the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

QATAR

Regional Coordinators:
Angela Flannery *Quay Law Partners, Sydney*
Yoshifumi Onodera *Mori Hamada & Matsumoto, Tokyo*

Data

Catherine Martinez *Cromwell & Moring, Doha*
Pascal Charles Dutru *Ministry of Communication and Information Technology, Doha*

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

The principal legislation governing data protection in Qatar is Law No 13 of 2016, concerning the Personal Data Privacy Protection Law (PDPPL), as well as related regulatory guidelines issued by the National Cyber Governance and Assurance Affairs (NCGAA) in November 2020 (the 'PDPPL Guidelines'). Although the PDPPL Guidelines are non-binding, they are intended to provide controllers with guidance for compliance with the PDPPL and should be referred to for interpreting PDPPL requirements.

There are no data policies, strategies or regulations which specifically apply to the metaverse in Qatar. However, the PDPPL governs the processing of personal data and the protection of data subjects. The PDPPL would be applicable as regards the extent activities within the metaverse involve the collection or handling of personal data in Qatar.

In addition to the PDPPL, the Telecommunications Law No 34 of 2006 also has implications for data protection service providers operating in the metaverse. It lays out the framework for Qatar's telecoms sector, including the licensing requirements applicable to service providers, radio spectrum management and consumer protection.

Other laws which apply to the processing of data in Qatar include Law No 16 of 2010, concerning the Electronic Transactions and Commerce Law, Law No 2 of 2011 on Official Statistics and Law No 14 of 2014, concerning the Cybercrimes Prevention Law.

It is important to note that a separate legal framework applies to the protection of data in the Qatar Financial Centre (QFC). The QFC is an onshore business and financial centre in Qatar which operates independently from the State of Qatar. The QFC has its own legal framework and court system. For the purpose of this questionnaire, discussion is limited to the laws of the State of Qatar.

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

The PDPPL regulates the processing of personal data, which would extend to personal data associated with the metaverse including, but not limited to, the personal data of data subjects processed via devices, third parties and avatars.

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?

The PDPPL applies to any organisation or entity that processes personal data (referred to as data controllers) and sets out the rights, obligations and responsibilities of these entities. Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realising a 'lawful purpose' for the controller or for the third party to whom the personal data is sent. In the absence of consent, the controller must demonstrate, when disclosing and transferring personal data to the data processor, that the transfer is for a lawful purpose and that the transfer of data is made pursuant to the provisions of the PDPPL.

The PDPPL Guidelines mandate certain measures in respect of any transfer of personal data, including but not limited to, notifying clients of the processing and the purpose of the processing, updating privacy notices or policies to include the information set out in the PDPPL Guidelines and conducting a Data Privacy Impact Assessment prior to any new processing activities.

Failure to implement the above measures presents a risk of non-compliance with the PDPPL which could result in civil sanctions.

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

Pursuant to the provisions of the PDPPL, key principles in respect of data protection include the following:

- Transparency, honesty and respect for human dignity.
- Purpose limitation: data should be collected for specified and legitimate purposes and not processed in a manner incompatible for those purposes.
- Data minimisation: excessive irrelevant data should be avoided.
- Accuracy – data controllers are responsible for ensuring the accuracy of the data they process.
- Storage limitation: personal data should be kept in a form that permits identification of data no longer than necessary for the purpose of which it is processed.
- Integrity and confidentiality: controllers must ensure that they have appropriate precautions in place to protect the personal data that they hold and keep it secure.
- Accountability: data controllers are responsible for demonstrating compliance with data protection principles and ensuring data processing activities are conducted in accordance with applicable laws and regulations.

Infringement in respect of the PDPPL can occur as there is often a lack of transparency and users are unclear about how their personal data is collected. Unauthorised data sharing is also in breach of data protection principles and retention of data beyond the necessary period conflicts with the principle of storage limitation.

A violation of the PDPPL may result in civil sanctions, namely fines of up to QAR 5m (approximately US$1.37m). To date, there have been no penalties or sanctions imposed for infringement of data protection under the PDPPL.

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 country/region? What are the most common types of infringement of these rules in the metaverse (eg, unlawful use of proprietary information) in your jurisdiction?

While there are no specific laws relating to the metaverse in Qatar, the legislative framework governing intellectual property, confidentiality and data ownership would apply to non-personal data in the metaverse.

Data sharing and licensing of non-personal data is governed by applicable legislation in regard to patents, trademarks, copyrights and trade secrets.

In Qatar, applicants may benefit from the following types of patent protection:

- national patents under Law No 30 of 2006 (the 'Patent Law');
- patents under the Paris Convention Treaty;
- international (PCT) patent; and
- regional (GCC) patent for protection in six member states.

Qatar Law No 9 of 2002 on Trademarks (the 'Trademarks Law') provides that the following categories are eligible for protection as a trademark: names, signatures, words, letters, numerals, designs, pictures, symbols, stamps, seals, vignettes, reliefs and any other sign or combination of colours, a single non-functional colour, a sound, a smell or a combination of signs, if used or intended to be used to distinguish the products of an industrial, occupational or agricultural enterprise forest exploitation or mining enterprises or goods sold or services offered in the course of trade.

Qatar Law No 7 of 2002 on the Protection of Author's Rights and Related Rights (the 'Copyrights Law') defines a copyright (or author's right) as a legal term used to describe the rights that creators have over their literary and artistic works.

Qatar Law No 5 of 2005 on the Protection of Trade Secrets (the 'Trade Secrets Law') imposes obligations of confidentiality and restrictions on the transfer of confidential information. The Trade Secrets Law defines trade secret information in terms of three key requirements: (1) the information in its totality, form or combined components is usually unknown, or cannot be easily obtained by others who normally deal in such information; (2) the information derives its value from being secret; and (3) the information is confidential due to the measures taken by its legal holder to maintain its confidentiality. The exercise of reasonable measures to safeguard business information is required to maintain trade secret status and protection under the Trade Secrets Law generally. Confidential business information that is not protected by such measures may lose its trade secret status and protection under the Trade Secrets Law.

Article 332 of the State of Qatar Penal Code also covers the disclosure of 'secrets' and mandates penalties for whoever knowingly and illegally divulges a secret entrusted in their official capacity, trade, profession in conditions other than those prescribed by the law or uses it for their personal benefit or for the benefit of another person, without the consent of the person concerned with the secret.

Both civil and criminal sanctions may apply to an infringement of the above laws and, in some cases, penalties may be doubled for repeat offenders.

Civil sanctions include injunctions to ban infringement and seizure of infringing copies and profits. Penalties such as fines are also applicable and, for a serious infringement, there is a risk of potential imprisonment.

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

Pursuant to Article 22 of the PDPPL, any electronic communication to an individual for the purpose of direct marketing is banned unless that individual's prior consent has been obtained. The PDPPL Guidelines clarify that such consent must be: (1) explicit and unambiguous; (2) an affirmative act (ie, pre-ticked boxes or first seeking consent via opt-out notices in the first marketing communication will not be lawful); and (3) easy to withdraw. In addition, controllers cannot collect a 'blanket consent' for more than one processing activity. For example, in collecting the individual's consent, controllers cannot use it for 'any or all future direct marketing communications'. Each consent must be for a specific direct marketing channel.

Notwithstanding the above, a controller may use direct marketing to market specific products and services to customers based on a legitimate interest. In so doing, there is a risk that a customer submits a complaint to the NCGAA for violating Article 22. Such a violation could result in financial penalties of up to QAR1m. In addition to the financial risk, there is potential reputational risk in receiving complaints and/or being fined.

Q 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring 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 PDPPL includes the following provisions applicable to the protection of minors.

Websites for children

The PDPPL requires the operators of websites targeting children to post specific notifications and obtain the explicit consent of a child's guardian.

Sensitive personal data

Personal data relating to children is considered sensitive personal data under the PDPPL. Processing of sensitive personal data requires a separate permit from the Ministry of Transport and Communications and additional safeguarding measures to be in place.

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

Article 15 of the PDPPL bans data controllers from taking any measures to prohibit cross-border data flows, which refers to accessing, watching, retrieving, using or storing personal data without restriction of the State's border. However, controllers are permitted to take measures against cross-border data flows if such processing is in violation of the PDPPL or might result in serious harm to the personal data or the individual.

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 rules applicable to automated decision-making in your jurisdiction?

The PDPPL requires data controllers to notify the regulator in the event of a data breach which may cause serious damage to a data subject. The PDPPL indicates that one example of processing, which is impacted by a breach, that could increase the severity of damage to individuals is the carrying out of automated decision making.

The data controller should notify the NCGAA and individuals of a personal data breach within 72 hours of becoming aware of it.

To date, there is no case law or regulatory decisions regarding infringement of the PDPPL in respect of automated decision making.

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

The PDPPL grants individuals the following rights with respect to their personal data:

- the right to protection and lawful processing;
- the right to withdraw consent;
- the right to object to processing in certain circumstances;
- the right to erasure;
- the right to request correction;
- the right to be notified of processing;
- the right to be notified of inaccurate disclosure; and
- the right to access their personal data.

If individuals are not satisfied with how the controller has handled their request, they can make a complaint to the NCGAA as the data privacy regulator. The PDPPL requires that controllers receive and investigate complaints from individuals about how their personal data is processed. It also requires the NCGAA to investigate complaints about controllers from individuals and issue reasoned binding decisions compelling the controller to take action where the NCGAA sees fit following any investigation.

There have been no penalties or sanctions imposed for infringement of the PDPPL to date.

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

In February 2024, the Ministry of Communications and Information Technology launched the Digital Agenda 2030 to advance the technology sector and promote digital transformation in Qatar. Pursuant to the Digital Agenda 2030, one of the objectives is to develop a national framework for four key emerging technologies (the metaverse, the internet of things (IoT), blockchain and AI) by 2030. The framework is expected to include strategies, policies and regulations that promote the effective development, deployment, scaling and widespread adoption of emerging technologies, while also ensuring safety and privacy.

Cybersecurity

Catherine Martinez *Cromwell & Moring, Doha*
Pascal Charles Dutru *Ministry of Communication and Information Technology, Doha*

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

While there are no cybersecurity policies, strategies and regulations which specifically apply to the metaverse in Qatar, legal regulations relating to cybercrime dealing with offences such as unauthorised access, data breaches and hacking have been enacted. Qatar also has a national cybersecurity strategy developed to focus on promoting cybersecurity capabilities and awareness within the government and private sectors as referred to below.

The legal framework governing cybersecurity in Qatar comprises the following:

- 2005: Qatar Computer Emergency Response Team (Q-CERT) to address cyber and critical infrastructure challenges.
- 2014: Qatar Law No 14 of 2014 on the Issuance of the Law on Combatting Cybercrimes (the 'Cybercrime Law'), which defines specific computer and data-related crimes, electronic forgery and intellectual property infringements.
- 2014: Qatar published its National Cyber Security Strategy to align the relevant agencies and create the entities and governance structures needed to address cybersecurity threats.
- 2018: Qatar presented its 2022 Cybersecurity Framework (QCF) for government institutions, critical infrastructure stakeholders and businesses surrounding the needs of the 2022 FIFA World Cup.
- 2018: The QCF comprises a set of guidelines that are engineered to ensure that organisations follow and maintain cybersecurity best practices. The QCF consists of six core components: strategy and governance; risk management; protection; detection and response; recovery; and collaboration and partnership.
- 2021: National Cyber Security Agency (NCSA) established to revamp its 2014 Cyber Security Strategy.

The following additional laws also contain provisions which may be applicable to cybersecurity:

- Qatar Law No 8 of 2008 on Promulgating the Consumer Protection Law (the 'Consumer Protection Law').
- Qatar Law No 34 of 2006 on the Promulgation of the Telecommunications Law (the 'Telecommunications Law').
- Qatar Law No 16 of 2010 on the Promulgation of the E-Commerce and E-Transactions Law (the 'E-Commerce Law').
- Qatar Law No 13 of 2016 on the Promulgation of the Personal Data Privacy Protection Law (PDPPL).

The Communications Regulatory Authority is responsible for enforcing cybersecurity regulations and standards for organisations in Qatar.

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

There are no secure by design principles applicable to the metaverse in Qatar. However, as Qatar has been actively investing in digital transformation and cybersecurity, consideration for the metaverse would align with the broader cybersecurity incentives referred to above.

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

There have been no cyberincidents in respect of the metaverse in Qatar.

Sanctions for cyber incidents can be civil and criminal. Article 8 of the Cybercrime Law stipulates that a sentence of not more than three years in prison and a fine of not more than QAR 100,000 (approximately US$27,460). Either of these penalties, shall be imposed on any person who, through an information network or information technology technique, violates social values or principles, publishes news, photos or video or audio recordings related to the sanctity of people's private or family life, even if the same is true, or insults or slanders others.

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

There are no specific cybersecurity standards applicable to the metaverse. However, the laws highlighted above and international standards such as the General Data Protection Regulation (GDPR) provide a guide to cybersecurity practices in virtual environments.

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

In February 2024, the Ministry of Communications and Information Technology launched the Digital Agenda 2030 to advance the technology sector and promote digital transformation in Qatar. Pursuant to the Digital Agenda 2030, one of the objectives is to develop a national framework for four key emerging technologies (the metaverse, IoT, blockchain and AI) by 2030. The framework is expected to include strategies, policies and regulations that promote the effective development, deployment, scaling and widespread adoption of emerging technologies, while also ensuring safety and privacy.