the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

PERU

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

Data

Maritza Reátegui *Rodrigo, Elías & Medrano, Lima*
Francisco Baldeón *Rodrigo, Elías & Medrano, Lima*
José Govea *Rodrigo, Elías & Medrano, Lima*

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

Even though specific metaverse legislation has not been enacted in Peru, the country's data protection laws will be applicable to any metaverse ecosystem that falls within its scope of application.

Data protection in Peru is mainly regulated by the Peruvian Personal Data Protection Law, Law No 29,733 (Data Protection Law); its regulations, enacted by Supreme Decree No 003-2013-JUS (Regulations); and the Security Directive passed by the Peruvian Data Protection Authority, enacted by Resolution No 019-2013-JUS/DGPDP (Directive).

Peru's data protection laws are applicable when: (1) the processing of personal data is performed in an establishment located in Peru belonging to the data controller; (2) the processing of personal data is performed by a data processor on behalf of a data controller established in Peru; or (3) if the data controller established outside Peruvian territory makes use of means located in Peru for the processing of personal data, unless the only processing involved involves the transit of data through Peru.

Although the Artificial Intelligence Law, Law No 31814, was enacted in 2023, this law does not establish any specific provisions applicable to the metaverse. The relevant regulations have yet to be enacted.

Urgency Decree No 006-2020, which creates the national digital transformation system, and Urgency Decree No 007-2020, which approves the digital trust framework, are also applicable to new technologies, but do not establish any specific provisions applicable to the metaverse.

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

There are no specific regulations regarding the protection of personal and non-personal data associated with the metaverse.

Nonetheless, Peruvian data protection laws protect personal data, which is defined as any information about an individual that identifies or makes the said individual identifiable. It includes all numerical, alphabetical, graphic, photographic, sound or any other type of information concerning an individual, which identifies or could be used to identify the individual through reasonable means.

Peruvian legislation recognises sensitive data as personal data. The Data Protection Law defines sensitive data as personal data consisting of biometric data that by itself can identify the data subject; data referred to as related to a person's racial and ethnic background; income; political, religious, philosophical, or moral opinions or creed; union membership; and data related to health or sexual orientation. Similarly, the regulations related to the Peruvian Data Protection Law define sensitive data as data relating to physical, mental and emotional characteristics, facts or circumstances of emotional or family life, personal habits corresponding to the most intimate sphere of a person's private life, data related to physical or mental health, among others that affect the intimacy of the data subject. The processing of sensitive data requires the written consent of the data subject.

The data protection standards applicable to personal data are described below.

Q 3. Who are the different stakeholders involved in the data value chains in the metaverse 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?

Peruvian legislation does not regulate stakeholders involved in the data value chains in the metaverse. The general obligations imposed on data controllers and data processors under the data protection laws in Peru are applicable to persons who are involved in such activities in the context of the metaverse ecosystem.

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

The main principles established in the country's Data Protection Law, which are applicable to the metaverse, are as follows:

- the principle of legality – data processing must be performed in accordance with the Data Protection Law. Data collection carried out by fraudulent, dishonest or illegal means is forbidden; and
- the principle of consent – data processing requires the data subject's consent. The regulations provide that the processing, including the transfer itself, of personal data require the prior, free, informed and explicit and unequivocal consent of the data subject:
  - free – consent must be free from error, bad faith, violence or wilful misconduct that may affect the will of the data subject;
  - prior – consent must be given prior to the collection of personal data or, as the case may be, prior to the processing for a purpose different than the one for which the data was originally collected;
  - explicit and unequivocal – consent must be expressed in conditions that do not allow doubts about its granting. Clicking a digital button will be considered as a form of specific and unequivocal consent; and
- informed – the data subject has the right to be informed in detail, simply, specifically, unequivocally and prior to collection, about the purpose for which their personal data will be processed; who will be or who may be the recipients, the existence of the database in which the data will be stored, as well as the identity and address of the data controller and, if applicable, the data processor of their personal data; the mandatory or optional character of the answers to the questionnaire presented to them, especially concerning sensitive data; the transfer of their personal data; the consequences of providing their personal data and of their refusal to do so; the time during which their personal data will be kept; and how to exercise the right of access, rectification, cancellation and opposition (ARCO) granted to them by law. If the personal data is collected online through electronic communication networks, the duty to provide certain information may be satisfied through the publishing of privacy policies, which must be easily accessible and identifiable.

Even if consent is not required (eg, when the data is necessary for the development, entering and compliance with a contractual relationship related to the data subject, or when the data is in the public domain), the duty relating to the provision of information must still be satisfied. Note that the consent of the data subject is not necessary, among other scenarios, when the data is necessary for the development, entering into and compliance with a contractual relationship concerning the data subject:

- the principle of purpose – personal data must be collected for a determined, explicit and legal purpose. Data processing must not be extended to any purpose other than the one unequivocally established at the time of collection, excluding cases involving activities of historical, statistical or scientific value, where a dissociation or anonymisation procedure is applied;

- the principle of proportionality – data processing must be adequate, relevant and not excessive in regard to the purpose for which it was collected;

- the principle of quality – personal data to be processed must be truthful, accurate and, if it is possible, updated, necessary, relevant and adequate regarding the purpose for which it was collected. It must be preserved in a way that ensures its security and only for the time necessary to fulfil the purpose of the processing;
- the principle of security – data controllers and those responsible for processing must adopt the technical, organisational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved. Security standards are described in the relevant regulations and in the directive; and
- the principle of adequate protection levels – for cross-border transfers, a sufficient level of protection must be ensured for the personal data to be processed, or at least, comparable to the Data Protection Law's provisions or to the applicable international standards.

The infractions that are detailed in the Peruvian data protection laws are the following:

Minor infractions:

- processing personal data in breach of the security measures established in the Data Protection Law and its regulations;
- collecting personal data that is unnecessary, inappropriate or inadequate in connection to the specific, explicit and lawful purposes for which it was obtained;
- not modifying or rectifying the personal data when it is known to be inaccurate or incomplete;
- not deleting personal data when it is no longer necessary, relevant or adequate for the purpose for which it was collected or when the time for its processing has expired, except for cases where a dissociation or anonymisation procedure has been applied;
- not registering databases or updating them with the Peruvian Data Protection Registry; and
- processing data in contravention of the provisions of the Data Protection Law and its regulations.

Serious infractions:

- not attending, impeding or hindering the exercise of the data subject's rights in accordance with the provisions of the Data Protection Law;
- processing personal data without the free, explicit, unequivocal, prior and informed consent of the data subject, when such consent is required in accordance with the Data Protection Law and its regulations;
- processing sensitive data in breach of the security measures established in the Data Protection Law and its regulations;
- collecting sensitive data that is unnecessary, inappropriate or inadequate in connection to the specific, explicit and lawful purposes for which it was obtained;
- processing personal data lawfully obtained for purposes other than those for which it was collected, except for cases where a dissociation or anonymisation procedure has been applied;
- obstructing the exercise of the supervisory function of the Peruvian Data Protection Authority (DPA);
- not complying with the confidentiality obligations set out in the Data Protection Law; and
- not registering databases or updating them with the Peruvian Data Protection Registry, despite having been requested to do so by the DPA, within the framework of a sanctioning procedure.

The most serious infractions:

- processing personal data in contravention of the obligations contained in the Data Protection Law and its regulations when this impedes the exercise of other fundamental rights or violates them;
- collecting personal data by fraudulent, unfair or unlawful means;
- providing false documents or information to the DPA;
- not ceasing the improper processing of personal data when there has been a prior requirement from the DPA because of a sanctioning or trilateral procedure; and
- not complying with the corrective measures established by the DPA because of a trilateral procedure.

The Peruvian Data Protection Authority (DPA) may impose the following fines, which are measured in tax units (otherwise known by the Spanish acronym UIT):

- minor infractions are sanctioned with a fine between 0.5 UIT and 5 UIT (approximately between US$700 and US$7,000);
- serious infractions are sanctioned with a fine between 5 UIT and 50 UIT (approximately between US$7,000 and US$70,000);
- very serious infractions are sanctioned with a fine between 50 UIT and 100 UIT (approximately between US$70,000 and US$140,000); and
- in no case may the fine exceed the equivalent of ten per cent of the annual gross income that the entity has earned in the previous fiscal year.

In theory, the data subject may also file a claim arguing damages or distress caused by the breach of their data protection rights under the Data Protection Law. However, we are not aware of any data protection breaches that have turned into a damages claim.

We are not aware of any case law or any decisions by a regulator regarding infringements of data protection principles in relation to the metaverse.

Q 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?

In Peru, there are currently no specific regulations governing the sharing or licensing of non-personal data. Moreover, the concept of non-personal data ownership is not formally recognised as a distinct entity. Nevertheless, there exists the potential for protection under the umbrella of trade secrets, offering a route to safeguarding non-personal data within the framework of proprietary business information.

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

In Peru, the Unfair Competition Law (Legislative Decree No 1044) serves as the comprehensive regulatory framework overseeing all forms of advertising and promotion for products and services within the Peruvian market. This coverage extends to digital marketing activities within the metaverse.

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

The processing of the personal data of minors (under the age of 18, in accordance with Peruvian law) requires the consent of their legal guardians, in accordance with the regulations. It is necessary to verify the consent provided by legal guardians.

However, the processing of the personal data of minors between the ages of 14 and 18 can be performed with their consent, if the information provided to them for obtaining such consent has been conveyed in language which is easily comprehensible for them, except in cases in which the law requires the assistance of their legal guardians.

The law requires such assistance according to the following: under Article 456 of the Peruvian Civil Code (Legislative Decree No 295) a minor above 16 can assume obligations or waive rights with their guardians' explicit or tacit consent, or with their ratification. If the minor is below 16 years old, the minor cannot enter into contracts by themselves without the participation of their legal guardian. Therefore, if minor assume obligations or waive rights, consent or ratification by their legal guardian is needed for minors above 16 years old, and participation by their legal guardian is needed for minors that are 16 years old and below. In our opinion, in these cases (the assumption of obligations or the waiving of rights), a data controller cannot collect minors' data for the purpose of the assumption of obligations or the waiving of rights.

In no cases can consent be given for the processing of minor's personal data in order for them to access goods or services that are strictly for adults (in Peru, individuals over the age of 18) (eg, alcohol, cigarettes).

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 following are the main rules that apply to cross-border transfers:

- the exporter must have obtained data subject's consent to perform the cross-border transfer of their personal data or rely on an exemption to such consent (eg, when the data transfer is necessary for the development, entering into or compliance with a contractual relationship involving data subject);
- the data subject must be informed of the cross-border transfer, the purposes of the transfer of their data and the type of activity that will be carried out by the recipient. Data subjects must be informed of the recipient's identity and, if such recipient is a data processor (eg, cloud storage providers), of its address;
- cross-border transfers will be possible when the recipient assumes all the obligations that correspond to the data exporter as the data controller. For purposes of assuming all the obligations that correspond to the data exporter as the data controller, the exporter may use contractual clauses or other legal instruments to establish such obligations, as well as the conditions under which data subject consented to the processing of their data;
- exporters of personal data must refrain from making cross-border transfers of personal data if the destination country does not provide adequate levels of protection. If the destination country fails to provide an adequate level of protection, the data exporter must guarantee that the treatment of the personal data meets adequate protection levels (eg, through contractual clauses and/or codes of conduct for specific business groups). This does not apply when, among other cases: (1) data subject has given their prior, informed, express and unequivocal consent to the transfer of data under such circumstances or (2) the cross-border transfer of personal data is needed for the performance of a contractual relationship in which the data subject is a party and the activities that the management of the contractual relationship requires. Note that no specific list of countries ('whitelist') with adequate protection levels has been published by the DPA; and

- data controllers must report the transfer of personal data abroad to the DPA. The DPA has established that providing data to a data processor located abroad will be understood as a cross-border data transfer. However, in these cases, the data subject's consent will not be required.

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?

In accordance with the Data Protection Law, data subject has the right not to be subject to a decision which legally or significantly affects them, based solely on the processing of personal data aimed at evaluating certain aspects of their personality or conduct, unless this occurs in the context of the negotiation, conclusion or execution of a contract, among others.

We are not aware of any case law or any decisions by a regulator regarding infringements of the rules applicable to automated decision-making.

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

Data subjects have rights of access, rectification, cancellation and opposition, which can be exercised in regard to the respective data controller. If the data controller rejects the data subject's request, the latter may start an administrative proceeding before the DPA against the data controller.

Data subjects may also bring a complaint before the DPA against a data controller or data processor. In this case, the DPA will conduct an investigative procedure and assess whether any breach of the rules has been committed.

The DPA is very active and has been involved in a high level of enforcement activity.

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

The regulations related to the Data Protection Law are to be amended shortly. On 26 August 2023, the draft of the new regulations was published according to Ministerial Resolution No 270-2023-JUS for public comments. The regulations related to the Artificial Intelligence Law, Law No 31814, will also be published shortly.

Cybersecurity

Maritza Reátegui *Rodrigo, Elías & Medrano, Lima*
Francisco Baldeón *Rodrigo, Elías & Medrano, Lima*
José Govea *Rodrigo, Elías & Medrano, Lima*

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

Even though specific metaverse legislation has not been enacted in Peru, cybersecurity measures set out in Peru's data protection laws are applicable to any metaverse ecosystem that falls within its scope of application.

In particular, cybersecurity measures are detailed in the regulations related to the Data Protection Law and in the Security Directive passed by the Peruvian Data Protection Authority, enacted by Resolution No 019-2013-JUS/DGPDP.

Although the Artificial Intelligence Law, Law No 31814, was enacted in 2023, it does not establish any specific cybersecurity measures applicable to the metaverse. The regulations related to the law have yet to be enacted.

Q 2. What are the security-by-design (physical and digital interfaces) principles applicable to the metaverse in your jurisdiction?

The Security Directive recognises the 'security-by-design' approach, which can be used referentially by entities when evaluating processes and tools that must be implemented to comply with the data protection regulations.

Neither the Data Protection Law nor its regulations specifically regulate this matter.

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

We are not aware of any cyber incidents that have occurred in the metaverse in Peru. Nevertheless, the abovementioned Security Directive regulates data breach notifications, in accordance with the following details:

- communication with the data protection authority – not required under Peruvian law;
- communication to the data subject – the data controller must inform the data subjects of any incident that significantly affects their property or moral rights. The minimum information requirements in the notice are: (1) a description of the incident; (2) the disclosed personal data; (3) recommendations to the data subject; and (4) the implemented corrective measures;
- when to notify? – data breaches must be notified to the data subject as soon as the occurrence of the incident is confirmed;
- when does a controller become 'aware'? – even though Peruvian law does not describe when, exactly, data controller become 'aware' of a particular breach, we consider that such an issue will depend on the circumstances of the specific breach, which means that data controller will become 'aware' when they have a reasonable degree of certainty that a security incident has occurred; and
- documenting breaches – the data controller must keep documentation on all breaches, including:

1. the date and time of the incident;
2. the name of the person that reports the incident;
3. a detailed description of the incident;
4. the disclosed personal data;
5. the name of the persons involved in solving the incident;
6. the consequences of the incident;
7. the implemented corrective measures;
8. the recommendations given to the data subjects;
9. details on whether the data has been recovered; and
10. in case of data recovery, the name of the person that recovered the data, a description and the date of the recovered data, and a description of the manually recovered data, etc.

The applicable sanctions have been described in the chapter on data. The Peruvian DPA is extremely active in auditing and enforcing compliance with the Security Directive.

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

In accordance with the Data Protection Law, for the purposes of the processing of personal data, the data controller must adopt technical, organisational and legal measures to guarantee the security of the data and prevent its alteration, loss, processing or unauthorised access.

In this regard, the regulations detail the following cybersecurity measures.

Access control

Computer systems that manage quantities of personal data must include in their operation the control of access to such personal data information, including the management of access from the registration of a user, the management of the privileges of such users, the identification of the user by the system, among which are rules on the creation of a username/password, the use of digital certificates and tokens, among others, and carry out the periodic verification of the assigned privileges, which must be defined through a documented procedure in order to guarantee their suitability.

Computer systems that manage quantities of personal data must include in their operation the generation and maintenance of records that provide evidence of the interactions with logical data, including for the purposes of traceability, information on user accounts with access to the system, login and logout times, and relevant actions. These records must be legible, timely and include a disposition procedure, including the destination of the records, once they are no longer useful, and rules for their destruction, transfer and storage, among others.

Similarly, security measures related to authorised access to data must be established through identification and authentication procedures, which guarantee the security of the processing of personal data.

Security controls

The specific environments in which information is processed, stored or transmitted must be implemented with appropriate security controls, taking as a reference, the physical and environmental security recommendations set out in the current edition of the *ISO/IEC 17799 EDI Information Technology: Code of Good Practices for Information Security Management.*

In addition, mechanisms for backing up the information in the database of personal data must be considered, with a procedure that contemplates the verification of the integrity of the data stored in the backup, including, when

appropriate, complete recovery in the event of an interruption or damage, guaranteeing a return to the state in which it was in at the time the interruption or damage occurred.

Transfer

The exchange of personal data from processing or storage environments to any destination outside the physical facilities of the entity will only proceed with the authorisation of the data controller and will be undertaken using the means of transport authorised by the same, taking the necessary measures, including data encryption, the use of digital signatures, and verification checks, among others, aimed at preventing unauthorised access, loss or corruption during transit to their destination.

Copies

The generation of copies or the reproduction of documents may only be carried out subject to the control of authorised personnel.

The necessary cybersecurity measures are further described in the Security Directive, which establishes different standards depending on the features of the database involved. The relevant criteria are: (1) the number of data subjects whose data is contained in the database; (2) the number of fields in the database (eg, name, address and telephone number); (3) the existence of sensitive data; and (4) the data controller of the database (an individual or entity).

Q 5. Are there any upcoming policies, strategies or regulations that will impact cybersecurity on the metaverse?

The regulations related to the Data Protection Law are soon to be amended. On 26 August 2023, the draft of the new regulations was published according to Ministerial Resolution No 270-2023-JUS for public comments. The regulations related to the Artificial Intelligence Law, Law No 31814, are also to be published shortly.

Competition law

Verónica Sattler *Rodrigo, Elías & Medrano, Lima*
Francisco José Floríndez *Rodrigo, Elías & Medrano, Lima*

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

Neither the metaverse nor digital platforms have been specifically targeted by Peruvian regulators, which includes the Peruvian Competition Authority.

Until recently, the Peruvian Competition Authority has focused most of its digital market-related efforts, issuing several market studies aimed at promoting competition.

The latter has included market studies on FinTech (financial technologies) and payment systems, which motivated a response by the Peruvian Central Bank that involved the implementation of specific regulations for payment card networks to incorporate, among others, recommendations on antirust-related matters.

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

In absence of specific regulations, antitrust infringements for illegal conduct in the metaverse are subject to the Peruvian Competition Law's general provisions.

As may be the case in other jurisdictions, the following exclusionary conduct is sanctioned under Peruvian Competition Law: (1) abuse of dominant position events; (2) vertical collusion; and (3) horizontal collusion. In Peru, exploitative conduct is not considered an infringement of competition law (eg, excessive pricing).

Abuse of dominant position events, vertical collusion and most types of horizontal collusion are subject to the 'rule of reason', while certain types of horizontal collusion (cartels) are sanctioned as 'absolute prohibitions' and, as of 2020, may be subject to criminal prosecution.

Parties affected by antitrust infringements, or the Competition Authority on their behalf, when damages involve common or undefined interests, may file civil damages claims against offenders. In this regard, the Peruvian Competition Authority issued a guideline that limits its ability to file claims only to those cases that involve damages to end consumers, thereby excluding its involvement in civil disputes between corporations.

The latter makes it unlikely that the Peruvian Competition Authority will pursue civil damages claims for possible antitrust infringements in the metaverse, as the initial cases are likely to involve disputes between corporations, rather than collective and/or undefined damages to end consumers.

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

The metaverse is subject to the Peruvian Competition Law's general provisions on market dominance and barriers to entry. This law does not include a specific threshold on market dominance, but informally a market share of 35 per cent or more may be indicative of market dominance.

Under Peruvian Competition Law, market dominance is assessed on a case-by-case basis considering the current market share, the characteristics of the offered and demanded goods and services, competitor access to financing and

distribution, among others. Specifically legal, economic and/or strategic barriers to entry will be considered to assess market dominance.

The assessment of market dominance is particularly important to evaluate where a market agent may be involved in the abuse of a dominant position or vertical collusion, as market dominance is a requirement for both infringements. In this regard, the Peruvian Competition Authority has largely focused on the prosecution of horizontal collusion subject to absolute prohibitions (cartels), although recently some relevant cases have involved abuse of dominant position events.

Although the Peruvian Competition Authority has yet to initiate a formal investigation connected to the metaverse, the authority has been studying specific digital platforms, the impact of FinTech on the market and is involved in an ongoing investigation into the alleged abuse of a dominant position in the digital payment sector.

Q 4. Are there any specific obligations on gatekeepers applicable to the metaverse in your jurisdiction?

There are no obligations specific to gatekeepers in Peru. In the absence of such regulations, general provisions are applicable under Peruvian Competition Law.

Considering the above, most cases connected to the metaverse may evolve as instances of access refusal and/or discriminatory treatment that may be considered to be possible abuse of a dominant position events. Antitrust claims for the abuse of a dominant position are subject to administrative fines and the affected party may also initiate civil damages claim before the judiciary.

However, these cases will only be successful if the alleged offender: (1) holds a dominant position in the market; (2) indirectly and/or directly competes with the affected party (competition relationship); and (3) the conduct negatively affects the market.

Considering the complexities connected to claims related to the abuse of a dominant position, the relevant supervisory authorities should carefully assess whether specific gatekeeper regulations and/or general regulations for digital platforms are required to guarantee the adequate development of digital markets.

Q 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 competition strategies, policies or regulations that aim to promote standardisation and access to fair and non-discriminatory licences. Possible claims are likely to be deemed to be 'abuse of a dominant position' events, subject to the fulfilment of the applicable requirements.

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

There are no specific strategies, policies and/or regulations aiming to promote interoperability in the metaverse. Most recent interoperability efforts have focused on payment systems, specifically on the interoperability of acquiring and processing services in regard to payment card networks and the interoperability of digital wallets, including quick-response QR codes.

7. Are there any upcoming policies, strategies or regulations that will impact competition in your jurisdiction?

The Peruvian Competition Authority is involved in regional and international forums to discuss and assess the development, supervision and promotion of competition in digital markets, including activities in the metaverse.

Furthermore, the Peruvian Central Reserve Bank is expected to continue in its interoperability efforts in connection with digital wallets.

Intellectual property

Maritza Reátegui *Rodrigo, Elías & Medrano, Lima*
Daniela Supo *Rodrigo, Elías & Medrano, Lima*

1. What public policies, strategies or regulations related to intellectual property are applicable to the metaverse in your jurisdiction?

In Peru, the metaverse currently lacks dedicated intellectual property (IP)-related public policies, strategies or regulations. Consequently, the application of generic IP regulations becomes pivotal for navigating the legal aspects within this digital realm.

Regarding copyright issues within the metaverse, adherence to the stipulations outlined in the Law on Copyright (Legislative Decree No 822) and Decision Number 351 of the Andean Community are imperative. These existing legal frameworks are deemed pertinent for addressing and regulating copyright-related matters in the dynamic landscape of the metaverse.

Similarly, in the realm of trademarks within the metaverse, reliance on the Industrial Property Law (Legislative Decree No 1075) and Decision Number 486 of the Andean Community are crucial for the regulation and protection of trademark rights. While specific regulations on the metaverse may be absent, these established laws offer a foundational basis for safeguarding IP in this digitally evolving environment.

2. How are intellectual property rights to 'virtual objects', 'buildings' and 'avatars', etc, protected in your jurisdiction?

In Peru, the protection of virtual objects is contingent upon the application of the aforementioned regulations. These regulatory frameworks collectively establish the legal foundation for ensuring the protection of IP rights relating to virtual objects.

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

In Peru, the safeguarding of digital replicas of physical objects relies on the application of the aforementioned regulations. Specifically, the Law on Copyright extends its protection to original works of authorship, potentially encompassing digital replicas of physical objects, provided they meet the requisite criteria for creativity.

To qualify for copyright protection, digital replicas must exhibit a certain level of originality, demanding a demonstration of creativity by their creators. This criterion ensures that the legal umbrella extends to those replicas that possess distinctive creative elements.

Moreover, Peru's trademark laws play a pivotal role in shielding distinctive signs, including logos and identifiers associated with physical objects. The unauthorised use of trademarks within digital replicas, especially if it introduces potential confusion, can prompt legal action, underlining the importance of adherence to trademark regulations.

This dual protection mechanism, governed by both copyright and trademark laws, reinforces the comprehensive legal framework dedicated to upholding the integrity and rights associated with digital replicas of physical objects in the Peruvian jurisdiction.

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

In Peru, the protection of user-generated content aligns with the regulations outlined for copyright. The Law on Copyright (Legislative Decree No 822) serves as the foundational legal framework, extending protection to original works of authorship, including user-generated content and derivative works.

Creators or copyright owners in Peru have the authority to take legal action in the event of infringement related to the following:

- initiating infringement action – the owner of the infringed right or the collective management company representing them has the right to initiate an infringement action;
- action for injunction – copyright owners are empowered to initiate an action for injunction, seeking the suspension or cessation of illegal activities related to the unauthorised use or reproduction of their content;
- legal consequences for infringement – in addition to potential fines, regulatory authorities may compel infringers to pay remuneration to the copyright owner or the company representing them for the unauthorised use of user-generated content; and
- procedural costs – creators can demand payment of procedural costs incurred during legal proceedings, ensuring that the financial burden of enforcing copyright protection is appropriately allocated.

This comprehensive legal framework emphasises the rights of creators and copyright owners, providing avenues for legal recourse and protection against unauthorised use or infringement of user-generated content in Peru.

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

There are no such entities.

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

There are currently no specific regulations or case law explicitly addressing the protection and enforcement of IP rights in the metaverse in Peru. Nevertheless, the existing IP laws, encompassing copyrights and trademarks, can be generally extended to cover digital environments.

In the absence of dedicated metaverse-specific regulations, it is probable that the Peru's prevailing intellectual property laws would serve as the underlying framework for safeguarding IP rights in the context of the metaverse.

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?

In Peru, there are currently no IP strategies, policies or regulations specifically tailored to the metaverse with a focus on promoting interoperability within this digital realm.

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

In Peru, there is currently a lack of competition strategies, policies or regulations specifically crafted for the metaverse, with the goal of promoting standardisation and ensuring fair and non-discriminatory access to licences within this digital landscape.

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

No specific issues relating to the metaverse have been addressed in Peru.

10. What are the roles metaverse providers?

Metaverse providers' responsibilities to prevent IP infringement lack explicit regulation. However, the National Institute for the Defence of Competition and the Protection of Intellectual Property (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual or INDECOPI) has, through numerous decisions, delineated the role of platform providers in regard to copyright infringements taking place on their platforms. In cases of copyright infringement, INDECOPI takes the view that platforms knowingly facilitating infringements share joint responsibility for the violation. Consequently, this precedent could potentially be extended to encompass the responsibilities of metaverse providers.

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

A consideration of the conflict between content moderation and freedom of expression is currently lacking in Peru.

12. Are there any by-design notice mechanisms?

There is a lack of any notice mechanisms that are inherently integrated into systems during the design process.

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

To date, there have been no announcements regarding any significant policies that would affect the current IP regulatory framework in Peru.

Digital transactions and ownership

José Villafuerte *Rodrigo, Elías & Medrano, Lima*

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

Peru currently lacks specific policies, strategies or regulations related to tokens, NFTs and digital assets on the metaverse.

However, it should be noted that the Superintendence of the Securities Market (Superintendencia del Mercado de Valores or SMV), the regulator of the Peruvian capital markets, has been frank in a press release stating that there is no specific regulation in Peru covering the offer and/or promotion of tokens, cryptocurrencies or virtual currencies, and that they are not backed by any government entity or financial supervisor. Therefore, companies that make such offers and/or promotions do not fall within its supervision.

Additionally, in 2021, the Peruvian Banking Regulator (Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones or SBS), published a report on the anti-money laundering and counter-terrorism financing (AML/CFT) risks related to virtual assets and virtual asset service providers (VASPs) in Peru. The work behind the report was carried out by the international consulting firm True North Partners, with technical assistance from the German Cooperation in Peru.

Consequently, by means of Supreme Decree No 006-2023-JUS, VASPs were recently incorporated as obliged subjects, required to provide information to the Peruvian Financial Intelligence Unit, for the purpose of identifying offences related to money laundering and terrorism financing. Pursuant to this decree, VASPs comprise any individual or legal entity, domiciled or incorporated in Peru, that is not covered by any other Financial Action Task Force (FATF) Recommendation and that, as a business, engages, for or on behalf of another individual or legal person, in one or more of the activities or transactions described in the decree, all of which are related to the provision of services related to virtual assets (such as the exchange, transfer or custody of such assets).

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

Peru currently lacks specific policies, strategies or regulations regarding digital transactions within the metaverse.

However, it is important to note that the Peruvian Civil Code specifically accepts that contracting parties may express their will through any digital, electronic or alternative means of communication, provided that there are no other specific formalities required by law.

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

Peru currently lacks specific policies, strategies or regulations regarding the ownership of digital assets on the metaverse.

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

The transfer of the ownership of assets is governed by the Peruvian Civil Code, which stipulates that the transfer of movable assets occurs through their physical delivery to the recipient, unless specifically stipulated by law. Concerning real estate, the mere obligation to transfer a particular property renders the recipient its owner, unless there is any legal provision or agreement to the contrary.

Peru currently lacks specific policies, strategies or regulations concerning property transfers within the metaverse.

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

Under the current Peruvian legal framework, there are no specific regulations that apply to currencies or cryptocurrencies used in the metaverse.

However, it is worth noting that, due to the lack of regulation specifically applicable to cryptocurrencies and crypto exchanges, the SBS has pointed out in various press releases certain statements in connection with the collection of funds from the sale of virtual currencies and their offering in Peru, as no specific local regulation exists, emphasising the risks involved when participating in investments with non-regulated entities.

Moreover, please refer to the response to the first question in this chapter regarding the press release from the SMV related to cryptocurrencies and the implementation of the Supreme Decree No 006-2023-JUS related to the AML/CFT obligations applicable to VASPs in Peru.

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

Not applicable.

Q 7. Are there any upcoming policies, strategies or regulations that will impact digital transactions in your jurisdiction?

On 23 June 2023, the Commission of Economy, Banking, Finance and Financial Intelligence of the Congress of the Republic of Peru approved a draft law on the commercialisation of crypto-assets (PL 1042/2021-CR). This draft law, which has yet to be approved by the Plenary of Congress, contains the following main aspects:

- it defines what should be understood by 'crypto-asset', 'cryptocurrency', 'cryptography' and 'blockchain', among others;
- creates a Registry of Cryptocurrency Exchange Platforms, in which banking and non-banking entities that provide cryptocurrency sale and exchange services must register;
- requires banking and non-banking entities that provide cryptocurrency sale and exchange services to be incorporated and domiciled in Peru, or as branches of a foreign company, and to be duly registered in the aforementioned registry;

- requires banking and non-banking entities that provide cryptocurrency sale and exchange services to establish in their bylaws that the exclusive corporate purpose of their business activity is the provision of cryptocurrency exchange services;
- requires banking and non-banking entities that provide cryptocurrency sale and exchange services to adopt control measures focused on detecting and preventing money laundering and terrorist financing activities; and
- establishes the obligation to comply with Peru's personal data protection regulations.

Finally, it should be mentioned that the SBS has announced that it is working on sectoral rules to regulate VASPs regarding the prevention of money laundering and terrorist financing.

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

There is no public information regarding any upcoming policies, strategies or regulations in Peru concerning the metaverse and asset ownership related to it.

Liability and insurance

Sabrina Montoya *Rodrigo, Elías & Medrano, Lima*

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

No.

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

No.

Q 3. What civil liability/tort liability rules are applicable to the metaverse in your jurisdiction? Who is the responsible stakeholder in the case of damages?

This area remains unregulated in Peru and there is no case law on the matter. As such, the general rules on civil liability/tort liability would apply. The responsible party will be whichever party is deemed to have caused the damage.

Q 4. How are liability rules enforced on the metaverse in your jurisdiction? Who are the responsible stakeholders in the case of damages?

This area is unregulated at present.

Q 5. What are the roles of intermediaries and gatekeepers when it comes to the enforcement of rights and liability?

This area is unregulated at present.

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

Given the lack of regulation, specific rules need to be established in Peru regarding the metaverse in order for there to be a market for metaverse insurance.

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

No.

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

No.

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

No.