ECIJA
Torre Mural. Av. Insurgentes Sur 1605 piso 10
Col. San José Insurgentes, C.P. 03900,
Ciudad de México, México
Tel: (+52) 5556626840
www.ecija.com

Why is the FBI investigating ZOOM? Comments on privacy and cybersecurity in the context of digital video conferencing platforms in Mexico.

This document has four parts. The first introduces and summarizes the analyzed facts; the second addresses considerations on the regulatory framework in terms of privacy and cybersecurity; the third analyzes the contractual and regulatory obligations that derive from this business model; conclusions are provided in the final part.

I. Introduction

The coronavirus pandemic has caused the suspension of most work and academic activities and practically all in-person meetings of large and medium sized groups of people, provoking a massive increase in the use of remote communication platforms such as: Zoom, Google Meet, Microsoft Teams and Skype among others.

The excessive increase in the use of digital platforms placed several of these in the sights of various international institutions, such as the FBI (Federal Bureau of Investigation) due to personal data protection, privacy, and cybersecurity concerns.

The United States Department of Homeland Security issued a statement regarding cybersecurity threats in remote communication platforms, with particular reference to the Zoom and Microsoft Teams applications.

Following the aforementioned investigations, the Zoom platform began to take measures to correct the problems that had arisen[1], such as the "zoombombing", which refers to strangers accessing the conferences in the platform, either in meetings, virtual classes, or in the workplace; updating its privacy policies, in order to be clearer regarding the data collected by the application; as well as avoiding the collection of unnecessary information from the Facebook accounts of its users.

II. Regulatory Considerations on Privacy and Cybersecurity

As a consequence of the health contingency, the memorandum that Homeland Security published on the use of digital platforms for teleworking, warned of the severe security risks that the use of these involve, mainly identifying four malicious practices: (i) phishing, (ii) malware distribution, (iii) cyber-attacks on communications, and (iv) registration of internet domains with words related to such as COVID19 and coronavirus, of questionable use.

[1] Zoom (2020); "A Message to Our Users", April 1, 2020, from the Official Zoom Blog; Website: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Analyzing from a Mexican law perspective, it is worth mentioning that any company that offers face-to-face or online services can operate in Mexico through legal entities incorporated in Mexico, or through foreign companies authorized to operate in our country[2], in terms of the Foreign Investment Law.

Likewise, they must first have sufficient security systems and privacy policies to ensure that the information of the users of the platforms is duly protected since, otherwise, they would be directly responsible for any misuse of it.

The first mechanism for preventing legal risks is the clear communication of the terms and conditions of use of the platforms. The Zoom case is sobering, since everything derived from a mishandling of this information, as recognized by the same platform[3].

Considering that these platforms handle a considerable amount of information and that due to its content such can be considered sensitive and strictly personal, these companies in Mexico are subject to a specific obligations regime, contained in the Federal Law for the Protection of Personal Data Held by Individuals. This law imposes various obligations on those processing personal data, including the so-called **privacy notice**, which constitutes the document by which the user is made aware of the use and treatment given to its information. Such notice presumes the existence of a reasonable expectation of privacy.

Consequently, if the terms and conditions of the privacy notice of any platform, falsify or omit information related to the encryption and protection of the information poured in the videoconferences held through the platform, such would be **an infringement to the privacy and treatment of personal data**, by omitting information in the privacy notice and violating the security of databases, programs or equipment.

Likewise, cybersecurity provisions to be followed by these platforms are a priority. However, in Mexico, the shortage of specialists and regulation make this a complex task, given that the applicable legal framework would be that established by the Federal Law for the Protection of Personal Data Held by Individuals.

It should be noted that, since the regulatory framework is insufficient in terms of cybersecurity, resorting to international regulation is necessary for its proper understanding and dimension, as is the case of the Convention on Cybercrime or the Budapest Convention[4], and the Ibero-American Convention of Cooperation on Investigation and Assurance of Evidence on Cybercrime of the member states of the Conference of Ministers of Justice of Ibero-American Countries. However, unfortunately, neither of the two international instruments have been ratified by the Mexican State to date.

[2] In terms of article 15 of the Commercial Code, those "companies legally incorporated abroad that are established in the Republic, or have an agency or branch therein, may exercise commerce, subject to the special requirements of this Code in all that it concerns the creation of its establishments within the national territory, its commercial operations and the jurisdiction of the courts of the Nation".

[3] Zoom (2020); "The Facts Around Zoom and Encryption for Meetings / Webinars", April 1, 2020, from the Official Zoom Blog; Website: https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

[4] It is the only binding international treaty on the matter and constitutes a kind of framework agreement for the Party States to implement within their legal system the relevant legislation to investigate and prosecute those crimes committed against computer systems or means, or through the use thereof, and facilitate international cooperation.

One of the measures derived from the international instruments referred to in the preceding paragraph is the definition of certain crimes, namely: (i) crimes committed against the confidentiality, integrity and availability of computer systems and data, (ii) crimes committed through the use of information and telecommunications technologies (computer fraud and counterfeiting), (iii) crimes due to their content (child pornography) and (iv) copyright crimes.

With respect to **crimes committed against the confidentiality, integrity and availability of computer systems and data**, in Mexico we find that, although they are not classified as such, similar criminal actions are provided in the Federal Criminal Code, under the heading of disclosure of secrets and **illegal access to computer systems and equipment**. The law classifies as a crime if an unauthorized person becomes aware of or copies information contained in computer systems or equipment protected by some security mechanism, whether owned by the State or by the national financial system, or in case authorized individuals, modify or destroy such information without justified cause.

III. Contractual and Corporate Implications of the Business Model

The operation of a business model such as Zoom, Microsoft Teams, or any similar platform, either through companies legally incorporated in Mexico or through foreign companies authorized to operate in our country, necessarily implies rigorous contractual and corporate controls to avoid legal contingencies, which could be considerable.

First, the privacy notice of these platforms requires careful and detailed wording; as well as implementing the respective security measures to guarantee the integrity, availability and confidentiality of the information, which will allow protecting personal data against damage, loss, alteration, destruction or unauthorized use, access or treatment, in case these platforms are used by public entities, in terms of the General Law for the Protection of Personal Data held by Obligated Subjects.

Considering the implications that the shortcomings in these matters could cause to the companies developing or operating said platforms, which could be a cause for criminal responsibility; they should have a **corporate integrity policy and a permanent control body**, in charge of verifying compliance with said policies which aim to prevent crime, in order to be entitled to the benefits that the same law establishes.

Having a compliance officer specialized in the aforementioned regulatory framework is essential (such as the model that is currently being developed for financial technology institutions), especially if we consider the exponential development of information technologies and the increased rate of their use.

Implementing **codes of ethics** within these companies (similar to those required in the field of telecommunications) is an additional useful and effective measure, especially if it provides innovative treatment to digital communication services from the perspective of **digital rights**[5]**.** These are understood as the extension of the rights of citizenship (human rights), but taken to the digital world, being able to serve as corporate due diligence mechanisms to contain and prevent possible legal claims for potential human rights violations.

[5] Namely: (i) universal and equal access to the internet, without discrimination of any kind, (ii) freedom of speech, information and communication, (iii) privacy and data protection, (iv) freedom of access to any website or social platform, (v) right to be forgotten, (vi) protection of children and teenagers, (vii) intellectual property, and (viii) right to digital disconnection from work, mainly.

IV. Conclusions

All digital services platforms can operate in Mexico, through an entity legally established in terms of Mexican law, or through a foreign company under the Foreign Investment Law.

The lack of awareness and prevention culture of companies is the greatest vulnerability that exists in the area of cybersecurity, privacy, and protection of personal data.

Consequently, the development of clear, comprehensive and current contracting policies in the provision of digital interconnection services by video call, are essential to avoid legal contingencies for violations of the privacy of users, negligent treatment of personal data, where appropriate, and participation in cybercrimes.

Likewise, the development of integrity, control, and compliance programs in these matters (privacy and cybersecurity) are essential tools for the effective prevention of legal risks associated with the business model of the platforms.

Finally, implementing a treatment from a human rights perspective of privacy and the protection of personal data of users or clients of the company, as the case may be, is essential to streamline the results of compliance programs in the field of the company, since the shortcomings in the matter, not only carry criminal, administrative and civil liabilities, but can also be comparable to human rights violations.

ECIJA México, S.C.

Joaquín Rodríguez
(jrodriguezz@ecija.com)

Ricardo Chacón
(rchacon@ecija.com)

Adalberto Mendez
(amendez@ecija.com)

Berenice Sagaón
(bsagaon@ecija.com)