the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

ARGENTINA

Regional Coordinator:
Alan Campos Elias Thomaz *CT | Campos Thomaz Advogados, São Paulo*

Cybersecurity

Florencia Rosati *Beccar Varela, Buenos Aires*

Q 1. Are there any cybersecurity policies, strategies or regulations applicable to the metaverse in your region/country?

While there are no cybersecurity policies, strategies or regulations specifically tailored for the metaverse, Argentina's existing cybersecurity framework can be applied to the metaverse environment. This framework consists of various laws, regulations and government bodies which oversee cybersecurity matters. Key elements include the following:

National Cybersecurity Strategy

Resolution No 829/2019 of the Secretariat of Modernisation approved the First National Cybersecurity Strategy, aiming to establish the essential principles and central objectives of the Argentine Republic regarding cyberspace protection. This Strategy served as a foundational document, intended as a starting point for the deployment of actions and policies aimed at achieving objectives. Following a public consultation to gather information, contributions, proposals, experiences and recommendations from various stakeholders, including the public, private, academic sectors and civil society, among others, Resolution No 44/2023 of the Secretariat of Public Innovation approved the Second National Cybersecurity Strategy. This Second National Cybersecurity Strategy lays down the guiding principles and develops the central objectives that will allow the setting of national provisions regarding cyberspace protection. Its purpose is to provide a secure context for its use by individuals and public and private organisations, developing, in a coherent and structured manner, prevention, detection, response and recovery actions against cyber threats, along with the development of a suitable regulatory and institutional framework. This could be relevant to the security of metaverse platforms.

Law No 26,388 on Cybercrime

This law amends the Argentine Criminal Code to address cybercrime, covering illegal access to computer systems, data interception and system interference. These provisions are crucial for the metaverse, as they set legal precedents for addressing cyber threats within virtual environments.

Law No 25,326 on Data Protection (DP Law)

Although primarily focused on data protection, this law has implications for cybersecurity within the metaverse, particularly regarding the handling and security of personal data within virtual environments.

Q 2. What are the secure by design (physical and digital interfaces) principles applicable to the metaverse in your region/country?

There are no secure by design principles applicable specifically to the metaverse in Argentina. However, the approach to security-by-design within the metaverse is shaped by the country's data protection regulations. The DP Law sets a clear expectation for data controllers to adopt all necessary technical and organisational measures to secure personal data against unauthorised access, alteration, loss or processing, ensuring files meet stringent integrity and security standards.

Further emphasising the importance of privacy from the initial design phase, Regulation No 18/2015 of the Data Protection Authority (DPA) introduces the concept of 'privacy from design' within the Guide of Good Practices in Privacy for the Development of Application Software. This approach dictates that privacy considerations should be integral to the design and development process, persisting through every stage of the lifecycle of systems, applications or devices.

Additionally, DPA Resolution No 47/2018 offers a set of 'Recommended Security Measures for the Processing and Conservation of Personal Data', spanning the entire data lifecycle from collection to destruction. This includes protocols for access control, data backup, vulnerability management and incident response. While compliance with these measures is not mandatory, their implementation is strongly recommended as an effective means of demonstrating adherence to the security obligations outlined in the DP Law, reflecting the DPA's focus on accountability in compliance practices.

Q 3. Have there been any cyber incidents in the metaverse in your region/country? How do the applicable policies, strategies or regulations react to cyber-incidents?

We are not aware of any cyber-incidents in the metaverse in Argentina. In addressing how applicable policies, strategies and regulations react to cyber incidents in Argentina, the following legal frameworks and entities play a key role.

DP Law

The DP Law does not contain express provisions regarding what constitutes a security incident or what actions should be taken if one occurs. However, it does set out confidentiality and security obligations that should be complied with whenever processing personal data.

Resolution No 47/2018 of the DPA

This Resolution recommends specific security measures to comply with the DP Law, emphasising an accountability framework. It suggests that in the event of a security incident, a detailed report should be prepared, including the nature of the incident, affected personal data, identities of affected individuals, mitigation actions taken and preventive measures for future incidents, to be sent to the DPA. These measures are not mandatory.

DPA

In the event of cyber incidents involving data breaches, the DPA could impose sanctions for: (1) failing to comply with the duties of confidentiality and security regarding personal data included in records, files, banks or databases; and (2) keeping local databases, programs or equipment containing personal data without the proper security conditions as determined by regulations. The fines for such misconduct, considered 'serious' infringements, could vary between ARS 80,001 (approximately US$95[1]) and ARS 90,000 (approximately US$107). The DPA could also impose sanctions for failing to comply with the duties of confidentiality and security concerning sensitive data, as well as those collected and processed for criminal and misdemeanour purposes. The fines for such actions, considered 'very serious' infringements, could range from ARS 90,001 (approximately US$107) to ARS 100,000 (approximately US$119).

Criminal Code (Law No 11,179) and Cybercrime Law (Law No 26,388)

These laws address cyber incidents with various provisions. Notably, the Cybercrime Law amends the Criminal Code to introduce specific offences related to information and communication technologies. These include:

- illegal access to confidential information (Article 153 of the Criminal Code), punishable by anything from 15 days to six years' imprisonment, depending on the circumstances of the offence and the nature of the information accessed;
- interception and capture of communications without judicial authorisation (Article 153 bis), punishable by one month to two years' imprisonment;
- data damage and computer sabotage (Article 183), involving unauthorised deletion, dissemination, deterioration, alteration or suppression of data, documents, messages or electronic communications, or any interference with computer systems, punishable by six months to three years in prison; and

1 Taking as a reference the exchange rate value for selling dollars from the Banco de la Nación Argentina of 28 February 2024.

- fraud by manipulation of computer systems (Article 173), punishable by anything from one month to six years' imprisonment.

Civil and Commercial Code (Law No 26,994)

The Civil and Commercial Code establishes civil liability for damages. Victims of security incidents can claim compensation for the harm suffered through civil actions. This includes damage to privacy, economic losses and other injuries resulting from cyberattacks.

While there is no specific case law related to cyber incidents in the metaverse, the following are notable cases involving cyber incidents in Argentina.

Yahoo de Argentina SRL, 6 June 2019

The DPA considered that the backup archives affected by the breach did not have the appropriate encryption level, the security copies were not encrypted by default and the company could not confirm the identities of the mechanics or individuals involved in the incident. Consequently, the DPA imposed a sanction of ARS 80,000 (approximately US$95).

Argentine Federal Police (PFA), 5 February 2020

In response to a security incident leaking 700 gigabytes of confidential information due to phishing attacks on non-institutional email accounts, the DPA found the PFA had not taken sufficient preventive actions nor complied with mandatory institutional email usage for confidential information transmission. The PFA received two warnings for failing to meet the DP Law's security and confidentiality obligations but was not pecuniarily sanctioned due to the internal nature of fund transfers between state departments.

Ministry of Health of San Juan, 20 May 2021

After a security breach exposed the personal data of 115,000 individuals applying for a driving licence, the DPA determined that the Ministry of Health had not maintained proper security conditions and failed in its duty of confidentiality. As a result, two warnings were issued for these serious breaches.

Mercado Libre, 20 August 2021

Following a complaint about unauthorised sharing of personal data through a fake account created using another individual's ID, the DPA investigated and found Mercado Libre's measures to mitigate harm and prevent future incidents sufficient. Despite identifying breaches of security and confidentiality obligations, no sanction was imposed, with the condition that Mercado Libre implemented necessary technical and organisational measures.

Cencosud SA, 21 September 2021

The DPA initiated an ex officio investigation against Cencosud, after becoming aware of a breach in its computer systems due to an 'Egregor ransomware' attack. The DPA found that Cencosud had not adopted preventive security measures nor informed its customers about potential data leaks. Consequently, a fine of ARS 290,000 (approximately US$353) was imposed for these serious and very serious infringements.

Q 4. Are there any cybersecurity standards in your region/country specifically applicable to the metaverse? What are the main obligations they set out?

To date, there are no cybersecurity standards in Argentina that are specifically designed for the metaverse. The existing abovementioned cybersecurity and data protection regulations provide a general framework that applies to digital environments, including the metaverse.

Q 5. Are there any upcoming policies, strategies or regulations impacting the cybersecurity in the metaverse?

Currently, there are no forthcoming policies, strategies or regulations specifically affecting cybersecurity within the metaverse.