliance with the legal norms.

Data security received special attention in the new legal framework with the requirement for security guidelines in the data handling process, as well as personal data protection protocols that must extend from the initial concept for products and services until their effective execution. Finally, companies

e-mails and chats, only in the context of a criminal investigation;

must notify the national data protection authority of any data security incidents, as well as the data owners and the general public, depending on the seriousness of the nature of the incident.

Articles 52 to 54 of the GDPA deal specifically with compliance and the application of administrative sanctions for any violations, penalties that vary from: a) a warning, with a specific time period in which corrective measures must be taken; b) a simple fine, of up to 2% (two percent), of the private law legal entity, economic group, or conglomerate in Brazil's billing in the last fiscal year, excluding taxes paid and limited to a total of R\$ 50,000,000.00 (fifty million Brazilian reals) per violation; c) a daily fine, up to a total limit of R\$ 50,000,000.00 (fifty million Brazilian reals); d) public disclosure of the violation, after its occurrence has been duly investigated and confirmed; e) a hold or stay on the personal data involved in the violation, until the said violation is remedied; and f) the elimination of the personal data involved in the violation.

Naturally, in accordance with the guarantees enshrined in the Brazilian Constitution, those sanctions may only be applied following an administrative law proceeding that allows for a full defense, respects the particulars of the concrete case, and takes into account the parameters and criteria established in the law itself². Nevertheless, it is important to note that those administrative sanctions may not be substituted for the application of the penal sanctions provided for in specific legislation. Under the express terms of art. 55-J, the national data protection authority not only must notify the internal control bodies of any non-compliance with the provisions of the law on the part of federal public organs and entities, but must also report to the competent authorities any criminal violations it is aware of.

In addition, the absence of a specific criminal law that effectively covers the conduct included in so-called cybercrime – violations carried out online – has forced recourse to the traditional crimes provided for in Brazilian law. For example, laws against fraud, misrepresentation, threats, and the various specific forms of libel, slander, and defamation of character (in the Brazilian context, "injuria", "calúnia", and "difamação"), among others, are resorted to when the seriousness of the facts goes beyond the limits of a mere administrative law

Jan • 2019



11 2501 0475 Av. Brigadeiro Faria Lima, 1826 - cj. 906 01451-908 Jardim Paulistano São Paulo - SP

¹ By way of example, the Internet Civil Law Framework did the following:

a) Instituted the mandatory removal of offensive content from sites, blogs, or social networks, following a court order, with criminal penalties for anyone producing or distributing said material; b) Allowed for the violation of the privacy and data protection rights of Internet users, including

c) Barred sites from collecting user data without consent.

² "Art. 52. (...)

I – The seriousness and the nature of the violation and of the personal rights affected; II – the good-faith of the violator; III – the advantage available to or sought by the violator; IV – the economic conditions of the violator; V – repeat offenses; VI – the degree of the harm done; VII – the cooperation of the violator; VIII - the repeated adoption and demonstration of internal mechanisms and procedures capable of minimizing any damage, focused on the safe and adequate handling of data in line with the provisions of paragraph 2, section ("inciso") II, of art. 48 of this Act; IX – the adoption of best practices and corporate governance; X – the ready adoption of corrective measures; and XI – proportionality between the seriousness of the violation and the severity of the saction".

RECHT & STEUERN | NEWSLETTER Neues Brasilianisches Datenschutzgesetz



11 2501 0475 Av. Brigadeiro Faria Lima, 1826 - cj. 906 01451-908 Jardim Paulistano São Paulo - SP violation. It must also be clarified that the GDPA is absolutely silent with respect to the creation of specific crimes to punish conduct in the virtual realm.

In this respect, if it is understood that the duty of professional confidentiality includes the obligation of data secrecy, any conduct that discloses such data without just cause may be held to be criminal if it is prejudicial to the other party. Moreover, it should be recalled that art. 154-A of the 2012 Penal Code defines as a crime the invasion of an information storage device for the purpose of adulterating or destroying data or information to obtain an unlawful advantage. This criminal classification may likewise aid in combating the abuses related to the new law.