



the global voice of  
the legal profession®

IBA Intellectual Property, Communications  
and Technology Law Committee

## Digital Regulations in the Metaverse Era

# CHILE

Regional Coordinator:

Alan Campos Elias Thomaz *CT* | *Campos Thomaz Advogados, São Paulo*



# Data

Alfonso Silva *Carey, Santiago*  
Raúl Mazzarella *Carey, Santiago*  
José Ignacio Mercado *Carey, Santiago*

---

## 1. Are there any data (personal and non-personal) policies, strategies or regulations applicable to the metaverse in your jurisdiction?

There are no specific policies, strategies or regulations applicable to the metaverse, but general regulations and strategies regarding personal data, digital platforms, digital marketing and the use of artificial intelligence (AI) may apply.

---

## 2. How are the various personal and non-personal data associated with the metaverse protected in your jurisdiction?

As mentioned above, no specific regulations have been adopted in Chile regarding the metaverse or for the protection of personal and non-personal data in the metaverse.

However, as far as personal data is concerned, general regulations on the processing of personal data may be applicable, as explained below. In this regard, please consider that the processing of personal data is regulated in Chile by Law 19,628 on the Protection of Private Life<sup>1</sup> (the 'DPL') of 1999, which defines 'personal data' as all the data 'relating to any information concerning identified or identifiable natural persons'.

Under the DPL, there are only two lawful bases for the processing of personal data: the law and the data subject's express, informed and written consent. In Chile, there are no other legal bases as in other jurisdictions (eg, legitimate interest). Also, it is important to note that entities that process personal data have general security and confidentiality obligations regarding the data they process. These obligations will apply to any personal data involved in the metaverse, such as the personal data of users and the personal data of metaverse employees.

From a consumer protection perspective, it is worth mentioning that after an amendment to Law 19,496, which includes provisions on the protection of consumer rights (the 'CPL') of 1997, Article 15 bis, the consumer rights protection entity, the National Consumer Service (Servicio Nacional del Consumidor or SERNAC), was granted powers and faculties in relation to activities which involve consumers' personal data. In this context, SERNAC issued 'interpretative guidelines' (ie, Exempt Resolution No 33 with an interpretative guideline on consumer protection regarding the use of artificial intelligence (AI) systems in consumer relations of 2022 and Exempt Resolution No 174 with an interpretative guideline on equity criteria in the provisions contained in standard form consumer agreements referring to the collection and processing of consumers' personal data of 2022) regarding the processing of personal data of consumers, stating, among others, that: (1) providers must limit the processing of consumers' personal data to the purposes for which it was initially collected and they were informed about; (2) such purposes must satisfy the reasons that motivated the contract between the parties; (3) the controller must apply principles of purpose limitation and proportionality mechanisms to its collection and processing activities for business-to-consumer (B2C) relationships; and (4) the clauses related to the processing of personal data must be drafted in clear terms and without generating a significant imbalance in the rights and obligations of the parties.

---

<sup>1</sup> See Ley Chile - Ley 19628 - Biblioteca del Congreso Nacional (bcn.cl) accessed 30 May 2024.

### **Q 3. Who are the different stakeholders involved in the metaverse data value chain and, in the case of personal data, what are their data protection roles? How are their activities regulated under regional/national policies, strategies or regulations?**

As previously mentioned, activities by Chilean companies in regard to the metaverse are very low. Notwithstanding the foregoing, there is increasing curiosity and expectations regarding the potential of the metaverse in relation to the collection and analysis of data generated by users' activities in the metaverse, as already happens regarding social networks and tracking cookies.

The development and use of the metaverse in Chile is not massive and, from a data protection perspective, the lack of a national data protection authority in the country leaves data subjects more exposed to potential unauthorised uses of their personal data in the context of the metaverse.

As mentioned, SERNAC has been empowered with certain faculties regarding the processing of personal data of consumers and, once the use of the metaverse becomes more popular in Chile, SERNAC will probably monitor such activities more closely, particularly in regard to sellers/suppliers within the metaverse.

The Chilean trade association for digital marketing companies (AMDD) has had an active role in the legislative discussion regarding digital marketing and the processing of consumers' personal data, and has issued a self-regulation code.<sup>2</sup> Among other things, such code establishes principles to be adopted during the processing of personal data, which are more complete compared to the general provisions established in the DPL.

The Comptroller General of the Republic of Chile has issued certain legal opinions regarding the use of digital networks (especially social networks) by public authorities, which may provide a clue regarding how such entities should use the metaverse, but without focusing on the processing of personal data involved in such activities.

### **Q 4. In relation to personal data, what are the data protection principles (eg, transparency) applicable to the metaverse? What are the most common types of infringement of data protection principles in the metaverse (eg, data minimisation) in your jurisdiction?**

As mentioned above, the DPL is an old regulation and, as such, it does not organically include data protection principles similar to those included in the European Union General Data Protection Regulation. The general principle of confidentiality and due care in the processing of personal data applies to the metaverse. Additionally, SERNAC through its interpretative guidelines has managed to enhance proportionality and purpose limitation principles for data processing in the framework of a B2C relationship. Please note that such guidelines only contain the interpretation by SERNAC regarding the law, so they are not directly binding on third parties.

Based on the current regulations, the most common type of infringement may arise from the lack of a legal basis to process personal data.

Additionally, SERNAC may consider abusive any clause included in the consent granted through the terms and conditions or privacy policy in which the consumer: (1) generically authorises the provider to process his/her personal data, without being previously informed of the purposes of the processing; (2) irrevocably authorises the provider to process his/her personal data; (3) relieves the provider of any liability or from complying with the security obligations related to the processing of his/her personal data; and (4) is compelled to authorise 'certain data collection and processing operations that are excessive or that deviate from the typical purpose that an average consumer seeks to satisfy through the consumer relationship, taking into consideration his/her reasonable expectations'.

Considering the lack of specific regulation, infringements occurring in the metaverse would be subject to the general sanctions of the DPL. Such sanctions vary depending on the type of breach, as follows:

2 See [www.amddchile.com/wp-content/uploads/2023/07/CODIGO\\_ETICA\\_AMDD\\_2023\\_compressed.pdf](http://www.amddchile.com/wp-content/uploads/2023/07/CODIGO_ETICA_AMDD_2023_compressed.pdf) accessed 30 May 2024.

- Fines associated with the exercise of the data subjects' rights: If the data controller does not respond to a request for information, modification, cancellation or blockage made by a data subject within two business days or denies it for any reason other than national security or the public interest, the data subject may file a claim before the ordinary civil courts. If the court rules against the data controller, it may establish a term for the data controller to comply with the ruling and impose a fine of up to 50 monthly tax units (*unidad tributaria mensual* or UTM). If the data controller does not comply with the court's decision within the term specified, the court may impose an additional fine of up to 50 UTM.
- Compensation for damages: The data subject is entitled to file legal action against the data controller for compensation for material and moral damage that he/she suffered from the unauthorised or improper processing of his/her personal data.

Additionally, from a consumer law perspective, SERNAC could initiate a procedure against acts or omissions that affect the exercise of consumers' rights regarding the use of their personal information within a consumption relationship, seeking the application of fines for the protection of the consumers' general interests, by filing a class action before the competent civil court or a judicial action before the competent local police courthouse (*juzgados de policía local*) to request the application of fines. Generally, the risks derived from non-compliance or breaches of the CPL are a general fine of up to 300 UTM, if there is no specific sanction provided, plus economic and moral damages.

A consumer may also individually seek the application of fines and request compensation for damages in the case of breaches of the CPL by filing an individual action before the local police courthouse.

There is no case law regarding the infringement of data protection in the metaverse. However, there are a few rulings that have established the liability of data controllers for a breach of the general principles set out in the DPL. For instance, in 2016, a well-known bank was ordered by a civil courthouse to compensate three customers for having improperly processed their personal data.<sup>3</sup> The lawsuit was motivated by the finding of documents abandoned in a clandestine landfill containing the personal information of a group of clients of the bank. In the court's opinion, the defendant infringed the provisions of Articles 6 and 11 of the DPL for not having properly safeguarded and properly treated the personal data of the plaintiffs, becoming liable for the damage caused.



## **5. In relation to non-personal data, how is data sharing/licensing regulated in your jurisdiction? Is data ownership recognised? How is proprietary information, including any rights to datasets regulated in your jurisdiction? What are the most common types of infringement of these rules in the metaverse (eg, unlawful use of proprietary information) in your jurisdiction?**

Information that corresponds to copyright is regulated by Law 17,336 on Intellectual Property<sup>4</sup> of 1970 ('Copyright Law'), while patents and trade secrets are protected under Law 19,039<sup>5</sup> of 1991, which sets forth the provisions applicable to industrial privilege and the protection of industrial property rights (the 'Industrial Property Law').

According to the Copyright Law, only datasets that 'by reason of the selection or arrangement of their contents, constitute intellectual creations' are protected, provided that such protection does not cover the data or materials themselves.

The unauthorised use of third-party copyright may correspond to a breach of the Copyright Law, leading to criminal and civil liability.

Criminal liability for a breach of the Copyright Law may be sanctioned with penalties of up to 540 days of prison and a fine of up to 1,000 UTM.

- Civil liability allows the copyright holder to claim one of the following alternative forms of compensation:
- compensatory damage: compensation for actual economic and moral damages, where the amount of damages can be determined based on the legitimate retail value of the protected objects; and

<sup>3</sup> Arellano v Banco Santander [2015] 16th Civil Court of Santiago, No C-29221-15.

<sup>4</sup> See <https://bcn.cl/3i17x> accessed 30 May 2024.

<sup>5</sup> See <https://bcn.cl/3i17u> accessed 30 May 2024.

- statutory damage: once the infringement has been judicially ascertained, a claim for a single compensatory amount is determined by the court in relation to the seriousness of the infraction and cannot exceed 2,000 UTM.

Under the Industrial Property Law, datasets may be protected as ‘trade secrets’ to the extent the information: (1) may be used in productive, industrial or commercial activities; (2) is of a secret nature, in the sense that it is not known or easily accessible to persons within the circles in which this type of information is normally used; (3) has a high value for the company because it is secret; and (4) has been and is subject to reasonable measures of protection by the company to keep it a secret.

A breach of the Industrial Property Law may lead to civil liability (compensation for damages) and criminal liability (up to five years in prison).

Please note that we are not aware of any case law or a regulator issuing a decision regarding infringements of the aforementioned rules applied to the metaverse.

## 6. Are there any policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?

There are no relevant policies, strategies or regulations applicable to digital marketing in the metaverse in Chile. However, the general consumer protection rules and standards would be applicable in the context of the metaverse.

In this sense, terms and conditions must be respected and the rules governing advertising activities and the sending of commercial and marketing communications must be complied with.

In this regard, pursuant to the CPL, if promotional information is sent to customers via email, it is necessary to: (1) indicate the subject matter of the communication; (2) identify the sender; and (3) include a valid address to which the consumer to whom the communication is addressed can request the suspension of such communication. Then, if a consumer requests not to receive this information or to unsubscribe, further communications should be prohibited from that moment onwards.

Additionally, providers must comply with the applicable rules regarding advertising described below in the answer to question 2 in the chapter on digital marketing and consumer protection.

An infringement of the rules regarding the sending of marketing communications may be sanctioned with fines up to 300 UTM. Please note that SERNAC has initiated legal proceedings against providers regarding the violation of this obligation.<sup>6</sup>

For information on the sanctions associated with advertising, please see the answer to question 2 in the chapter on digital marketing and consumer protection.

## 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring the protection of minors’ data? What is the age of consent for data protection purposes? Is it necessary to verify the consent provided by a responsible adult?

The DPL does not include any provisions regarding the personal data of minors, and there are no policies, strategies or regulations focused on this topic, other than a general concern regarding the risks involved in such processing activities.

Under the general rules in the Civil Code, the legal capacity to act and be held accountable under the law is fully applicable at 18 years old. However, males over 14 and under 18 and females over 12 and under 18 have limited legal capacity, and can be represented by a responsible adult or personally if they are duly authorised. Hence, the age of

<sup>6</sup> *SERNAC v Entel PCS* [2020] 2nd Local Police Court of Santiago, No 7943-2020.

consent for individuals to act in a personal capacity is 18 years old, but people under 18 and those over 12 or 14, as per the specifics of the case, could give their consent through their representatives or if they are duly authorised by them.

The law does not expressly require identity verification, but if consent is granted by someone that is under age, it would not be valid and the processing activities would not be considered lawful.

---

## **Q 8. How are 'international data transfers' regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of these rules in your jurisdiction?**

The DPL does not expressly regulate the cross-border transfer of personal data, nor does it establish restrictions for the transfer of personal data to certain countries or jurisdictions. However, cross-border data transfers may be considered a type of data processing activity, based on the definition set forth in the DPL. Hence, to the extent that the general data processing rules and requirements set forth in the DPL are met, cross-border transfers of personal data could be considered valid and legal.

As mentioned above, the data processing (which in this case would be the transfer of data) must be authorised by the data subject (eg, through the acceptance and approval by the data subject when he/she gives his/her consent to the processing of his/her personal data) and the parties must take the corresponding measures to ensure compliance with the confidentiality obligations regarding the personal data and the obligation to handle personal data with due care.

In this regard, in order to properly comply with the general due diligence obligations, it is necessary to take all those measures that, considering the regulatory and market environment, are necessary to ensure the confidentiality of the personal data and to protect such data from unauthorised or illegal access by third parties.

Please note that we are not aware of any case law or decisions by a regulator on this matter.

---

## **Q 9. How is automated decision-making regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of the rules applicable to automated decision-making in your jurisdiction?**

There is no general regulation on this topic. However, there are some specific rules on automated decision-making.

For instance, regarding employees of digital platform companies, Article 152 quinquies E of the Labour Code forbids discrimination through automated decision-making mechanisms. Concerning the implementation of algorithms, digital platform companies must respect the principles of equality and non-discrimination. To this end, such companies must take all necessary measures and safeguards to avoid any type of discrimination, particularly in regard to the allocation of work, the offer of bonuses and incentives, and the calculation of remuneration, among others.

Moreover, from a consumer protection perspective, SERNAC issued an interpretative guideline on consumer protection regarding the use of AI systems in consumer relationships<sup>7</sup> (Resolution No 33 of 18 January 2022).

We are not aware of any relevant case law or any decisions by a regulator in this regard.

---

7

See [www.sernac.cl/portal/618/articles-64740\\_archivo\\_01.pdf](http://www.sernac.cl/portal/618/articles-64740_archivo_01.pdf) accessed 30 May 2024.

## 10. What rights are granted to individuals for protecting their rights in the metaverse and how can they be exercised? What is the level of enforcement based on private claims in your jurisdiction?

There are no specific rules on this topic but general rules on data subject's rights could apply.

Data subjects have the right to access their personal data, free of charge, and this right cannot be limited or restricted by any agreement or contract. Likewise, the data subject has the right to request information concerning his/her personal data, such as: (1) what data is being collected; (2) the sources of the data; (3) the purpose for which the data is being collected; and (iv) the possibility of disclosure of the data to third parties.

The data subject may request the deletion thereof if such data storage lacks legal grounds or is outdated, or the data is used for commercial communications and the data subject does not wish to receive such communications.

The data subject is entitled to request the modification of his/her personal data when it is erroneous, inaccurate, misleading or incomplete.

The data subject may request the blocking of the processing or retention of his/her personal data when the controller cannot establish the accuracy of such data, or the validity of such data is doubtful and there are no legal grounds for the rectification or elimination of the data. Additionally, the data subject may request blocking when he/she voluntarily provided personal data or when it is used for commercial communications and the data subject is no longer interested in being part of the respective register, either on a permanent or temporary basis.

The data subject may oppose the use of his/her personal data for the purposes of advertising, market research or opinion-based surveys.

Also, the rights of data subjects fall within the scope of the consumer protection regulation. SERNAC has taken a more active role regarding the protection of consumers' personal data used within B2C relationships. The CPL grants certain powers to SERNAC, such as overseeing compliance by suppliers with the DPL, initiating voluntary proceedings for the protection of the collective or diffuse interests of consumers and administratively interpreting the DPL. Therefore, in the case of infringements of the CPL that impact data subjects, suppliers may face litigation brought by SERNAC, requesting the imposition of fines and compensation for damages.

## 11. Are there any upcoming policies, strategies or regulations that will impact the use of data in the metaverse?

Currently, a bill of law on data protection<sup>8</sup> (DPL Bill) is being discussed by the Chilean Congress, which aims to enhance privacy protection in the country in order to comply with international standards on the processing of personal data and to bring the country's regulations closer to European standards (ie, the General Data Protection Regulation) and closer to the guidelines issued by the Organisation for Economic Co-operation and Development (OECD).

Among other things, the DPL Bill provides the following main aspects:

- creates a Data Protection Agency as the national authority for data protection matters, with powers to supervise compliance with the law and to punish violations with fines of up to 20,000 UTM;
- establishes new mandatory principles applicable to the processing of personal data;
- regulates in greater detail the concept and requirements for consent and establishes a new statute of exceptions for consent;
- creates a National Registry for Compliance and Penalties;
- sets forth new proceedings relating to the prosecution of liabilities concerning international data transfers;
- establishes a duty to adopt security measures and reporting obligations with respect to security breaches;

8

See [www.senado.cl/appsenado/templates/tramitacion/index.php?boletin\\_ini=11144-07](http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07) accessed 30 May 2024.

- sets forth an obligation for data controllers to report breaches of security measures to the Data Protection Agency and also to the data subject, if such breaches concern sensitive personal data, data relating to children under the age of 14 or data relating to economic, financial, banking or commercial obligations;
- establishes the principle of security, which states that, during the processing of personal data, the data controller must ensure adequate security standards, protecting it against unauthorised or unlawful processing, and against its loss, leakage, accidental damage or destruction;
- grant data subjects the right to object and not to be subject to decisions based on automated processing of his/her personal data, including profiling, with few exceptions;
- specifies the situations where international data transfer activities are permitted; and
- expressly regulates the processing of minors' personal data, establishing that to process the personal data of 'children' (under 14 years of age), the consent of the parents or legal representatives, or the person in charge of the personal care of the child, is required, unless expressly authorised or mandated by law, while to process the personal data of adolescents over 16 years of age, the authorisation rules provided by law for adults will apply.



# Cybersecurity



## 1. Are there any cybersecurity policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Currently, there are no laws in Chile that comprehensively regulate cybersecurity or any cybersecurity measures to be applied in the metaverse.

However, there is a National Cybersecurity Policy 2023–2028 ('Chilean Cybersecurity Policy'), which establishes the public policy objectives on this matter. The Chilean Cybersecurity Policy was established with the purpose of guiding the actions of the state in the field of cybersecurity, establishing an action plan, goals and objectives in order to address the multiple challenges and obstacles faced by the country in this area. These challenges include the increase in cybercrimes, the vulnerability of infrastructure and other relevant issues in cyberspace.

It is important to note that the Chilean Cybersecurity Policy focuses on five main objectives, the establishment of: (1) resilient infrastructure; (2) individuals' rights; (3) a cybersecurity culture; (4) national and international coordination; and (5) the promotion of industry and scientific research.

Additionally, there is a National Cyber Defence Policy (the 'Chilean Cyber Defence Policy'), which complements the Chilean Cybersecurity Policy in regard to those aspects directly related to the defence of the country's sovereignty through digital networks and the protection of infrastructure considered to be 'critical'.

The Chilean Cyber Defence Policy focuses on three main areas: (1) cyber defence methods; (2) the promotion of transparency and trust among states through international cooperation; and (3) the development of capabilities in the cyber defence field. The implementation of this policy requires support from and progress made by national defence institutions.

Also, there are sectoral regulations that specifically regulate some cybersecurity matters, establishing security measures to be adopted by certain entities and obligations to report breaches of security measures, such as cyber incidents or cyberattacks. These sectoral regulations have been enacted primarily in highly regulated sectors, such as banking, energy and telecommunications.

As mentioned, the DPL contains a very broad and general obligation to 'take care of the data with due diligence and be liable for damages', which opens the possibility of determining the specific security obligations on a case-by-case basis, depending on the standards of care used in each industry and/or the particular data processing scenario. In addition, under Article 7 of the DPL, persons that are involved in the processing of data have a perpetual obligation of confidentiality in regard to the data that have not been obtained from sources that are available to the public.

The issues brought about by cybersecurity in the metaverse have not been specifically addressed through local laws or regulations. However, it is important to mention that the Chilean Congress has recently approved a bill on cybersecurity (CFB), which aims to establish the institutional principles and general regulations to structure, regulate and coordinate the cybersecurity actions of public bodies and between them and individuals, as well as to establish the requirements for the prevention, containment, resolution and response to cybersecurity incidents and cyberattacks.

The bill will be applicable to institutions providing services qualified as 'essential' and those that are qualified as 'operators of vital importance', which could impact cybersecurity requirements in the metaverse, specifically for Chilean users.

The CFB has been published in the country's *Official Gazette* on 8 April 8 2024. The law will come into effect on the date indicated in an executive decree issued by the President of the Republic, which has not yet been issued. Further details of this can be found in the answer to the final question of this chapter.

## **Q 2. What are the security by design principles applicable to the metaverse in your jurisdiction?**

As explained above, there are no general laws on cybersecurity in Chile. Consequently, there are no general legal provisions regarding security-by-design principles.

Notwithstanding the foregoing, certain sectorial regulations have incorporated security-by-design principles and concepts. For example, Exempt Resolution No 1318 of the Undersecretary of Telecommunications ('Subtel'), dated 10 August 2020, approves the technical standards on general cybersecurity fundamentals for the design, installation and operation of networks and systems used to provide telecommunications services, which introduces concepts such as 'non-repudiation' and 'technological neutrality'.

The Chilean National Congress is currently discussing legislation related to security-by-design principles that could have an impact on the future of the metaverse. In this sense, the DPL Bill establishes the principle of security, requiring data controllers to ensure adequate security standards to protect against unauthorised or unlawful processing, as well as loss, leakage, accidental damage or destruction of data. Additionally, it establishes the principle of confidentiality, mandating that both the data controller and those with access to data keep it confidential.

As regards the cybersecurity framework law, it establishes the principle of security and privacy by default and by design, whereby computer systems, applications and information technologies must be designed, implemented and managed with the security and privacy of the personal data they process in mind.

The application and interpretation of these new rules regarding security-by-design will depend on the administrative authorities responsible for overseeing compliance.

## **Q 3. Have there been any cyber-incidents in the metaverse in your jurisdiction? How do the applicable policies, strategies or regulations deal with cyber-incidents?**

We are not aware of any cyber incidents or cyberattacks that have taken place or have affected any type of metaverse in Chile.

As explained above, as of the time of writing, there are no general cybersecurity laws in force in Chile. Consequently, there are no general legal provisions that refer to or specifically regulate the legal consequences of a cyber incident.

The Chilean Cyber Defence Policy addresses the issue of massive cyberattacks against the sovereignty, population, infrastructure or interests of Chile, and establishes that these may be considered as an armed attack, and in accordance with Article 51 of the Charter of the United Nations, may use the means it deems appropriate, both physical and digital, in the exercise of its right to self-defence.

Other laws could have an impact on this issue. For instance, the DPL allows data subjects affected by breaches of security measures to bring claims before the ordinary courts to obtain compensation for the pecuniary and moral damage caused by a lack of diligence in the care of personal data. The court will determine the amount of compensation for the interested parties.

From a consumer protection perspective, cyber incidents may also have an impact on consumer protection matters. In certain cases, cyber incidents may need to be reported or notified to SERNAC, for example, when the interests of consumers have been or could potentially be affected. To avoid or mitigate possible litigation, SERNAC highly recommends that companies take all necessary actions and measures to stop these incidents impacting consumers. Suppliers must act with the corresponding level of diligence and professionalism applicable to their industry.

Additionally, Law 21,459 (the 'Cybercrime Law'), based on the Council of Europe's Convention on Cybercrime, known as the Budapest Convention, includes several rules that allow for the prosecution of criminal offences, such as illegally accessing an information system without a specific purpose; an attack on a computer system, as well as the integrity of its data; the illegal interception of information; and computer-related forgery. Additionally, computer-related fraud is expressly regulated. The Cybercrime Law also sanctions anyone who sells, transfers, or stores in any way computer data,

they know was obtained illicitly, that is, that were obtained through any of the crimes described in the Cybercrime Law. Additionally, the misuse of a device is addressed.

Please consider that the cybercrimes described above may generate criminal liability for legal entities, as they are included in the list of crimes in Law 20,393 ('Economic Crimes 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.

The Chilean Congress is currently considering additional legislation that may have an impact on the response to cybersecurity incidents. As far as the CFB is concerned, the following points are noteworthy: the duty to report cybersecurity incidents with significant effects to the National Computer Security Incident Response Team ('National CSIRT'), a body within the National Cybersecurity Agency; the principle concerning a responsible response, whereby the measures implemented to respond to cybersecurity incidents or cyberattacks may in no case mean carrying out or supporting offensive operations; and the obligation to resolve cybersecurity incidents. For its part, the DPL Bill considers the duty to report breaches of security measures to the Data Protection Agency, and to the data subjects impacted, in certain circumstances.

Finally, we are not aware of any case law or administrative decisions on cybersecurity in regard to this matter.

---

#### **4. Are there any cybersecurity standards in your jurisdiction specifically applicable to the metaverse? What are the main obligations they set out?**

There are currently no specific cybersecurity standards applicable to the metaverse in Chile.

The issues brought about by cybersecurity in the metaverse have not been specifically addressed through local standards. The CSIRT, a body that is part of the Ministry of the Interior to which state administration bodies must report cybersecurity incidents, has defined the metaverse as 'a world beyond the universe comprising a virtual and 3D space where people interact through virtual reality and whose promoters hope, eventually, to enable people to live their lives as in the real world' (CSIRT, Cyber Dictionary, Volume 22, 3, the metaverse) and has not yet provided any cybersecurity guidelines, standards or requirements to be implemented in the metaverse.

However, it is important to note that the National Cybersecurity Agency, which is established by the CFB (Agencia Nacional de Ciberseguridad or ANCI) may in the future set cybersecurity standards specifically applicable to companies engaged in the development or management of the metaverse (if they are considered to be essential service providers or operators of vital importance). For further details, please see the answer below.

---

#### **5. Are there any upcoming policies, strategies or regulations that will impact cybersecurity in the metaverse?**

Yes, as explained, the CFB has recently been approved by the Chilean Congress and has been published in the country's *Official Gazette* on 8 April 2024.. The CFB creates the ANCI and imposes novel cybersecurity requirements on services that are within scope. In particular, all services within scope will need to report security incidents with significant effects to the ANCI within three hours of becoming aware of the incident.

Private institutions that provide 'essential services', such as 'digital infrastructure, digital services and information technology services managed by third parties', as well as those that the ANCI qualifies as being of 'vital importance' within the definition of essential services described in the CFB, will fall within scope of the law and must comply with certain requirements. The ANCI reserves the authority to extend the list of services subject to the requirements in particular situations (eg, where their impact may be relevant to economic activities). The ANCI may also qualify a private institution as an operator of vital importance, even if it does not provide essential services, under certain conditions, such as if it has acquired a critical role in supplying goods or services to the population.

The CFB imposes certain security obligations (such as reporting incidents to the ANCI or adopting technical and organisational measures to prevent breaches) and can impose high penalties for non-compliance, reaching up to almost \$3m in certain cases.

Considering the broad terms used by the CFB to define essential services, it is possible that the metaverse could be classified as 'digital infrastructure' or a 'digital service'. Therefore, institutions involved in the metaverse may be deemed essential services and subject to the provisions of the CFB.

Additionally, the DPL Bill will also have an impact on the security and cybersecurity obligations of data controllers in the metaverse. For instance, it sets forth the following specific security and cybersecurity obligations: (1) to protect privacy by design and by default; (2) to adopt security measures considering the state of the art and the costs of implementation, together with the nature, scope, context and purposes of the processing, as well as the likelihood of the risks posed and the severity of their effects in relation to the type of data processed; (3) to report security breaches to the future Data Protection Agency and also to data subjects in certain circumstances; and (4) to register all communications related to the reporting of security breaches to the future Data Protection Agency or to data subjects, among others.

# Digital identity and authentication

## 1. Are there any digital identity and authentication policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Currently, there are no digital identity and authentication policies, strategies or regulations specifically applicable to the metaverse in Chile. Consequently, authentication methods may be governed by the terms and conditions of each metaverse provider.

In general terms, there is no single way to prove the digital identity of a person in Chile. Law 19,799 on Electronic Documents, Electronic Signatures and Certification Services (the 'ESL') establishes that contracts signed by electronic signature will be valid and produce the same effects as those entered into in writing and on paper. Pursuant to the general provisions in the ESL, one mechanism to prove a person's digital identity in the metaverse would be through the use of an electronic signature, either simple or advanced.

A simple electronic signature is 'any type of sound, symbol or electronic process that enables the recipient of an electronic document to identify, at least formally, its author'.<sup>9</sup> An advanced electronic signature is a signature that is 'certified by an accredited provider and which has been created using means that the holder keeps under his/her exclusive control, so that it is linked only to the holder and the data to which it refers, allowing the subsequent detection of any modification, verifying the identity of the holder and preventing him/her from being unaware of the integrity of the document and its authorship'.<sup>10</sup>

In such a context, it is important to note that a specific digital authentication system has become standard in interactions by individuals with public bodies, the system is known as the 'ClaveÚnica'. The ClaveÚnica is an authentication system whose authentication factor is a password managed by the user and linked to his/her national identity number (*rol único nacional*). Although other authentication mechanisms exist and may exist in the future, the ClaveÚnica has become the official identification mechanism for digital procedures<sup>11</sup> and, in view of the public authorities in the country, is the 'basis of the digital identity model in Chile'.<sup>12</sup>

The ClaveÚnica is regulated by Decree No 9, published on 17 August 2023, issued by the Ministry General Secretariat of the Presidency. The regulation establishes an obligation for public agencies to use the ClaveÚnica for user access to their digital platforms, with some exceptions.

There have been some efforts to integrate the ClaveÚnica into private entities. For example, pursuant to Decree No 24, published on 9 April 2019, issued by the Ministry of Economy, Development and Tourism, electronic signature certification service providers (private entities) may use the ClaveÚnica system when granting an advanced electronic signature certificate. Nevertheless, there are no other formal initiatives to integrate the ClaveÚnica system with private sector services, such as the metaverse.

It is likely that in the future there will be more formal initiatives to integrate the ClaveÚnica system with other private entities (eg, companies involved in the development of the metaverse), particularly because it is one of the OECD's recommendations for Chile.<sup>13</sup>

9 Law 19,799 on Electronic Documents, Electronic Signatures and Certification Services 2002, Art 2, letter f.

10 Law 19,799 on Electronic Documents, Electronic Signatures and Certification Services 2002, Art 2, letter g.

11 Christine Weidenslaufer and Raimundo Roberts, 'Identidad digital: conceptos y legislación' (Biblioteca del Congreso Nacional, October 2022) [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33658/2/Identidad\\_Digital\\_BCN\\_2022.pdf](https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33658/2/Identidad_Digital_BCN_2022.pdf) accessed 16 February 2024.

12 División de Gobierno Digital, SEGPRES, 'Guía Técnica para integración de ClaveÚnica' (Gob Digital, 28 November 2023) [https://cms-dgd-prod.s3-us-west-2.amazonaws.com/uploads/pdf/Guia\\_Tecnica\\_de\\_integracion\\_a\\_ClaveUnica\\_\\_1.pdf](https://cms-dgd-prod.s3-us-west-2.amazonaws.com/uploads/pdf/Guia_Tecnica_de_integracion_a_ClaveUnica__1.pdf) accessed 16 February 2024.

13 Organisation for Economic Co-operation and Development, 'Digital Government in Chile – Improving Public Service Design and Delivery' (OECD Digital Government Studies, 30 May 2020) [www.oecd-ilibrary.org/sites/9ecba35e-en/index.html?itemId=/content/publication/9ecba35e-en&\\_csp\\_=692a35bb643f9f775b9b2c161f8e7ea8&itemIIO=oecd&itemContentType=book](http://www.oecd-ilibrary.org/sites/9ecba35e-en/index.html?itemId=/content/publication/9ecba35e-en&_csp_=692a35bb643f9f775b9b2c161f8e7ea8&itemIIO=oecd&itemContentType=book) accessed 16 February 2024.



## 2. What are the different types of digital identity in the metaverse: what are the different tiers and types of ID and what are the different levels of protection in your jurisdiction?

In Chile, there are no regulations on the different tiers and types of identification in the metaverse or on the different levels of protection related to digital identity in this context.

Due to the lack of regulation, as explained, issues relating to digital identity in the metaverse are likely to be governed by the terms and conditions of the metaverse developers or any other contractual obligations undertaken by metaverse users, as well as by the general rules and principles set forth in the DPL and CPL.



## 3. How is self-determination exercised and protected in the metaverse in your jurisdiction?

There are no regulations on the exercise and protection of self-determination in the metaverse. Therefore, there are no enforceable sanctions, case law or decisions by a regulator on this topic.

However, Chile is already showing interest in limiting the control of different digital platforms and protecting the rights and freedoms of those involved. For instance, in 2021, the Political Constitution was amended by incorporating the protection of 'brain information' (also referred to as 'neurodata' or 'brain data'), which is related to self-determination, into the country's constitutional rights. Also, the bill that regulates digital platforms (addressed in more detail below) establishes the principle of equivalence between digital and physical space by virtue of which every user of a digital platform enjoys at least the same rights and freedoms in the digital environment as in the physical environment and is subject to the same duties and prohibitions.



## 4. How is the role of intermediary ID providers regulated in your jurisdiction? What are some of their main obligations?

The role of each ID provider may be different depending on the use case, as explained below for the ClaveÚnica and for the electronic signatures regulated by the ESL.

The Ministry General Secretariat of the Presidency, through its Digital Government Division, manages the ClaveÚnica, and the Civil Registry and Identification Service is responsible for the enrolment of new users.

As mentioned, the ClaveÚnica has become the official authentication mechanism for individuals in terms of their relationship with public bodies, and its adoption is mandatory by such bodies with certain exceptions. In most cases, the ClaveÚnica allows the user to be identified 'with a certain level of reliability' and, in others, allows for the unequivocal verification of the user's identity (eg, for the purposes of Decree No 24, as mentioned above).

Additionally, concerning the adoption of the ClaveÚnica system, certain technical requirements must be met, such as the following: (1) the system should be based on OpenID Connect and OAuth 2.0 standards, or higher; (2) the user identification data associated with the authentication factors shall be stored in encrypted form, using algorithms such as Bcrypt, PBKDF2, SHA-3 and Argon2, or higher; and (3) data transmission during the authentication process shall be carried out using encrypted communication protocols, such as TLS v1.2, or higher, among others.

In addition, as mentioned above, electronic signatures, whether simple or advanced, could be a way of proving a person's digital identity (ie, ID providers). As regards advanced electronic signatures, the ESL establishes certification service providers for such electronic signatures, which must be accredited before the Under-Secretariat for the Economy and Smaller Businesses (the 'Accreditation Body').

The ESL establishes obligations for providers of such services, such as the following: (1) to have rules on certification practices that are objective and non-discriminatory, which are communicated to users in a simple manner and in Spanish; (2) to maintain a publicly accessible register of certificates; (3) in the event that the activities of a service provider are voluntarily ceased, give prior notice of this situation to each of the holders of electronic signatures certified by them;



(4) to publish on their websites the resolutions by the Accreditation Body that affect them; (5) to unequivocally verify the identity of the applicant prior to the issuance of an advanced electronic signature certificate; (6) pay the supervision fee to the Accreditation Body; (7) request the cancellation of their registration in the register of accredited providers of the Accreditation Body, with no less than one month's notice when they are going to cease their activity and provide information on the destination of the certification data; and (7) indicate to the Accreditation Body any other relevant circumstance that may prevent the continuation of their activities.

---

## **Q 5. Are there any upcoming policies, strategies or regulations that will impact the digital identify and authentication process on the metaverse?**

To the best of our knowledge, there are no upcoming policies, strategies or regulations that will impact the digital identity and authentication process specific to the metaverse.



# AI in the metaverse



## 1. Are there any artificial intelligence (AI) policies, strategies or regulations applicable to AI or the use of AI in the metaverse in your region/country?

Currently, there are no laws that comprehensively regulate AI in Chile or its use in the metaverse.

However, there is a National Artificial Intelligence Policy (the 'Chilean AI Policy'), which establishes the public policy objectives on this matter. The Chilean AI Policy is structured around four cross-cutting principles and three interdependent axes (enabling factors; development and adoption; and ethics, policy issues and socio-economic impacts), and is complemented by an AI action plan.

It is important to note that the Chilean AI Policy establishes several objectives on the ethical use of AI in terms of labour relations, as well as in regard to its relationship with consumers, intellectual property (IP) and cybersecurity, among others. It is expected that these objectives will be reflected in the creation of new laws or legislative amendments.

Additionally, there are sectoral laws and guidelines that specifically regulate some AI-related matters. For instance, the aforementioned Article 152 quinquies E of the Labour Code (incorporated by Law 21,431) prohibits discrimination against employees of digital platforms through automated decision-making mechanisms, along with guidelines issued by the National Consumer Protection Bureau that address the use of AI in consumer relationships in order to safeguard consumer rights.

The emergence and development of the metaverse, and specifically the use of AI in relation to it, brings with it a number of issues that will need to be addressed, such as the use and functions of AI when interacting with users in the metaverse (eg, which uses will be completely prohibited and the conditions for biometric identification through AI).

The issues brought about by AI in the metaverse have not been specifically addressed through local laws or regulations. However, it is important to mention that the Chilean Congress is currently discussing a bill on AI ('AI Bill'), which aims to establish a legal framework for the development, commercialisation, distribution and use of AI systems, thereby safeguarding the fundamental rights enshrined in the constitution. The AI Bill would be applicable to any AI system used in Chile and could impact the use of AI in the metaverse, specifically in relation to Chilean users.

The Chilean AI bill is explained in more detail below.



## 2. How is transparency and accountability in regard to AI ensured in your jurisdiction?

As explained above, there are no general laws on AI in Chile. Consequently, there are no specific legal provisions to ensure transparency and accountability in the use of AI in general.

However, some of the aforementioned legal provisions could contribute to ensuring transparency and accountability. For instance, the cited Article 152 quinquies E of the Labour Code forbids discrimination of employees through automated decision-making mechanisms, penalising such an infringement with fines of up to 60 UTM in the case of large companies (which may be doubled in the event of a repeat offence).

In addition, under Law 20,285 on access to public information of 2008 (the 'Transparency Law'), an individual may request that a public body provide information on the AI algorithm used by that body and how it works.

According to the Article 10 of the Transparency Law, every person has the right to request and receive information from any public body under the conditions set out in the law. The public body must disclose the information within 20 business days (extendable up to 30 days), unless there is a third-party objection, or an exception or reason for confidentiality or secrecy. In the case of a denial concerning the disclosure of information or a failure to disclose the information within the statutory period, the applicant has the right to file a claim before the Council for Transparency in order to be granted



access to the information. Decisions by the Council for Transparency can be challenged through a judicial remedy called a 'claim of illegality', which can be filed before the competent Court of Appeal.

Therefore, the Transparency Law could be a way to ensure transparency in regard to the use of AI. It is important to mention that there is also a data repository managed by a Chilean university that collects and displays information on automated decision support systems that have been developed and/or are being used by public institutions in Chile.

Also, although not mandatory for suppliers, the National Consumer Protection Bureau's guidelines on the protection of consumers' rights with regard to the use of AI systems in consumer relationships requires, among other things, the provision of truthful, timely and transparent information to the consumer, such as: (1) the purpose or aim of the AI systems used; (2) how they impact the contracting process or the performance of the contract, if applicable; (3) the nature of the interrelationship of the AI system with the consumer, where applicable (in particular, whether the consumer is interacting with an AI system and not with a human being, together with the associated implications); and (4) the personal data that are processed by the system. All of this is aimed at ensuring more transparency around such systems for consumers.

In addition, as regards non-mandatory guidelines, the Chilean AI Policy specifically states that one of its objectives is to establish standards and recommendations for algorithmic transparency for critical applications. In this sense, the Chilean AI Policy requires that the provision of information on how the decision-making algorithms used by public bodies work, as well as the data involved in such decision-making, including the training phase, must be timely and clear. Also, it addresses the issue of algorithmic bias, as explained in more detail below.

Other laws that could have an impact on this issue are also currently under discussion by the Chilean National Congress. For instance, the DPL, which is currently subject to its third constitutional procedure, allows data subjects to object and not be subject to decisions based on automated processing of their personal data, including profiling, which produces legal effects or significantly affects them, requiring the data controller to take the necessary measures to ensure the rights and freedoms of data subjects, their right to information and transparency, and the right to obtain an explanation, to request human intervention, to express their point of view and to request a review of a decision.

In some cases, pursuant to the Transparency Law, individuals have made requests to a public body for information on an AI algorithm used by that body. For instance, on 28 June 2019, an individual requested from the Undersecretary of Public Health information on the prioritisation algorithm used for the waiting list for the public healthcare system. This public body did not respond to the request within the legal term, which led the applicant to file a claim before the Council for Transparency, and the information was finally provided during this process (although not by order of the Council for Transparency).

Moreover, it is relevant to mention from a consumer protection standpoint that the CPL sets forth information duties that require suppliers to provide sufficient information in order to ensure transparency, objectiveness and informed decision-making processes by consumers. These duties relate to the consumers' fundamental right to not be arbitrarily discriminated against by suppliers in the provision of goods and services, and that any difference in the treatment of consumers must be based on well-informed objective conditions. Failure to comply with these information duties may be sanctioned with a fine of up to 300 UTM. The same sanctions may be imposed in the case of unjustified discriminatory actions, plus damages, if applicable.

However, considering the lack of specific regulation, we are not aware of any other relevant case law or administrative decisions on transparency and accountability related to this matter.



### **3. How is algorithmic bias mitigated in your jurisdiction? Are there any policies, strategies or regulations aimed at promoting fairness and non-discrimination?**

There are no general regulations to mitigate algorithmic bias. However, there may be specific legal provisions that contribute to mitigating this bias, such as Article 152 quinquies E of the Labour Code regarding digital platform employees. Pursuant to this article, the digital service platform company must respect the principle of equality and non-discrimination and take all necessary measures and safeguards to avoid any kind of discrimination among employees, particularly in the allocation of work, the offer of bonuses and incentives, and the calculation of remuneration, among others. As mentioned, an infringement of this rule may be sanctioned with fines of up to 60 UTM in the case of large companies (which may be doubled in the event of a repeat offence).



Furthermore, as previously mentioned, from a consumer protection standpoint, although there are no specific measures to mitigate algorithmic bias, suppliers may diligently take all action necessary to ensure that no instances of arbitrary discrimination affect consumers. The CPL sanctions suppliers who unjustifiably discriminate against consumers in the offer and provision of goods and services, with a fine of up to 300 UTM plus damages. Consumers or SERNAC may file claims before the courts in order to request the imposition of fines and compensation for damages.

In addition, as already mentioned, the Chilean AI Policy establishes that care must be taken to identify bias in algorithms, databases and other components of AI systems, and to mitigate the risks of affecting fundamental rights, especially rights related to privacy and the protection of personal data. As a public policy instrument, non-compliance does not entail any penalty or fine.

Moreover, the current version of the AI Bill requires that an AI system classified as high risk must comply with several requirements prior to authorisation, including having an input data management plan that includes the assessment of potential bias and the identification of potential gaps or deficiencies in the data and how to address them.

We are not aware of any case law or administrative decisions related to this matter.



#### **4. What is the intellectual property law treatment of AI-generated content used in the metaverse in your jurisdiction? Who are the rightsholders of such content?**

There are no laws regulating the IP rights of AI-generated content used in the metaverse. Consequently, the issue of ownership regarding AI-generated content has been addressed on the basis of the existing IP legislation, which has been understood to protect only works that are the result of human intelligence, not AI.<sup>14</sup>

On the basis of the current legislation, it could be argued that if the content is generated solely by AI, it would not be properly protected by IP rights; instead, if the content is developed with the assistance of AI and there is sufficient human intervention, it could be a work that is protected by IP rights. The Department of Intellectual Rights (ie, the agency in charge of managing the registration system related to copyright and related rights) has adopted a similar criterion and, for instance, has accepted the registration of images made with the assistance of the AI tool Midjourney provided there is sufficient human intervention.<sup>15</sup>

Given that the situation is not legally established, it is not clear who would be the rightsholder in situations where the work is protectable by IP rights, but it will probably be the party that deployed the creative effort (if any) to develop the work with the contribution of AI (eg, through the selection of prompts or changes in the output delivered by the AI tool).



#### **5. Which stakeholders are liable for any damage caused to third parties due to the use of AI in the metaverse? What sanctions (civil, criminal or administrative) may apply in the case of an infringement?**

There are no specific rules on the attribution of liability in such a case. However, the general rules on civil liability may apply, which are explained in more detail in the chapter on liability and insurance.

We are not aware of any case law or administrative decisions on this matter.

14 Ana Karin Chávez, 'Rediseñando la titularidad de las obras: Inteligencia artificial y robótica' (2020) 9(2) Revista Chilena de Derecho y Tecnología, 153 <https://rchdt.uchile.cl/index.php/RCHDT/article/view/57674/64366> accessed 19 February 2024.

15 Nicolás Mladinic, 'Es oficial: Aprobado Certificados por derechos de autor de mis fotos con IA en Chile' (LinkedIn, 4 December 2023) <https://linkedin.com/pulse/es-oficial-aprobado-certificados-por-derechos-de-mis-nicol%C3%A1s-x8dve/?originalSubdomain=es> accessed 19 February 2024.

## 6. Are there any upcoming policies, strategies or regulations that will impact AI in your jurisdiction?

Yes, as explained, the AI Bill is currently being discussed by the Chilean National Congress, which aims to establish a legal framework on the matter.

The AI Bill includes the following main aspects: (1) it creates a National Commission on AI with various powers, such as to rule on applications for authorisation submitted by developers, suppliers and users of systems, to develop recommendations to improve the regulation of AI systems, to prepare an annual report on AI systems, to create and maintain the registry of AI systems indicated in this regulation, and to rule on serious incidents or malfunctions of AI systems; (2) it classifies AI systems according to risk (unacceptable risk and high-risk AI systems); (3) it establishes obligations for developers, suppliers and users of AI systems, such as requests for authorisation from the commission prior to initiating the development, commercialisation, distribution and use of the AI system and to report to the commission about serious incidents or malfunctions of AI systems; and (4) it establishes penalties associated with non-compliance with the law, which could amount to 400 UTM , including criminal liability in some cases. It is important to note that the bill states that persons involved in the authorisation procedure of the AI system must respect, among other things, IP rights and confidential business information.

Although the AI Bill will probably have many amendments during the legislative process, we strongly recommend analysing the AI Bill in detail, once enacted, and how AI works in the metaverse to assess possible risks.

Also, as explained below, a bill of law from 2021 is being discussed by the Chilean National Congress that aims to regulate digital platforms, which, among its rules, establishes that digital consumers have the right to be informed every time they interact with algorithms or AI tools. Additionally, it establishes that digital platforms should have mechanisms in place to identify whether the publication of content is made by a person or AI.



# Human rights, accessibility and digital ethics



## 1. Are there any human rights, accessibility and digital ethics strategies, policies and regulations applicable to the metaverse in your jurisdiction?

There are no human rights, accessibility and digital ethics strategies, policies or regulations directly applicable to the metaverse.

However, Chile has signed and ratified various treaties on human rights, such as the Universal Declaration of Human Rights; the American Declaration of the Rights and Duties of Man; the International Covenant on Civil and Political Rights; the American Convention on Human Rights; the International Covenant on Economic, Social and Cultural Rights; and the Convention on the Rights of the Child.

Therefore, many of the rights and principles established by these international instruments could be applied by extension in the context of the metaverse. For instance, these rights include freedom of expression, the protection of personal data and privacy, the freedom of thought, equality, and non-discrimination and inclusion.



## 2. Considering the various health risks associated with the metaverse and related technologies, are there any strategies, policies or regulations in your jurisdiction aimed at protecting public health?

There are no strategies, policies or regulations aimed directly at protecting health in the metaverse. In Chile, the phenomenon of health protection from the harmful effects derived from technology and digital platforms, which could include the metaverse in the future, has not been directly addressed by legislators or public authorities. However, general rules on this topic could be applicable.

Concerning the general regulation on health, Article 19 No 9 of the Political Constitution of 1980 ensures free and equal access to healthcare, whether in regard to actions on promotion, protection, recovery or rehabilitation. It is the duty of the state to guarantee the execution of health-related actions, whether via the public or private system. People can choose whether to be treated by the public or private system. Furthermore, this right is enshrined in multiple international treaties signed and ratified by Chile.

In the field of public health, a violation of this right by health workers could result in administrative liability.

Also, Law 20,584 of 2012, which regulates the rights and duties of individuals in relation to actions related to healthcare, allows providers to offer digital health services, appointments and procedures aimed at the prevention, promotion, protection, recovery or rehabilitation of people's health. The applicable regulations require providers who implement technological tools in this field to, among other things: (1) enable the unequivocal identification of both patients and intervening healthcare professionals and technicians; (2) implement technological neutrality; (3) guarantee the secure transmission of data and clinical information necessary for the provision of the service; and (4) allow the traceability and registration of actions carried out by such tools.

Sanctions for non-compliance will apply to public and private healthcare providers (which could indirectly impact the company that owns the metaverse) and can lead to fines of up to 1,000 UTM (depending on the infraction and its severity) and other non-pecuniary sanctions (eg, removal from the registry of healthcare providers).

Considering the lack of rules applicable specifically to the metaverse, we are not aware of any case law or regulatory decisions on this topic.

### **3. Considering the various discrimination risks associated with the metaverse and related technologies, are there any strategies, policies or regulation in your jurisdiction aimed at ensuring non-discrimination?**

There are no strategies, policies or regulations to ensure non-discrimination in the metaverse.

As to the general regulation on non-discrimination, Law 20,609 stands out, establishing measures against arbitrary discrimination and a judicial procedure to re-establish the right when an act of that type is committed. It is noteworthy that the provisions in this law may be applicable to individuals, private entities and public bodies.

Considering its broad scope of application, the provisions in Law 20,609 could be applicable to the metaverse.

Sanctions for non-compliance with Law 20,609 could lead to civil and administrative liability. Fines for an act of arbitrary discrimination can reach up to 50 UTM, which will be used for the public benefit.

In addition, from a telecommunications law perspective, non-discrimination in regard to access to the internet, applications (such as the metaverse) or legal services or activities are regulated in Chile by the rules on net neutrality.<sup>16</sup> In accordance with the aforementioned regulations, internet service providers (ISPs) cannot arbitrarily discriminate against the right of any user to send, receive or offer any content, application or legal service through the internet, as well as any other activity or legal use performed through the network. As the metaverse may be in the form of an application, an over-the-top service and/or any other kind of legal internet service, net neutrality is an anti-discrimination rule regarding access to the metaverse. For a more detailed description of these regulations and the sanctions involved, please see our answer below.

Also, as explained above, Article 19 No 1 of the Political Constitution was amended in 2021 to incorporate the protection of brain activity and the information coming from it. In this regard, a bill was presented in 2020 that aims to protect neurorights and mental integrity, and the development of research and neurotechnologies. For instance, this bill establishes that the freedom to carry out neuroscience procedures and to use neurotechnologies will always be limited by human rights, that the state must allow access to advances in neuroscience and neurotechnologies without discrimination, as well as establishing civil and criminal sanctions for non-compliance with the bill's provisions.

We are not aware of any case law or decisions by a regulator regarding the infringement of general non-discrimination rules in the metaverse.

### **4. Considering the risks to the freedom of expression and censorship associated with the metaverse, are there any strategies, policies or regulations in your jurisdiction aiming to mitigate them/promote the freedom of expression and non-censorship?**

There are no strategies, policies or regulations on the protection of the freedom of expression and non-censorship in the metaverse.

As to the general regulation, the freedom of expression is enshrined in Article 19 No 12 of the Political Constitution. This right is also enshrined in various international treaties signed and ratified by Chile, such as the Universal Declaration of Human Rights (Articles 18 and 19), the International Covenant on Civil and Political Rights (Article 19) and the American Convention on Human Rights (Article 13).

At a legal level, Law 19,733 ('Press Law') regulates some aspects of the principle of the freedom of expression, especially in the context of the media. Penalties for non-compliance with the Press Law go up to 30 UTM. Likewise, the Transparency Law also regulates access to public information, which is related to enforcement concerning the freedom of expression. Sanctions for non-compliance with this law can lead to administrative liability by the respective public official.

In addition, from a telecommunications law perspective, the freedom of expression and censorship are also regulated through the rules designed to safeguard net neutrality, mentioned above. In accordance with the aforementioned

<sup>16</sup> Law 18,168, the General Telecommunications Law, and Decree 368/2011, the Net Neutrality Regulation, from the Undersecretary of Telecommunications.



regulations, ISPs may not censor certain applications or content at their own will, because they need to follow strict rules in this regard. Indeed, as mentioned before, ISPs cannot arbitrarily block, interfere with, discriminate against, hinder or restrict the right of any internet user to use, send, receive or offer any content, application or legal service through the internet, as well as any other activity or legal use performed through the network.

Additionally, ISPs must provide to their users or other ISPs that have a contract to use their connectivity services, internet access that does not arbitrarily distinguish between content, uses or services, based on the source or ownership thereof.

Moreover, the Net Neutrality Regulation specifies the aforementioned rules stating, among other matters, that every action that arbitrarily prioritises or discriminates between content providers, applications or users will be considered as a practice restrictive of the freedom of utilisation of content, applications or services provided through the internet.

Notwithstanding the above, please bear in mind that there are three lawful exceptions to the net neutrality rules mentioned above. Indeed, certain blocking or censorship of applications or content may apply when required: (1) by a court order; (2) by the ISP at the request of a user at his/her own expense; or (3) by the ISP without a third-party request if the content is illegal.

In our opinion, although the net neutrality rules are aimed at ISPs, they could impact relevant metaverse functionalities because they prevent censorship and may affect the availability of the service.

In this sense, the net neutrality rules are a guarantee to applications, over-the-top services, content providers and/or legal internet services in general, with metaverse operators included, that their applications or content cannot be arbitrarily blocked by an ISP and, consequently, that the general public has the right to access the metaverse if it is not deemed to be illegal, safeguarding in this manner the freedom of information.

As regards sanctions, non-compliance with the net neutrality rules could result in the application of administrative sanctions by Subtel, which may vary from a written admonition to a fine for approximately \$340–\$65,000. This fine may be trebled in the case of repeat offences. Also, if the fine is not paid within 30 days from the moment in which the corresponding authority's resolution is enforceable, that circumstance may lead to the cancellation (*caducidad*) of the applicable licence. Please also note that each day that passes after being notified by the regulator of the relevant infraction will be considered a new infringement. In any case, a sanction may be imposed by the authority only after a charge proceeding is duly notified and opened against the corresponding offender. In this kind of proceeding, the alleged offender always has the opportunity to present a defence.

Since there is no direct regulation on the protection of the freedom of expression and censorship in the metaverse, we are not aware of any case law or regulatory decisions on this topic.



## 5. Considering the risk of misinformation and the risks associated with fake news and deep fakes in the metaverse, are there any strategies, policies or regulations in your jurisdiction aiming to mitigate them/promote the freedom of expression and non-censorship?

There are no current laws or regulations specifically applicable to fake news and deep fakes in the metaverse. Accordingly, there are no sanctions that may apply or, to the best of our knowledge, any case law or decisions by a regulator on this matter.

However, it is worth noting the creation, in 2023, of an advisory commission, dependent on the Ministry of Science, Technology, Knowledge and Innovation to study disinformation in the country. The commission has issued two reports referring to issues concerning fake news and disinformation, with a special emphasis on digital platforms.<sup>17</sup>

In addition, there are some bills currently being discussed by the Chilean National Congress. For example, one bill seeks to criminalise the spread of fake news<sup>18</sup> and another seeks to regulate disinformation by modifying the Press Law.<sup>19</sup>

<sup>17</sup> Advisory Committee against disinformation, 'Recommendations to Counter Disinformation In Chile' (Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, 2023) <https://drive.google.com/file/d/1JqqYP4WrAnGJcomluGor4PrxVvTwT1tT/view> accessed 27 February 2024.

<sup>18</sup> See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16611&prmBOLETIN=16068-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16611&prmBOLETIN=16068-07) accessed 3 June 2024.

<sup>19</sup> See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16698&prmBOLETIN=16146-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16698&prmBOLETIN=16146-07) accessed 3 June 2024.

Also, there are other bills that have an impact on this issue and penalise or aggravate criminal liability for deepfakes (specifically, in the context of the use of AI), such as the bill that amends the Criminal Code to punish the misuse of AI,<sup>20</sup> the bill that amends the Criminal Code to incorporate, as an aggravating circumstance of liability, the use of AI in the commission of an offence,<sup>21</sup> and the bill that amends the Criminal Code as regards the offence of identity theft in the context of the use of AI.<sup>22</sup>

## 6. Are there any strategies, policies or regulations in your jurisdiction aimed at ensuring accessibility and inclusion in the metaverse? How are they enforced?

There are no strategies, policies or regulations aiming to ensure accessibility and inclusion in the metaverse. However, the general rules on accessibility and inclusion could be applicable.

Law 20,422 of 2010 provides the general regulation on accessibility and inclusion, which establishes standards for equal opportunities and social inclusion for people with disabilities. This law seeks to guarantee equal opportunities for disabled people and promote their inclusion.

Law 20,422 establishes as a principle that environments, processes, goods, products and services, as well as objects or instruments, tools and devices must be understandable, usable and practical for all people, in conditions of safety and comfort, in as autonomous and natural a way as possible. This principle could apply to both public and private institutions, which could include companies developing or managing the metaverse.

Penalties for non-compliance with this law, in the case of an affected individual, can be up to 120 UTM.

In addition, from a telecommunications law perspective, Subtel is currently promoting a government plan called the Zero Digital Gap Plan (Plan Brecha Digital Zero), which seeks to allow connectivity and, consequently, access to the metaverse for all residents in Chile regardless of where they live in the country or their economic circumstances. To achieve this purpose, the government is working on a series of policies and regulations. In this sense, the government has presented a bill of law before the National Congress, which aims to recognise internet access as a public telecommunications service and, among other policies, it allows the payment of internet access service bills to be subsidised for the most vulnerable users in the national territory.<sup>23</sup> In addition, new telecommunications infrastructure projects are being developed, which also consider strategies to prevent the theft of telecommunications cables in vulnerable zones. As already mentioned, all these efforts seek to improve internet accessibility in Chile, which will in turn allow more users to have the possibility to connect to the metaverse.

We are not aware of any case law or regulatory decisions on this topic.

## 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring the protection of minors on the metaverse?

There are no policies, strategies or regulations that aim to ensure the protection of minors in the metaverse. However, the general rules on the protection of minors could be applicable.

Law 21,430 of 2022 guarantees and offers comprehensive protection on the rights of children and adolescents, which provides the general regulation on the protection of minors. The purpose of this law is to establish a statute to guarantee and offer comprehensive protection on the rights of children and adolescents, which makes possible their enjoyment and effective exercise of such rights by them, with emphasis on those human rights recognised in the Political Constitution, the UN Convention on the Rights of a Child, the other international treaties ratified by Chile, and in the applicable laws.

20 See [www.senado.cl/appsenado/templates/tramitacion/index.php?boletin\\_ini=15935-07](http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=15935-07) accessed 3 June 2024.

21 See [www.senado.cl/appsenado/templates/tramitacion/index.php?boletin\\_ini=16021-07](http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=16021-07) accessed 5 June 2024.

22 See [www.senado.cl/appsenado/templates/tramitacion/index.php?boletin\\_ini=16112-07](http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=16112-07) accessed 5 June 2024.

23 Please be advised that this is a bill of law and its provisions may be modified during the proceedings before the National Congress of Chile.



Law 21,430 applies to all individuals, companies or public bodies. In this regard, such law establishes that every person, institution or group must respect and facilitate the exercise of children's rights. For instance, among other obligations, it is established that no child or adolescent may be subjected to arbitrary or unlawful interference with his/her private life, family, home or correspondence, and has the right to the protection of his/her personal data, as well as the right to prevent the processing or transfer of his/her personal data.

Sanctions may involve administrative and even criminal liability in some cases, but, in general, the rules are focused on public bodies and private institutions that perform the public function of providing protection, promotion, prevention, restitution or reparation of the rights of children and adolescents.

In addition, from a telecommunications law perspective, the net neutrality rules set forth an obligation for ISPs to offer, at the expense of the user that requests it, parental control services for content that violates the law, morals or customs, provided that the user is informed in advance and in a clear and precise manner regarding the scope of such services.

We are not aware of any relevant case law or regulatory decisions on this matter.



## 8. Are there any policies, strategies or regulations in your jurisdiction focused on ethics-by-design in regard to the metaverse? How are these rules enforced?

There are no policies, strategies or regulations focused on ethics-by-design in regard to the metaverse. Therefore, there are no enforceable sanctions, case law or regulatory decisions on this topic.



## 9. Are there any upcoming policies, strategies or regulations impacting human rights, accessibility and digital ethics requirements in the context of the metaverse in your jurisdiction?

There are a few bills currently being discussed by the National Congress related to human rights, accessibility and digital ethics requirements. These include the following:

- a bill introduced in September 2021 for the regulation of digital platforms (Bulletin No 14561-19<sup>24</sup>), which aims to regulate digital freedom of expression, mandates the protection of vulnerable people and prohibits discrimination on digital platforms, among other things;
- a bill introduced in August 2023 that modifies several legal bodies to protect people from information disruption on digital platforms (Bulletin No 16206-07<sup>25</sup>), which aims to reduce information disorders caused by the creation, publication, dissemination, promotion or financing of false, harmful or illegal content, as well as hate speech on digital platforms; seeks to protect people impacted by these practices; and addresses concepts such as disinformation, erroneous, harmful, illegal information and hate speech;
- the AI Bill was put forward in April 2023, which aims to regulate AI systems, robotics and connected technologies, in the different areas of application (Bulletin No 15869-19<sup>26</sup>); please see the chapter on AI and the metaverse for further details;
- the CFB; please see the chapter on cybersecurity for further details; and
- the DPL Bill; please see the chapter on data for further details.

24 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15047&prmBOLETIN=14561-19](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15047&prmBOLETIN=14561-19) accessed 3 June 2024.

25 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07) accessed 3 June 2023.

26 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07) accessed 3 June 2024.



# Competition law

## 1. Are there any competition strategies, policies or regulations applicable to the metaverse in your jurisdiction?

There are no specific strategies, policies or regulations related to competition issues applicable to the metaverse in Chile.

However, the economic agents that operate or are active in the Chilean market, or whose conduct may generate actual or potential effects in Chile, are subject to the general provisions set forth in Law Decree No 211 of 1973<sup>27</sup> ('DL 211'). DL 211, with its modifications, is the law responsible for establishing the system for the defence and protection of competition in Chile.

Despite the lack of specific regulation in connection to the metaverse, the criteria established by the country's competition authorities (ie, the National Economic Prosecutor's Office (Fiscalía Nacional Económica or FNE) and the Competition Court (Tribunal de Defensa de la Libre Competencia or TDLC)) regarding the assessment of digital markets, established both in recent case law and in promotional materials, as explained below, delivers relevant guidelines on DL 211's application.

## 2. Are there any strategies, policies, regulations or best practices on how to carry out an antitrust/competition risk assessment?

DL 211 establishes both the conduct considered anti-competitive and the respective sanctions. It also establishes the authorities responsible for enforcement, with their corresponding faculties and procedures.

Regarding anti-competitive conduct, DL 211 establishes under broad terms that any event, action or agreement that impedes, restricts or hinders competition, or that tends to produce such effects, shall be sanctioned. Notwithstanding the aforementioned, DL 211 also outlines examples of certain practices that are considered, among others, to be anti-competitive, which include the following: (1) collusion; (2) unilateral conduct, such as abuse of a dominant position and predatory pricing; (3) interlocking; and (4) infringement of the obligations arising from the merger control procedure (ie, gun jumping).

The FNE has issued several guidelines, which are relevant for assessing the extent of each type of conduct and to clarify the FNE's criteria on different issues, such as vertical restraints,<sup>28</sup> horizontal concentrations<sup>29</sup> and turnover thresholds.<sup>30</sup>

In addition, Title IV of DL 211 establishes a mandatory ex ante merger control system for transactions that: (1) qualify as concentration operations; (2) have effects in Chile; and (3) meet or exceed certain sales thresholds established by the FNE.

Chilean legislation provides the following sanctions on this matter:

- Sanctions in connection with competition law: Article 26 of DL 211 establishes that the TDLC may impose any of the following sanctions: the modification or prohibition of the acts or contracts that are contrary to the provisions of DL 211; the modification or dissolution of the legal entities involved in infringements of competition law; and the application of fines up to the equivalent of 30 per cent of the offender's sales from the products or services related to the infringement during the time period in which the conduct was committed or for up to double the economic benefit obtained by the infringement. If it is impossible to determine the sales and the economic benefit, the TDLC can apply fines of up to 60,000 annual tax units (unidad tributaria annual or UTA). For cartel cases, the temporary prohibition of contracting with public bodies can be applied; and in the case of breaches of the duty to mandatorily notify a transaction,

<sup>27</sup> See [www.bcn.cl/leychile/navegar?idNorma=236106](http://www.bcn.cl/leychile/navegar?idNorma=236106) accessed 3 June 2024.

<sup>28</sup> See [www.fne.gob.cl/wp-content/uploads/2017/10/Gu%C3%ADa-Restricciones-Verticales.pdf](http://www.fne.gob.cl/wp-content/uploads/2017/10/Gu%C3%ADa-Restricciones-Verticales.pdf) accessed 3 June 2024.

<sup>29</sup> See [www.fne.gob.cl/wp-content/uploads/2022/05/20220531.-Guia-para-el-Analisis-de-Operaciones-de-Concentracion-Horizontales-version-final-en-castellano.pdf](http://www.fne.gob.cl/wp-content/uploads/2022/05/20220531.-Guia-para-el-Analisis-de-Operaciones-de-Concentracion-Horizontales-version-final-en-castellano.pdf) accessed 3 June 2024.

<sup>30</sup> See [www.fne.gob.cl/wp-content/uploads/2017/10/Guia-Interpretacion-Umbrales-1-1.pdf](http://www.fne.gob.cl/wp-content/uploads/2017/10/Guia-Interpretacion-Umbrales-1-1.pdf) accessed 3 June 2024.

finances for up to 20 UTA may be applied for each day of delay, from the day when the operation came into force.

- Civil sanctions: Article 30 of DL 211 establishes that claims for damages brought before the TDLC shall be compatible with the fines and criminal sanctions that may be applied, provided that they are filed based on previous rulings issued by the TDLC.
- Criminal sanctions: Article 62 of DL 211 contemplates prison penalties in cases of collusion, as well as the inability to hold administrative positions in public or private entities, among other sanctions.

The aforementioned rules have been applied by Chilean competition authorities in a large number of cases,<sup>31</sup> the majority of which concern traditional markets.

However, the FNE has recently shown a tendency to take a closer look at the competitive variables specific to digital markets and online platforms. In this sense, the FNE's Guidelines for the Analysis of Horizontal Mergers (Guía para el Análisis de Operaciones de Concentración Horizontales<sup>32</sup>), recently updated in 2022, dedicates a special section to digital platforms.

This interest in digital markets is also reflected in recent investigations that the FNE has carried out. For example, in 2021, the FNE initiated an investigation regarding the country's three main digital restaurant platforms, which recently ended with out-of-court settlements,<sup>33</sup> in which all the companies involved committed to modifying their contracting conditions to promote competition.

In a similar vein, in 2022, the FNE initiated a market study regarding Chile's digital accommodation market.<sup>34</sup> In its preliminary report, the regulator refers to the far-reaching impact that digital platforms will have on the development of the industry and identifies some regulatory gaps that could be addressed to further promote competition.



### 3. What are the rules regarding market dominance and barriers to entry applicable to the metaverse in your jurisdiction?

As previously mentioned, there are no specific competition rules applicable to the metaverse in Chile.

However, unilateral conduct, such as exclusionary and exploitative practices, is covered by DL 211 and, hence, could be relevant. Specifically, Article 3 b) penalises the abusive exploitation of a dominant position in the market, while Article 3 c) penalises predatory practices, or unfair competition, carried out with the aim of achieving, maintaining or increasing a dominant position. These types of unilateral conduct are analysed on a case-by-case basis.

In this sense, the types of practices covered by Article 3 DL 211 could refer to exclusivity agreements or incentives (eg, conditional exclusive rebates), arbitrary price discrimination, tied sales, resale price fixing, predatory pricing and unjustified refusal to sell, among others.

When analysing these types of conducts, the FNE weighs their actual and potential anti-competitive effects, and the possible efficiencies that may result from them. For this assessment, the FNE will traditionally analyse whether the undertakings have a dominant position,<sup>35</sup> the market conditions (such as entry and exit barriers) the effects of the conduct and the potential efficiencies.

31 A brief overview of the most recent case law from the TDLC is accessible through the TDLC's yearly report (Anuario Público) [www.tdlc.cl/anuarios-tdlc/](http://www.tdlc.cl/anuarios-tdlc/) accessed 21 August 2024. On a similar note, the FNE publishes a yearly report (Cuenta Pública Participativa) where it highlights some of its most relevant actions and investigations throughout the past year [www.fne.gob.cl/wp-content/uploads/2023/05/Cuenta-Publica-Final-290523-JG.pdf](http://www.fne.gob.cl/wp-content/uploads/2023/05/Cuenta-Publica-Final-290523-JG.pdf) accessed 3 June 2024.

32 See [www.fne.gob.cl/wp-content/uploads/2022/05/20220531.-Guia-para-el-Analisis-de-Operaciones-de-Concentracion-Horizontales-version-final-en-castellano.pdf](http://www.fne.gob.cl/wp-content/uploads/2022/05/20220531.-Guia-para-el-Analisis-de-Operaciones-de-Concentracion-Horizontales-version-final-en-castellano.pdf) accessed 3 June 2024.

33 National Economic Prosecutor's Office, 'TDLC aprueba acuerdos extrajudiciales firmados entre la FNE y las plataformas Uber Eats, PedidosYa y Rappi que eliminan las cláusulas de nación más favorecida en contratos con restaurantes' (FNE, 28 December 2023) [www.fne.gob.cl/tdlc-aprueba-acuerdos-extrajudiciales-firmados-entre-la-fne-y-las-plataformas-uber-eats-pedidosya-y-rappi-que-eliminam-las-clausulas-de-nacion-mas-favorec/](http://www.fne.gob.cl/tdlc-aprueba-acuerdos-extrajudiciales-firmados-entre-la-fne-y-las-plataformas-uber-eats-pedidosya-y-rappi-que-eliminam-las-clausulas-de-nacion-mas-favorec/) accessed 28 February 2024.

34 See [www.fne.gob.cl/wp-content/uploads/2023/12/Resumen\\_Ejecutivo\\_IP\\_VF-EM08.pdf](http://www.fne.gob.cl/wp-content/uploads/2023/12/Resumen_Ejecutivo_IP_VF-EM08.pdf) accessed 3 June 2024.

35 In connection with this issue, the FNE's Guidelines on Vertical Restraints state that the FNE will generally consider a vertical restriction to be lawful when the market share of the seller and the buyer is each 35 per cent or less. FNE (2014), 'Guía para el Análisis de Restricciones Verticales' [www.fne.gob.cl/wp-content/uploads/2017/10/Gu%C3%ADa-Restricciones-Verticales.pdf](http://www.fne.gob.cl/wp-content/uploads/2017/10/Gu%C3%ADa-Restricciones-Verticales.pdf) accessed 3 June 2024.

Regarding the sanctions applicable to these types of conduct and relevant case law, please see our previous answer.

---

#### **4. Are there any specific gatekeepers' obligations applicable to the metaverse in your jurisdiction?**

There are no rules that establish specific obligations for gatekeepers in Chile. Therefore, there are no specific sanctions, case law or regulatory decisions on this specific topic.

---

#### **5. Are there any competition strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote standardisation and access to fair and non-discriminatory licences?**

There are no specific competition strategies, policies or regulations applicable to the metaverse in Chile that aim to promote standardisation and access to fair and non-discriminatory licences. Therefore, there are no specific sanctions, case law or regulatory decisions on this specific topic in the context of the metaverse.

---

#### **6. Are there any competition strategies, policies or regulations in your jurisdiction that aim to promote interoperability in the metaverse?**

There are no competition strategies, policies or regulations in Chile that aim to promote interoperability in the metaverse. Therefore, there are no specific sanctions, case law or regulatory decisions on this specific topic in the context of the metaverse.

---

#### **7. Are there any upcoming policies, strategies or regulations that will have an impact on competition in your jurisdiction?**

Yes. The Economic Crimes Law could have an impact on competition. This law establishes the criminal liability of legal entities for collusion offences. However, the collusion offences established in Article 62 of DL 211 will not apply to legal entities until the procedural statute coordinated with the administrative sanctions is legally regulated, which has not been implemented to date.

Although there are several legislative bills regarding competition regulation, as of this date they have not made significant progress. An important part of these bills seeks to strengthen the criminal penalties associated with competition infringements, as well as to grant more powers to the FNE.

Additionally, the Ministry of Economy, Development and Tourism is currently working on the analysis and evaluation of possible improvements to DL 211, related to the streamlining of the procedures regulated by this legal body.



# Intellectual property

## **Q 1. What are the public policies, strategies or regulations relating to intellectual property which are applicable to the metaverse in your jurisdiction?**

There are no public policies, strategies or regulations on intellectual property (IP) applicable to the metaverse in Chile.

## **Q 2. How are intellectual property rights concerning ‘virtual objects’, ‘buildings’ and ‘avatars’, etc, protected in your jurisdiction?**

Even though there are no specific regulations regarding the protection of IP rights in the metaverse, considering that the country's IP regulations focus on the protection of intangible assets, we consider that there are arguments to support the view that users of the metaverse should respect the IP rights of inventors, owners and titleholders.<sup>36</sup>

From this perspective, the main rules applicable in this regard in Chile would be the Industrial Property Law and the Copyright Law, as mentioned above in our previous answers.

## **Q 3. How are digital replicas of physical objects protected in your jurisdiction?**

The Copyright Law authorises the copyright owner, or those who have been authorised by the owner, to reproduce the owner's works by any means. The Copyright Law defines ‘reproduction’ as ‘the permanent or temporary fixation of the work in a medium that allows its communication or the obtaining of copies of all or part of it, by any means or process’.<sup>37</sup>

Based on this definition, the reproduction of a copyrighted work without the express authorisation of its owner would constitute an infringement of the Copyright Law.

## **Q 4. How is user-generated content and other derivative works protected in your jurisdiction?**

User-generated content and other derivative works are protected by the Copyright Law and the rights it confers on authors, which defines ‘derivative works’ as ‘a work that results from the adaptation, translation, or other transformation of an original work, provided that it constitutes an autonomous creation’.<sup>38</sup> To be legitimately deemed the author of a derivative work, it is mandatory that the owner of the original work authorises the adaptation, translation or transformation of such original work.<sup>39</sup>

36 Andy Ramos, ‘The metaverse, NFTs and IP rights: to regulate or not to regulate?’ (*WIPO Magazine*, June 2022), [www.wipo.int/wipo\\_magazine/en/2022/02/article\\_0002.html](http://www.wipo.int/wipo_magazine/en/2022/02/article_0002.html) accessed 28 February 2024.

37 Law 17,336 on Intellectual Property of 1970, Art 5, letter u).

38 Law 17,336 on Intellectual Property of 1970, Art 5, letter i).

39 Law 17,336 on Intellectual Property of 1970, Art 9.

## 5. Are there any collective rights management organisations active in your jurisdiction that also manage intellectual property rights in regard to the metaverse?

There are no collective rights management organisations managing IP rights in the metaverse. However, the Copyright Law allows for the existence of collective management organisations concerning copyright and related rights, which in the future could manage IP rights in the metaverse. In this regard, the Sociedad Chilena del Derecho de Autor manages the copyright and related rights of authors, composers, artists, performers and other owners of rights in musical works.

## 6. How are intellectual property rights protected and enforced in the metaverse in your jurisdiction?

We consider that the liability arising from an infringement in the metaverse could be pursued under the civil and criminal actions contemplated in the Industrial Property Law and in the Copyright Law.

The sanction for non-compliance could lead to civil and criminal liability. Please see our previous answer on this topic in the chapter on data.

In the case of an infraction of the Copyright Law, as mentioned, the affected party could claim compensatory or statutory damages, and file criminal actions to pursue fines and penalties of up to 540 days in prison.

In the case of an infraction of the Industrial Property Law, as explained, the affected party could claim compensation for damages and file criminal actions to pursue fines and penalties of up to five years in prison.

## 7. Are there any intellectual property strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote interoperability in the metaverse?

There are no strategies, policies or regulations aimed at promoting interoperability in the metaverse. Therefore, there are no enforceable sanctions, case law or regulatory decisions on this topic.

## 8. Are there any competition strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote standardisation and access to fair and non-discriminatory licences?

There are no strategies, policies or regulations to promote standardisation in the metaverse. Therefore, there are no enforceable sanctions, case law or regulatory decisions on this topic.

## 9. Are there any other intellectual property issues related to the metaverse that have been addressed in your jurisdiction?

No other IP issues related to the metaverse have so far been addressed by the legislator or the relevant public authorities in Chile.



## 10. What are the different roles of metaverse providers?

Please note that there are no specific rules for metaverse providers that establish defined roles for them. However, they can be considered as ISPs.

The legislation related to ISPs in Chile encompasses various laws and regulations covering different aspects, such as the provision of telecommunications services, consumer protection and specific regulations for internet usage. Below are some of the relevant laws and regulations:

- the General Telecommunications Law: this law establishes the general framework for the regulation of telecommunications services in Chile, including internet services; Subtel is the entity responsible for its enforcement;
- the CPL: this law addresses the rights and duties of consumers in general, including those related to telecommunications services, such as transparency concerning the provision of information and service quality; and
- Law 20,453 on net neutrality: this law ensures net neutrality, prohibiting discriminatory practices by ISPs regarding data and service traffic.

In addition, the Copyright Law establishes some rules and limitations in terms of ISP liabilities. Among other dispositions, the Copyright Law contemplates the obligation for ISPs to notify their users in writing of any content that allegedly could be an infringement that they have posted, provided that the following requirements are met:

- they receive notice of the alleged infringement from the owner of the rights or their representative by electronic means or in another written form;
- the owner of the rights or their representative must be domiciled or have a residence in Chile and, where appropriate, have sufficient power to be filed in court on behalf of the owner;
- the allegedly infringed rights are identified, with a precise indication of their ownership and the nature of the infringement;
- the infringing material and its location on the network or system of the service provider to whom the communication is sent is identified, through the URL or its equivalents; and
- contains data that allows the service provider to identify the user responsible for the alleged infringing material.

Once a communication is received with the indicated requirements, ISPs must inform the alleged user of the situation, providing the background information sent by the rightsholder or his/her representative, within a period of five business days from the receipt of the aforementioned communication.



## 11. How does your jurisdiction moderate content and how does it balance this with freedom of expression?

There is no discussion regarding this topic with respect to the metaverse in Chile.



## 12. Are there any by-design notice mechanisms?

No such mechanisms exist so far in the context of the metaverse.

**Q 13. Are there any upcoming policies, strategies or regulations relating to intellectual property in your jurisdiction?**

To the best of our knowledge, there are no relevant upcoming policies, strategies or regulations affecting IP applicable to the metaverse in Chile.



# Digital transaction and ownership



## 1. Are there any relevant policies, strategies or regulations applicable to tokens, non-fungible tokens (NFTs) and digital assets in the metaverse in your jurisdiction?

There are no relevant policies, strategies or regulations on tokens, NFTs and digital assets in the metaverse, nor a regulation on these assets themselves. However, there are rules in Law 21,521 of 2023 (the 'Fintech Law') that indirectly regulate these matters and eventually could be applicable to the metaverse.

The purpose of the Fintech Law is to establish a general framework to encourage the provision of financial services through technological means.

The Fintech Law defines the concept of 'virtual financial assets' or 'crypto-assets' as the 'digital representation of units of value, goods or services, except money, whether in local currency or foreign currency, which can be transferred, stored or exchanged digitally'.<sup>40</sup> Also, the law defines 'financial instrument' as 'any security, contract, document or incorporeal good, designed, used or structured with the purpose of generating monetary income, or representing an outstanding debt or a virtual financial asset'.<sup>41</sup>

In view of the above definitions, there are grounds to argue that a company owning a metaverse could be subject to the rules set forth by the Fintech Law concerning activities such as 'alternative transaction systems' or the 'custody of financial instruments', for example, if the metaverse allows the exchange of virtual financial assets (eg, a virtual currency or a crypto-asset like an NFT), or if the company keeps record of who owns what virtual financial assets in the metaverse.

However, it is important to point out that this interpretation may not be aligned with the scope and regulated subjects that the legislator had in mind when issuing this regulation, which was focused on digital financial services and crypto-asset exchanges. Regulating the issuance, trading and storing of digital assets within a metaverse service exceeds that focus, but, a priori, we cannot rule out this possibility completely because the broad legal definitions above allow us to reach that conclusion, at least from a theoretical point of view.

In addition, relevant regulators have provided definitions or opinions on crypto-assets. In this regard, the following should be noted:

- the Financial Market Commission (Comisión para el Mercado Financiero or CMF) has stated that a cryptocurrency is a representation of a nominal unit, whose main purpose is the exchange of goods and services, issued by a public or private originator and supported in an electronic file (blockchain, distributed ledger technology (DLT) etc);<sup>42</sup>
- the Chilean Internal Revenue Service (IRS) has said that 'bitcoin is a digital or virtual asset, supported in a unique digital record called blockchain, deregulated, disintermediated and not controlled by a central issuer, whose price is determined by supply and demand';<sup>43</sup> and
- for its part, the Central Bank has defined cryptocurrencies or virtual currencies as 'digital representations of value that, among other uses, are intended to serve as a medium of exchange'.<sup>44</sup>

We are not aware of any case law or any decisions by a regulator on this matter. However, there is case law and there are decisions by the regulator relating to digital assets and crypto-assets. Some of these decisions are listed below.

40 Law 21,521 2023, Art 3, No 3. As can be observed, the regulation makes the concept of 'virtual financial asset' equivalent to that of 'crypto-asset', even though they are not, according to the definition given, because not all digital representation of units of value, goods or services are supported by cryptographic technology.

41 Law 21,521 2023, Art 3, No 8.

42 Kevin Cowan Logan, 'Criptomonedas. La visión desde la CMF' CMF [www.cmfchile.cl/portal/prensa/615/articles-24977\\_doc\\_.pdf](http://www.cmfchile.cl/portal/prensa/615/articles-24977_doc_.pdf) accessed 28 February 2024.

43 Ruling No 963, issued on 14 May 2018, by the Chilean Internal Revenue Service [www.sii.cl/normativa\\_legislacion/jurisprudencia\\_administrativa/ley\\_impuesto\\_renta/2018/ja963.htm](http://www.sii.cl/normativa_legislacion/jurisprudencia_administrativa/ley_impuesto_renta/2018/ja963.htm) accessed 28 February 2024.

44 Ruling No 219, issued on 6 February 2018, by the Financial Market Commission [www.bcentral.cl/documents/33528/2818839/rp\\_1228.pdf/9b64613c-380f-2699-8dcd-9cd22bc45e42?t=1615897070780](http://www.bcentral.cl/documents/33528/2818839/rp_1228.pdf/9b64613c-380f-2699-8dcd-9cd22bc45e42?t=1615897070780) accessed 28 February 2024.





In Supreme Court Rol No16.857-2018, dated 3 December 2018, the Supreme Court ruled that a bank may close the accounts of companies engaged in the issuance, creation, brokerage or intermediation of cryptocurrencies, given that these activities lack regulatory recognition, and the characteristics and components of cryptocurrencies make it difficult to comply with the obligations required by the regulations for the prevention of money laundering, the financing of terrorism and drug trafficking. The closure of the bank account by the bank was not considered an arbitrary and illegal act that causes deprivation, disturbance or threat to the legitimate exercise of a constitutional guarantee.

The CMF General Rule No 502, regulates the registration, authorisation and obligations of financial service providers under the Fintech Law of 12 January 2024. In relation to virtual assets, this General Rule sets forth that only crypto-assets that have a public document detailing the technical specifications may be admitted to trading. This document must provide relevant information on the underlying technology and key aspects for acquirers, such as the digital representation of the assets, the associated rights, the holders of such rights and their nature. The minimum specifications will be defined by the relevant alternative system. This public document may be an English or Spanish translation of the original, or one prepared by the alternative system for this purpose.

The CMF, Ordinary Official Letter No 100641 of 9 November 2023 is also pertinent. In response to a consultation on the need to obtain a permit or authorisation to invest the assets of a company in cryptocurrencies, the CMF expressed that, according to national legislation, it is not required to issue any authorisation to make such an investment. The reason for such a statement is based on the fact that, according to the Fintech Law, only those services specifically contemplated in Articles 2 and 3 of such law are subject to regulatory controls. In addition, according to Article 3 of Decree Law 3,538 of 1980, in its current version, the CMF is responsible for the supervision of persons who issue or intermediate publicly offered securities. Therefore, and by virtue of the foregoing, it is not within the commission's competence to supervise investments in cryptocurrencies of private entities.

The CMF Ordinary No 18762 of 23 February 2023 is also important. A consultation on the application of the Fintech Law and whether the activity by exchange services involving virtual currencies and legal currencies through ATMs is framed within this legislation, as well as its interpretation on the scope of the definition of financial assets or crypto-assets. In this sense, the Fintech Law defines crypto-assets as digital representations of units of value, goods or services, excluding legal tender in Chile and foreign currencies. However, the law also amends Article 35 No 8 of the Organic Law of the Central Bank, allowing the Central Bank to regulate payment systems that include digital representations backed by money, whether domestic or foreign currency.

The application of the Fintech Law or the Central Bank regulations will depend on the specific terms and conditions of the service offered. Because the consultation is made in general terms, it is not possible to issue a definitive pronouncement without analysing all the background information related to a company's operations.



## 2. Are there any relevant policies, strategies or regulations applicable to digital transactions in the metaverse in your jurisdiction?

There are no relevant policies, strategies or regulations applicable to digital transactions in the metaverse. Therefore, there are no enforceable sanctions, case law or regulatory decisions on this topic.

However, please see our answer to the previous question on the potential application of the Fintech Law, which includes storing and trading virtual financial assets.



## 3. How is property defined in terms of the metaverse? Are there any relevant policies, strategies or regulations applicable to the ownership of digital assets on the metaverse in your jurisdiction?

There is no specific regulation regarding property in the metaverse. Also, there are no relevant policies, strategies or regulations applicable to the ownership of digital assets in the metaverse.

However, general regulations contained in the Civil Code could apply to the metaverse as well.



The Civil Code defines property as ‘the real right (or right in rem) in a corporeal thing, to enjoy and dispose of it arbitrarily, not being against the law or against another’s right’. It also states that there is a kind of property over incorporeal things (ie, personal rights or credits).

Considering this provision, it could be deemed that, in the metaverse, individuals are entitled to those rights and obligations provided in the terms and conditions of the corresponding platform or under any agreement the parties may be involved with in the metaverse. However, and in the application of the rule stated above, these rights will be limited by law, as well as by the rights of others, that is, the terms and conditions governing the metaverse platform may not contradict, for example, public policy rules.

Ultimately, what can be said about the metaverse leads back to the contractual arrangement that may exist for that particular platform between the parties (ie, platform host and user) and the rules it sets for transferring the rights that each user acquires (eg, how to transfer a virtual asset), with the only limitation being to not contradict public policy.

We are not aware of any case law or regulatory decisions on this topic.



#### 4. How are property transfers regulated in your jurisdiction?

As stated above, property transfers are subject to the general rules in the Civil Code. In the case of property owned in the metaverse, this would be classified within the ownership of a personal right (ie, that granted to the user by the contractual regulation established in the terms and conditions of the platform, as long as it does not contravene Chilean law). Therefore, the transfer of such property would be subject to the rules on the assignment of rights established in the Civil Code.

The Civil Code sets forth the following requirements for this assignment to be valid between the assignor and assignee:

- the right must be transferable, that is, personal rights, the right of usufruct, use and habitation, the right of maintenance and so on, cannot be assigned;
- there must be a title transferring the title of ownership (*título traslativo de dominio*); and
- the assignor must deliver (*entrega*) the title to the assignee.

In addition, the debtor must be notified of the assignment or accept it to be enforceable against him/her and third parties. For these purposes, a notification must be made with the exhibition of the title and the acceptance shall consist of a fact that supposes it, such as a principle of payment to the assignee.



#### 5. How are currencies, including cryptocurrencies, used in the metaverse regulated in your jurisdiction? Who are the main stakeholders and what are the obligations? What sanctions (civil, criminal or administrative) may apply for non-compliance with these obligations?

There is no specific regulation of cryptocurrencies used in the metaverse, so there are no specific stakeholder obligations or penalties for non-compliance.

However, if the Fintech Law is deemed applicable to crypto-assets or other virtual financial assets and the platforms on which they are traded (eg, metaverse), the parties involved in these types of transactions would be subject to the requirements in this law (eg, crypto-asset issuers, platforms for crypto-asset transactions and advisors).

The Fintech Law establishes a regulatory framework for services that are based on Fintech technologies, such as crowdfunding platforms, alternative transaction systems, credit and investment advisory services, custody of financial instruments, order routers and financial instrument intermediaries. The law also creates an open banking system that allows the exchange of client information between different financial or related service providers.

In this sense, the CMF must issue a series of rules that regulate the information requirements that these service providers must comply with, both for their registration and for subsequent stages, collateral and minimum equity requirements, corporate governance and risk management standards, among others.

## 6. How are transactions and the ownership of assets in the metaverse taxed in your jurisdiction? What sanctions (civil, criminal or administrative) may apply for non-compliance with these obligations?

Currently, Chile lacks specific tax regulations regarding the metaverse and its transactions, and therefore general tax principles would be applicable in such instances. Thus, for now, similar or analogous concepts on tax legislation should be explored until more precise legislation is enacted.

It is worth noting that the Chilean IRS has issued certain guidelines on the taxation of digital assets, such as cryptocurrencies<sup>45</sup> and NFTs under the existing legal framework. These guidelines serve as a valuable starting point for understanding the tax implications of such assets in Chile.

In this context, it becomes necessary to clarify the primary issues regarding taxation in the metaverse as follows: the nature of the asset, the nature of the transaction regarding the asset, and the location of the assets and the parties.

In relation to the nature of the asset, what is commonly contained within the metaverse is the asset or the rights attached to a unique NFT, which for instance can be digital art, collectibles or multimedia content, such as music and videos. The Chilean IRS considers cryptocurrencies and NFTs as digital or virtual assets, with all the tax consequences that this implies.<sup>46</sup>

When addressing the question about the nature of the transaction, it is important to note that not every NFT grants the same assets or rights to the purchaser or acquirer. Depending on the circumstances and the agreement between the parties involved, it could be considered either a sale of a digital asset or the granting of a licence with certain rights.<sup>47</sup> The Chilean IRS has ruled that the disposal of a digital asset should be subject to corporate income tax and final taxes, unless the disposal is carried out by an individual, which in that case means that the special rules in Article 17 of the Chilean Income Tax Law (ITL) apply.<sup>48</sup>

Concerning the disposal of a digital asset, in a non-metaverse scenario, if the transaction involves the total transfer of an asset, which is subject to copyright protection, it must be determined whether the income is received by the author (as a natural person) of the digital asset attached to the NFT, or by another seller. In the former case, Article 17 No 8, letter e) of the Chilean Income Tax Law could potentially apply, resulting in a non-taxable event. For any other seller of copyright or even any other digital asset, if the transferor is an individual, letter m) of No 8 of Article 17 of the ITL should be followed, and the individual Chilean tax payer will be taxed under the standard regime that applies to individuals, and if the seller is a company, No 5 of Article 20 of the ITL should be considered, with the transaction subject to corporate income tax.

However, the same aforementioned example in the context of the metaverse would present challenges that would directly affect the tax treatment of the income received. In that case, difficulties may arise regarding the legal formalities required to transfer the author's rights, which may not be met in the metaverse under current Chilean legislation (eg, the requirement for a public deed or private instrument authorised by a notary public). Hence, as the formalities of the transfer would not be met, it is expected that the transfer of copyright would be void. Consequently, it could be deemed that the author is only granting a licence to use the digital asset for tax purposes and as such the previously mentioned rules in Article 17 would not be applicable.

Moreover, there may be challenges regarding VAT and around the disposal of digital assets. If the transaction is solely focused on the disposal of a digital asset, VAT would not be triggered, as the law does not consider as a taxable event the sale of intangible goods.

45 See [www.sii.cl/normativa\\_legislacion/jurisprudencia\\_administrativa/ley\\_impuesto\\_renta/2018/ja963.htm](http://www.sii.cl/normativa_legislacion/jurisprudencia_administrativa/ley_impuesto_renta/2018/ja963.htm) accessed 3 June 2024.

46 Ruling No 3637/ 2022, 979/2022 and 1422/ 2023 by the Chilean Internal Revenue Service.

47 Rebecca Lee and Dorothy Lo, 'What are the sales and use tax implications of the metaverse?' (PWC, 2023) [www.pwc.com/us/en/tech-effect/emerging-tech/metaverse-tax-implications.html](http://www.pwc.com/us/en/tech-effect/emerging-tech/metaverse-tax-implications.html) accessed 28 February 2024.

48 Ruling No 1803/2022 by the Chilean Internal Revenue Service.



Alternatively, if we consider that an NFT attaches rights to the exploitation or temporary assignment of the asset, the situation will resemble the granting of a licence. If the licensor is an individual resident in Chile, it would be subject to the standard tax regime for individuals. If the licensor is an enterprise resident in Chile, it would be subject to corporate income tax. In both cases, VAT could potentially apply pursuant to the special taxable event in Article 8, letter H) of Decree Law No 825 (the 'VAT Law'), which considers the assignment or sublicensing of IP rights, unless the person that benefits from the licence attached to the NFT is a foreign tax resident and the services are considered to be exportable services by the Chilean customs authority.

Additionally, Chile also applies VAT in the case of service providers who are tax residents abroad and provide remote services to be used in the national territory by individuals (referred to as 'Digital Services').<sup>49</sup> This includes the supply or delivery of digital entertainment content, such as videos, music, games or similar items, through downloads, streaming or other technology. In this scenario, the fee that the metaverse host would charge to Chilean individuals would be, in principle, subject to VAT.

Finally, regarding the territoriality or where the transaction takes place, this is one of the most complex points to address, and there is currently no international consensus on it. However, in general, the taxation source could be considered as where the server is located, and the residency of the parties involved should be where the IP address is connected.<sup>50</sup>

From a Chilean perspective, according to the ITL, any person domiciled or resident in Chile is required to pay tax on their income from any source. This implies that the Chilean IRS will not hesitate to impose taxes on gains or profits derived from a Chilean tax resident in the metaverse. Nevertheless, challenges may arise in determining the source of the asset and income, the taxation rights between different jurisdictions involved, and the fact that the IP address could be easily changed to other jurisdictions.

In conclusion, under the current legal framework, the Chilean IRS has tools to tax income derived from transactions in the metaverse, by applying the general principles and rules. However, several aspects require further clarification, including a common understanding between countries regarding the nature of the metaverse, the assets involved, the various transactions that can occur, and the location of the assets and parties, as well as domestic clarification on the taxation of digital assets. Therefore, an international agreement is necessary to address potential future scenarios of double taxation or non-taxation between jurisdictions resulting from differing interpretations on the metaverse.

The omission of a declaration or payment of tax constitutes an offence subject to a fine. Consequently, the Chilean IRS will be able to assess and demand payment for undeclared tax, proceeding thereafter with collection methods. It should be noted that this could also constitute a tax crime, depending on whether or not there is wilful or malicious behaviour involved.



## 7. Are there any upcoming policies, strategies or regulations that will impact digital transactions in your region/country?

Yes. Some of these bills are mentioned below:

Bulletin No 10.133-03,<sup>51</sup> which amends Law 19.496 and Law 19.628, aims to regulate the protection of private life in relation to the sending of publicity. The main objective of this bill is to amend the existing laws in this area. It seeks to establish specific regulations for the sending of advertising, requiring explicit authorisation from consumers to carry out such practices. The intention behind this initiative is to ensure greater control and protection for consumers with regard to the receipt of advertising material, while promoting transparency and respect for the privacy of individuals in the context of direct marketing.

Bulletin No 14.785-24,<sup>52</sup> which regulates the dissemination of content, information and services on digital platforms and social networks, is also noteworthy. The aim of the bill is to safeguard fundamental rights to ensure the full exercise

49 Chilean Law 21,210 of 24 February 2020 established that remote remunerated services provided by non-residents not domiciled in Chile must pay VAT from 1 July 2020. This rule introduced a new special taxable event in letter 'N' of Art 8 of the VAT Law.

50 Kim Young Ran, 'Taxing the Metaverse' (2023) 112 Georgetown Law Journal, Cardozo Legal Studies Research Paper No 724, <https://ssrn.com/abstract=4549974> accessed 28 February 2024.

51 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=10554&prmBOLETIN=10133-03](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=10554&prmBOLETIN=10133-03) accessed 3 June 2024.

52 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15276&prmBOLETIN=14785-24](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15276&prmBOLETIN=14785-24) accessed 3 June 2024.



of the freedom of expression in an environment of plurality and diversity in the context of social networks and the internet. This would be achieved by regulating transparency, compliance with human rights standards, due process and accountability in the dissemination of content, information and services on digital platforms. In sum, this bill: (1) defines digital platforms and social networks; (2) imposes a series of responsibilities on them to operate in Chile; (3) establishes a regulation for digital infrastructure; (4) defines the duties towards their users; and (5) establishes fines between 100 and 1000 UTM for those who violate the law.

Bulletin No 16.206-07,<sup>53</sup> which amends various legal bodies to protect people from information disruption on digital platforms, is also relevant. The bill aims to reduce information disruption caused by the creation, publication, dissemination, promotion or financing of false, harmful or illegal content, as well as hate speech on digital platforms. Regarding the scope of application of the law, all service providers involved with digital platforms that offer services in Chile and have a substantial connection with the country (ie, have an establishment in Chile or a significant number of users) will be bound by the law. Failure to comply with the obligations imposed by the bill will be punishable by a fine of 100 to 1,000 UTM, depending on the nature of the infringement, among other non-pecuniary sanctions.

Bulletin No 16.343-03,<sup>54</sup> which amends Law 19,496 to restrict the number of advertising and promotional communications allowed on a daily basis, is also relevant. The bill restricts the number of advertising and promotional communications allowed once a day, which may only be made from Monday to Friday, between 09.00 and 18.00 hrs. It also enshrines the right to positive silence for the consumer, by virtue of which the intention to suspend the sending of advertising is presumed if within a period of three days from the first contact made by the supplier, the person does not express his/her intention to suspend the sending of advertising.



## 8. Are there any upcoming policies, strategies or regulations that will impact the ownership of assets in the metaverse in your jurisdiction?

Please see our previous answer.

53 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07) accessed 3 June 2024.

54 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=10554&prmBOLETIN=10133-03](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=10554&prmBOLETIN=10133-03) accessed 3 June 2024.



# Digital marketing and consumer protection

## **Q 1. Are there any relevant policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?**

No. For further details, please see our answer on this topic in the chapter on data.

## **Q 2. Are there any relevant policies, strategies or regulations regarding misleading advertising or other unfair commercial practices on the metaverse in your jurisdiction?**

No. There are no relevant policies, strategies or regulations that directly address misleading advertising or other unfair commercial practices in the metaverse. However, general regulations related to misleading advertising could also be applicable to the metaverse.

In this regard, the CPL sets forth principles applicable to advertising activity carried out by suppliers, requiring it to be truthful, objective and not misleading or deceptive to consumers. Accordingly, the consumer's right to truthful and timely information on the goods and services offered, the price, contracting conditions and other relevant characteristics, is fully applicable to advertising activities.

Additionally, a supplier infringes the CPL rules if, through any advertising message, it misleads or deceives consumers with regard to the components of the product and the percentage in which they concur, the suitability of the good or service for the purposes it is intended to satisfy, the relevant characteristics of the good or service, the price or rate, and the method of payment, among others.

Likewise, the CPL also punishes those suppliers who, using any type of advertising message, confuse consumers regarding the identity of competing companies, activities, products, names, trademarks or other distinctive signs.

If a supplier does not comply with its obligation to provide consumers with truthful and timely information, fines up to 300 UTM may be imposed. Additionally, if it does not comply with the specific rules on advertising, it could incur fines of up to 1,500 UTM and, if the advertising affects the quality of products or services that affect the health or safety of the population or the environment, it could incur in fines of up to 2,250 UTM.

SERNAC may file an action for the protection of the general interest of consumers before the respective local police court, requesting the application of the maximum amount of each of the fines for each infringement verified, for the benefit of the public purse.

Additionally, a consumer who believes that they have suffered damage due to the actions of a supplier may initiate individual action before the competent local police court for the imposition of fines, in addition to compensation for the damage suffered.

Although we are not aware of any case law in the context of the metaverse regarding this subject, please note that SERNAC has initiated judicial action against providers in cases of misleading advertising.<sup>55</sup>

55 *SERNAC v Empresas La Polar SA* [2020], 30th Civil Court of Santiago, ROL No 14.882-2022.

### 3. Are there any relevant policies, strategies or regulations aiming to promote consumer protection in the metaverse in your jurisdiction?

There are no relevant policies, strategies or regulations aiming to promote consumer protection in the metaverse. However, as explained above, we deem that general rules regarding consumer protection may apply, in any case, to the extent that a consumer relationship exists.

In this regard, there is currently a consumer protection system made up of mainly the CPL and all the regulations that complement such law.

Additionally, industry best practices are in some way embodied in the interpretative guidelines issued by SERNAC in the exercise of its interpretative powers, which, without being binding for suppliers, make up the guidelines governing the industry.

Finally, it is also relevant to consider, from the point of view of advertising in general, the ethical guidelines established in the Chilean Code of Advertising Ethics by the Self-Regulatory and Advertising Ethics Board (Consejo de Autorregulación y Ética Publicitaria or CONAR), which sets forth the ethical standards applicable to all advertising and marketing communications, in terms of content, form and execution. These standards are binding for all companies associated with CONAR and serve as a guide for those not associated with the board, although their infringement only entails ethical sanctions.

### 4. What is the minimum amount of information that should be provided to consumers? Who are the stakeholders responsible for providing this information?

As mentioned above, consumers have the right to be provided with truthful and timely information on the goods and services offered by providers, the pricing, contracting conditions and other relevant characteristics.

The minimum information that must be provided to consumers can vary according to the type of transaction or product but, in general, it includes aspects such as the following: information on the product or service; information on the total price; information on the supplier or seller; and information on the purchase or contracting process.

The interested party responsible for providing this information is the supplier or seller of the product or service.

If a supplier does not comply with its obligation to provide consumers with truthful and timely information, fines up to 300 UTM may be imposed.

Please note that there are cases in which SERNAC has initiated legal action for breaches of this duty by suppliers.<sup>56</sup>

### 5. Are there any relevant policies, strategies or regulations applicable to platform-to-consumer relationships in your jurisdiction? What are the main obligations of platform providers?

Yes. In addition to the applicable general rules in the CPL, the rules outlined in the Electronic Commerce Regulation of 2021 (Reglamento de Comercio Electrónico<sup>57</sup>) are applicable. The Electronic Commerce Regulation aims to strengthen the transparency and quality of information provided to consumers on e-commerce platforms.

The regulation applies to sellers who offer goods or services on e-commerce platforms in exchange for a price or fee, and to operators of e-commerce platforms where the products or services of third-party sellers are offered.

<sup>56</sup> *SERNAC v Falabella Retail SA* [2020], 3rd Civil Court of Santiago, No 17.348-2020.

<sup>57</sup> See [www.bcn.cl/leychile/navegar?i=1165504](http://www.bcn.cl/leychile/navegar?i=1165504) accessed 3 June 2024.



Regarding the main obligations of e-commerce platform operators, they must provide consumers with the information provided by the seller prior to purchasing the product or contracting the service, that is, information on the seller, information on the role of the e-commerce operator, and information on the essential features of the products or services, among others.

In the event of non-compliance with the provisions in the Electronic Commerce Regulation, fines of up to 300 UTM may be imposed.



## 6. Are there alternative dispute resolution mechanisms available for consumers in your jurisdiction? How are they implemented on the metaverse?

Yes. Under the CPL rules, once a conflict between a consumer and a provider has arisen, the parties may pursue mediation, conciliation or arbitration.

Suppliers must provide information about the nature of each of the mechanisms offered, which will be free of charge and will only be initiated by the express will of the consumer, which must be stated in writing.

The regulation on mediation, conciliation and arbitration in consumer matters (Reglamento de mediación, conciliación y arbitraje en materias de consumo<sup>58</sup>) sets forth the necessary rules for the proper application of these mechanisms.

We are not aware of any cases in which these mechanisms have been implemented in regard to the metaverse. Notwithstanding the above, please note that transactions and disputes arising in virtual environments may be subject to the same laws and regulations as transactions and disputes in the physical world. Therefore, alternative dispute resolution mechanisms for consumer disputes can also be applied in the metaverse if the parties involved freely agree to submit to them and the relevant legal regulations are followed.



## 7. Are there any upcoming policies, strategies or regulations that will impact digital marketing in the metaverse in your jurisdiction?

Yes.

Currently, there are various bills of law being discussed by the Chilean National Congress that, although not directly focused on the metaverse, may affect digital marketing in the physical world, and which, supplementarily, could also be applied to the metaverse.

These bills address different issues, such as the clarity required from suppliers in the information they provide through audio-visual or electronic media (Bulletin No 12225-03<sup>59</sup>), the sending of invasive advertising (Bulletin No 10133-03<sup>60</sup>) and the punishment of the crime of false or misleading advertising to the detriment of the consumer (Bulletin No 16534-07<sup>61</sup>).



## 8. Are there any upcoming policies, strategies or regulations that will impact consumer protection in the metaverse in your jurisdiction?

We are not aware of any upcoming policies, strategies or regulations specifically impacting consumer protection in the metaverse.

58 See [www.bcn.cl/leychile/navegar?i=1185894](http://www.bcn.cl/leychile/navegar?i=1185894) accessed 3 June 2024.

59 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12749&prmBOLETIN=12225-03](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12749&prmBOLETIN=12225-03) accessed 3 June 2024.

60 *Ibid.*

61 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=17102&prmBOLETIN=16534-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=17102&prmBOLETIN=16534-07) accessed 3 June 2024.



However, the Chilean National Congress is currently discussing a bill of law (Bulletin No 16,271-03<sup>62</sup>) that aims to amend the CPL, to improve the protection of the rights of consumers in terms of their individual interests, by strengthening the powers of SERNAC ('SERNAC Bill'). The SERNAC Bill aims to grant sanctioning powers to SERNAC.

Among other important modifications, the SERNAC Bill sets forth more rights for consumers to protect them by:

- establishing a new and better after-sales standard, making it mandatory to receive, register and respond to consumer requests;
- ensuring that consumers can modify or cancel online contracts easily;
- extending the liability of online platforms that act as intermediaries in the sale of goods and services;
- raising the standard of conduct of companies, making them guarantee conditions concerning attention and dignified and equitable treatment of consumers;
- prohibiting the promotion or use of stereotypes that justify or naturalise relations of subordination, inequality or discrimination based on sex, gender or sexual orientation in advertising; and
- eliminating the requirement for a contractual relationship between the affected consumers and the infringing company as a requirement to file class action lawsuits.

Likewise, the SERNAC Bill seeks to modify the current definition of consumer to eliminate the requirement for an 'onerous legal act' to qualify as a consumer.

62 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16826&prmBOLETIN=16271-03](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16826&prmBOLETIN=16271-03) accessed 3 June 2024.



# Liability and insurance

## **Q 1. Are there any relevant policies, strategies or regulations applicable to liability in the metaverse in your jurisdiction?**

There are no relevant policies, strategies or regulations applicable to liability in the metaverse. However, depending on the case, the general rules on liability could be applied.

As regards civil liability, a distinction must be made between contractual liability and non-contractual liability (torts), as well as the liability of the metaverse provider vis-à-vis users or other third parties (business-to-peer or B2P) and liability for actions committed between users within the metaverse (peer-to-peer or P2P), as explained below.

Chilean law provides for the possibility that any party to a contractual relationship (such as the relationship between the company providing access to a metaverse platform and its users, which will probably be governed by the respective terms and conditions) may claim from the other party the effective performance of the contract in case of a breach, or the termination of the contract due to a breach. In the previous cases, the affected party may demand compensation for damage caused by reason of the breach, including consequential damage, lost profits and depending on the interests involved in the contract, even moral damage.

In the case of a non-contractual relationship, the general civil liability system establishes that any person who is affected by damage caused by a third party will be entitled to demand compensation for the damage actually caused from the party whose conduct caused the damage, which includes actual damage, loss of profits and moral damage.

As regard B2P liability, it should be noted that the Copyright Law provides for rules establishing that certain types of internet-related service providers<sup>63</sup> shall be exempt from having to compensate IP rights owners in the case of damage suffered by these owners due to actions committed through the ISP's networks, provided the ISP fulfils certain conditions. These conditions may vary depending on the service provided.

Therefore, if the companies involved in the functioning and operation of a metaverse platform fall within one of the types of ISPs contemplated in the Copyright Law, they could be exempted from civil liability for IP infringements committed via a metaverse platform.

From the criminal law perspective, there are no regulations applicable to the commission of criminal offences in the metaverse and subsequent criminal liability. The current understanding entails the impossibility of applying by equivalence the crimes recognised in the legal system to acts committed in the metaverse. It is therefore expected that national legislation will focus on speeding up the regulation of those criminal offences that occur more frequently in cyberspace or whose commission is facilitated within it, such as money laundering, fraud, biometric hacking, terrorist financing, fraud, child abuse and sexual crimes.<sup>64</sup>

We are not aware of any case law or regulatory decisions related to civil or criminal liability in the context of the metaverse.

## **Q 2. Are there any relevant policies, strategies or regulations applicable to insurance for damage caused in the metaverse in your jurisdiction?**

We are not aware of any specific policies, strategies or regulations governing insurance in Chile for damage caused in the metaverse, nor any insurance policy with coverage of the metaverse commercialised in Chile.

63 The Copyright Law distinguishes between companies engaged in: (1) data transmission, routing or connection supply service providers; (2) temporary automatic data storage; and (3) service providers that, on the user's request, store data in their networks or systems, either by themselves or third parties, or provide services that include search, linkage or reference to websites by means of search engines, including hyperlinks and directories.

64 Daniela Dupuy, 'Crímenes y Metaverso' in Juan Corvalán (dir.), *Metaverso, web3 y gaming* (Thomson Reuters, 2023).

However, please be aware that if acts committed in the metaverse cause damage to third parties that could be subject to general liability, in that scenario such liability could be covered by general liability insurance. Also, it is likely that certain digital assets will need to be protected against cyber threats in the digital world, such as hacking or identity theft, which could be covered by cybersecurity insurance.

An additional issue to be resolved is whether risks occurring in the metaverse should be covered by insurance companies incorporated in the metaverse itself or in the real world. There is no clarity on this to date. Consequently, as the metaverse is in constant development, we do not discard that in the near future tailor-made insurance policies related to the metaverse will be issued in Chile. If so, it is likely that certain policies, strategies and regulations will be issued to deal with this matter.

---

### **3. What are the metaverse-applicable civil liability/tort liability rules in your jurisdiction? Who are the responsible stakeholders in the case of damages?**

There are no liability rules specifically applicable to the metaverse. Consequently, there are no responsible stakeholders in the case of damages or specific sanctions applicable in the context of the metaverse. However, depending on the case, the general liability rules could be applied. For further details on the liability rules, please see our previous answer.

In addition, applying the general liability rules, the person whose act caused the damage must be liable for it. It is unclear whether the provider of the metaverse would eventually be liable for acts committed by third parties within the metaverse (eg, for an omission to take all the necessary measures to prevent such damage). This will have to be analysed on a case-by-case basis.

We are not aware of any case law or any decisions by a regulator on this matter.

---

### **4. How are liability rules enforced in the metaverse in your jurisdiction? Who is the responsible stakeholder in the case of damages?**

As explained, there are no liability rules specifically applicable to the metaverse nor any responsible stakeholders in the case of damages or specific sanctions applicable in the context of the metaverse.

If the general liability rules could be applied in the metaverse, a breach of contract or non-contractual liability of the non-performing party or the tortfeasor shall be enforced in a civil court.

Regarding criminal liability, there are no rules that establish what crimes can be committed in the metaverse. However, there are some crimes that, in principle, could be committed in the metaverse. For instance, the Cybercrime Law provides a range of conduct for which both individuals and legal entities could be held liable; the Copyright Act could also be extended to the metaverse to punish the improper use of works created or used in the metaverse; and certain crimes enshrined in the Criminal Code could be committed in the metaverse, such as electronic fraud, blackmail and extortion.

We are not aware of any case law or regulatory decisions on this matter.

---

### **5. What are the roles of intermediaries and gatekeepers when it comes to the enforcement of rights and liability on the metaverse?**

There are no specific rules for intermediaries and gatekeepers in the metaverse establishing defined roles for them. However, the mentioned rules on liability and enforcement could be applied, including the exceptions regarding ISPs.

In this regard, if the intermediary or gatekeeper commits an act that causes damage to third parties, it could be subject to general liability and its liability may be pursued before a civil court. It is unclear whether the intermediary or gatekeeper



can exempt itself from liability based on the actions or omissions of other responsible parties in the metaverse, as well as whether it would eventually be liable for acts committed by third parties within the metaverse.

## **Q 6. What are the relevant insurance topics regarding the metaverse in your jurisdiction?**

The concept of the metaverse and its impact on the legal and insurance industry in Chile is an emerging topic. Nowadays, the challenge faced by the Chilean insurance market would entail the incorporation of new technologies, aiming to digitalise insurance services (eg, providing quotations, underwriting and claims management processes through digital channels).<sup>65</sup> In this regard, the digitalisation of the insurance business might also comprise new technology trends, such as the metaverse. Regardless, as stated above, there are still no relevant insurance topics regarding the metaverse in Chile.

## **Q 7. Are there any relevant policies, strategies or regulations applicable to criminal liability on the metaverse in your jurisdiction?**

There are no relevant policies or regulations specifically applicable to criminal liability in the metaverse.

However, certain crimes in principle, could be committed in the metaverse, such as cybercrimes, IP crimes and electronic fraud. As mentioned, there is no general rule stating which crimes can be committed in the metaverse.

## **Q 8. Are there any upcoming policies, strategies or regulations impacting liability (civil/tort/criminal) on the metaverse in your jurisdiction?**

The mentioned bill introduced in September 2021 on the regulation of digital platforms (Bulletin No 14561-19<sup>66</sup>), establishes that the digital platform provider shall be objectively liable for all damage, whether pecuniary or non-pecuniary, caused to users. The judge may order the provider to pay up to double such damages when he/she derives from the breach of the rights established in the law, in addition to ordering the temporary blocking of the platform, when such breaches are of a systematic nature. In addition, the bill introduced in August 2023, that modifies several legal bodies to protect people from information disruption on digital platforms (Bulletin No 16206-07<sup>67</sup>) could impact liability by establishing new obligations that the provider must comply with and related sanctions.

To the best of our knowledge, there are no other relevant upcoming policies, strategies or regulation impacting liability in the metaverse. However, there is an interest in regulating various aspects of virtual reality and the metaverse. For instance, in March 2023, the seminar on 'Opportunities and Challenges of the Metaverse' was held at the National Congress, organised by the Senate, and other entities, in which the need for legislation to regulate the benefits and threats that may arise from the use of the metaverse was discussed.

65 Diario Financiero, 'Corredores de Seguros y Transformación Digital de la Industria' (2023), 20. See [www.df.cl/noticias/site/docs/20230620/20230620170940/suplemeto\\_20230622.pdf](http://www.df.cl/noticias/site/docs/20230620/20230620170940/suplemeto_20230622.pdf) accessed 14 February 2024.

66 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15047&prmBOLETIN=14561-19](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15047&prmBOLETIN=14561-19) accessed 3 June 2024.

67 See [www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07](http://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16757&prmBOLETIN=16206-07) accessed 3 June 2024.

## 9. Are there any upcoming policies, strategies or regulations related to insurance on the metaverse in your jurisdiction?

We are not aware of upcoming insurance policies, strategies or regulations that will specifically address the metaverse. Nevertheless, the Chilean insurance regulator, the CMF, has published certain guidelines on the use of digital technologies in the insurance market (Insurtech).<sup>68</sup> Among others, these guidelines point out the increased vulnerability of insurers to cyber-attacks, the use of AI and more complex products. In this regard, Insurtech might also include guidelines regarding the insurance market in the context of the metaverse in the future.

68 Patricio Espinoza, Marco Jaque, Paulo Bobadilla and Raúl Salazar, 'Desarrollo, regulación y supervisión de tecnologías digitales en la industria de seguros' (CMF, 2020) [www.cmfchile.cl/portal/estadisticas/617/articles-38712\\_doc\\_pdf.pdf](http://www.cmfchile.cl/portal/estadisticas/617/articles-38712_doc_pdf.pdf) accessed 15 February 2024.



# Jurisdiction and governance

## **Q 1. Are there any upcoming policies, strategies or regulations setting out rules on how to identify the governing law on the metaverse?**

There are no upcoming policies, strategies or regulations being developed in Chile related to the determination of the governing law in regard to metaverse platforms. However, the general rules on this matter could be applicable.

In the case of contractual relationships (eg, the relationship between the metaverse provider and the user), the governing law shall be the law of the contract (except for certain matters where Chilean law is mandatory). Please note that contract law is governed by freedom of contract and the prevailing interpretation is that choice of law clauses are valid and enforceable under Chilean law (except in the case of purely domestic contracts).

However, if the metaverse user is considered a consumer under the CPL, the choice of law clause could be considered abusive, as consumers have the non-waivable right to exercise their rights and bring actions before the competent courts for the protection of their interests.

In the case of other relationships not primarily based on a contract, considering the principle of territoriality established in the Chilean Civil Code, it is reasonable to understand that Chilean law will apply. In this sense, the Chilean Civil Code establishes that Chilean law is mandatory for all inhabitants of the Republic of Chile, including foreigners.

## **Q 2. Are there any upcoming policies, strategies or regulations setting out rules on how to identify the jurisdiction on the metaverse? Is there any case law or are there any decisions by a regulator regarding determining jurisdiction in the metaverse in your jurisdiction?**

There are no upcoming policies, strategies or regulations in development on how to identify the applicable jurisdiction in regard to the metaverse. Therefore, there is no case law or decisions by a regulator on this topic.

## **Q 3. What are the regulators and government bodies tasked with ensuring compliance with the applicable laws on the metaverse in your jurisdiction?**

There is currently no regulatory authority or public body whose functions refer specifically to the metaverse because this technology category is not specifically recognised or regulated as such in our legislation.

Although there is no public authority or entity specifically designated to oversee compliance with laws that may be applicable to the metaverse, it may be that a sectoral authority carries out oversight on activities taking place on a metaverse platform. For instance, as regards consumer relationships within the metaverse, SERNAC could pursue compliance with the CPL if it considers that the company providing access to such a platform, or a company that offers its products or services through it, has not adequately complied with the provisions in the CPL.

## **Q 4. Are there any dispute resolution mechanisms available in your jurisdiction?**

There are several dispute resolution mechanisms that are recognised in Chilean legislation as alternatives to the judicial process for the resolution of conflicts. Among these mechanisms, the most noteworthy to mention are the following: (1)

conciliation, which is even established as an essential stage in most legal proceedings for several matters; (2) mediation, which is a common mechanism in family and labour matters; (3) and, above all, arbitration, which has a special law on international commercial arbitration.

Particularly, with respect to mediation and arbitration, the Santiago Chamber of Commerce has an Arbitration and Mediation Centre (Centro de Arbitraje y Mediación or CAM), with rules specifically prepared for international and domestic arbitration, and for both arbitration of law and *ex aequo et bono*. CAM is also in charge of appointing and overseeing arbitrators. It is common for contracts between private parties in Chile whose dispute resolution mechanism is arbitration to submit to the appointment of an arbitrator by the CAM, under the rules of the said institution.

The implementation of these dispute resolution mechanisms is generally not mandatory, so their use will depend on the consent of the involved parties.

Regardless of the general rule already mentioned, it should be noted that in Chile, there are certain matters that cannot be submitted to arbitration in any case and must always be heard by ordinary courts of justice. This is the case, for example, with disputes over alimony, criminal cases and conflicts between a legal representative and their principal, among other matters. Moreover, as explained above in regard to consumer matters, consumers are not obliged to accept or submit to arbitration, as they can always exercise their rights and bring actions before the competent courts for the protection of their interests.

On the other hand, there are also some matters where recourse to arbitration is mandatory, without it being possible to resolve the dispute through ordinary courts. This is the case with disputes between partners in certain types of legal entities, as well as the division of assets of an inheritance.



## 5. How is arbitration implemented on the metaverse in your jurisdiction?

Currently, there are no cases in Chile related to the metaverse that have been decided either through the courts or through dispute resolution mechanisms, so there is no previous experience to determine how arbitration is currently implemented in relation to metaverse platforms.



## 6. Are there any upcoming policies, strategies or regulations regarding determining the governing law and jurisdiction on the metaverse in your jurisdiction?

As explained, there are no upcoming policies, strategies or regulations to determine the governing law or the jurisdiction in regard to the metaverse. In addition, there is no case law or any decisions by a regulator on this topic.

However, at the level of soft law, it is not impossible that stakeholders may establish standards or good practice guidelines in this area that could be applied in Chile.