Photo by Fit Ztudio on Shutterstock

LEXOLOGY
Getting the Deal Through

Market Intelligence

DIGITAL TRANSFORMATION 2022

Global interview panel led by Kemp IT Law

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by Kemp IT Law, this *Digital Transformation* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Government policy
Procurement best practice
Contractual negotiations
Cybersecurity & data protection

START READING

About the editors

Richard Kemp and Deirdre Moynihan
Kemp IT Law

Richard Kemp is a partner at Kemp IT Law. He has advised clients on digital transformation projects in the professional services, transportation, retail and market data sectors. Widely recognised as one of the world's top IT lawyers, he is in *The Legal 500*'s Hall of Fame and is one of *Who's Who Legal*'s 20 global elite data law thought leaders. Richard set up Kemp & Co in 1997, Kemp Little in 2001 and Kemp IT Law in 2014. Under the strapline 'IT Law at the Apex', Kemp IT Law has won over 100 awards for client service and innovation since 2015.

Deirdre Moynihan is a partner at Kemp IT Law LLP. She routinely advises organisations in all sectors on digital transformation projects, and has a particular focus on data-related issues and on supporting law firms procuring and deploying new technologies. Deirdre, a Certified Information Privacy Professional and Manager, has been recognised as a 'Next Generation Lawyer' by *The Legal 500* from 2021–2023, including for 'adeptly handl[ing] digital transformation projects'. Deirdre is included in *Who's Who Legal* 2021 as an expert in data law and is recommended by *Chambers* and *The Legal 500* for 'deep sector expertise' in IT and as a 'formidable and effective negotiator and a pleasure to work with' by 'providing clear and decisive advice'.

Contents

While reading, click this icon to return to the Contents at any time

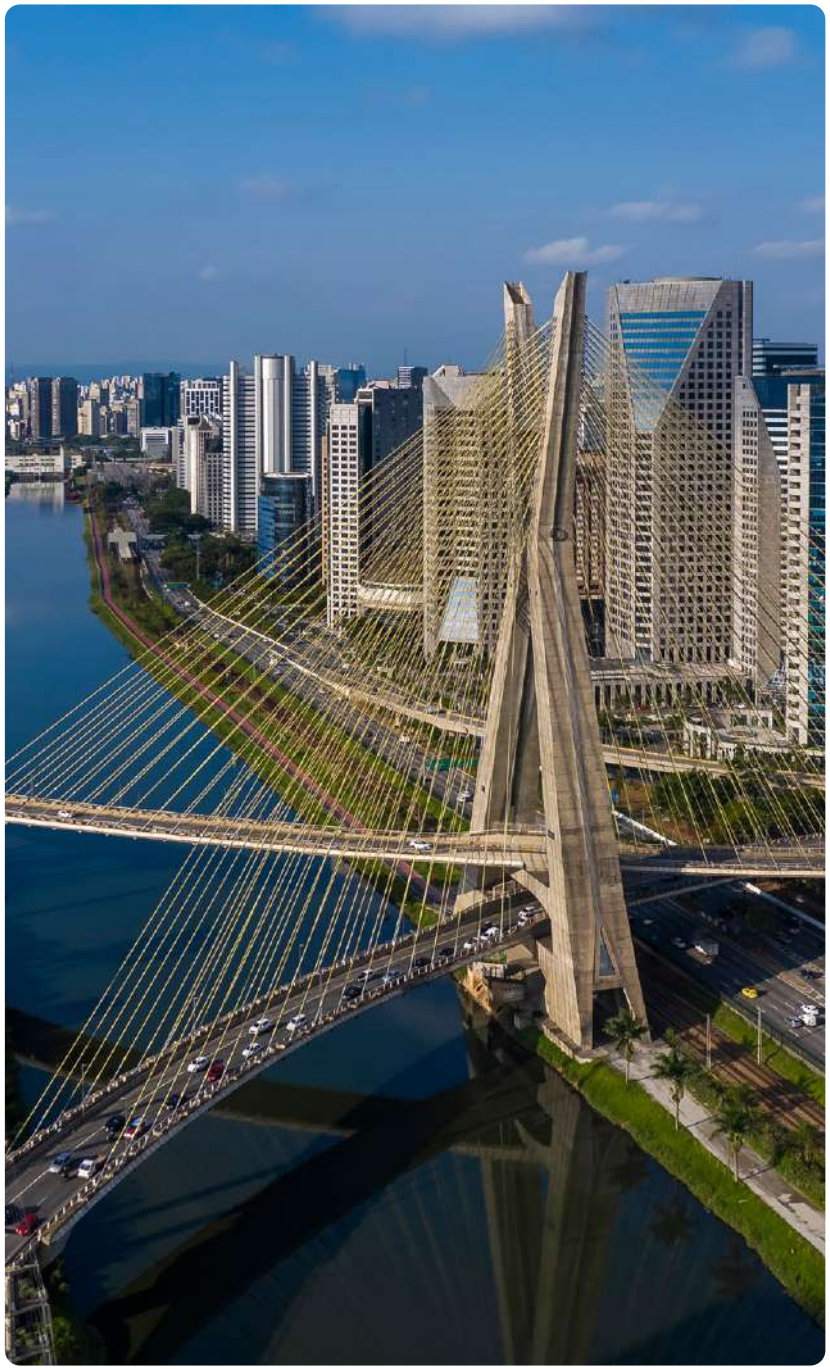

Photo by Erich Sacco on Shutterstock

Brazil

Ricardo Barretto Ferreira da Silva is a senior partner and head of TMT legal practice at Azevedo Sette Advogados. He is an attorney with experience in TMT, corporate, tax, M&A, intellectual property, privacy and data protection. He was co-founder, vice president (1989–1994) and president (1995–1998) of the Brazilian Information Technology and Telecommunications Association. He has had various articles published in Brazil and abroad on IP, IT, media, telecoms, privacy, data protection, outsourcing, and copyright.

Lorena Pretti Serraglio is a senior associate at Azevedo Sette Advogados. Lorena coordinates projects to assist clients with compliance with the Brazilian General Data Protection Act and the preparation of legal opinions, contracts, and memos. She is a consultant of the Special Data Protection Commission of the Federal Council of Brazilian Bar Association.

Juliana Gebara Sene Ikeda is a partner in the TMT legal practice at Azevedo Sette Advogados and head of the intellectual property area. Juliana coordinates projects in order to structure technology companies in Brazil and assists clients with the preparation of legal opinions, contracts and memos in the areas of technology, digital law and IP issues on the internet. She has also co-authored articles on these areas.

Sylvia Werdmüller von Elgg Roberto is an associate at Azevedo Sette Advogados. She acts in the areas of technology, media, and telecommunications, focusing on telecommunications matters. Her education includes a bachelor's degree from Mackenzie University Law School, Brazil and ongoing post-graduate study in digital law from Escola Paulista de Direito, Brazil.

QUESTIONS

1 What are the key features of the main laws and regulations governing digital transformation in your jurisdiction?


Ricardo Barretto Ferreira da Silva


Lorena Pretti Serraglio


Juliana Gebara Sene Ikeda


Sylvia Werdmüller von Elgg Roberto

In Brazil, the Decree No. 9,319/2018 has created the National System for the Digital Transformation and established the governance structure for the implementation of a Brazilian Strategy for Digital Transformation (e-Digital). Its digital transformation aims to include economic digital transformation, which stimulates an economy based on data, with incentives to the development of telecommunications infrastructure and the attraction of data centres to Brazil; a world of connected devices, recognising the potential of the internet of things (IoT) applications; and new business and market models, especially in the digital field, more competitive and flexible.

E-Digital also brings the governmental digital transformation, focusing on offering simple and intuitive digital public services through a single and centralised platform, wide access to information and open data, interoperability between governmental databases, availability of a digital identification for the citizens, the implementation of the Brazilian General Data Protection Act (Law No. 13,709/18) (LGPD), among other initiatives.

It is worth mentioning that Decree No. 10,332/2020 institutes the Digital Government Strategy for 2020-2022, in the scope of the bodies and entities from the Federal Public Administration, autarchies and foundations, observing the provisions of E-Digital.

Further to this, Decree No. 10,046/2019 provides for governance in data sharing within the Federal Public Administration and institutes the Citizens Base Register and the Central Data Governance Committee; Decree No. 9,854/2019 institutes the National Plan of Internet of Things and the Chamber of Management and Monitoring of the Development of Machine-to-Machine Communication Systems and IoT; Decree No. 10,278/2020 establishes the technique and the

> "We have seen the creation of the digital portal, which offers digital public services and guarantees identification of every citizen accessing these services."

requirements for the digitalisation of public or private documents, so that these digital documents produce the same legal effects as the original physical documents; and Decree No. 10,382/2020 institutes the Strategic Management and State Transformation Program (TransformaGov), which intends to implement measures of institutional transformation in the Federal Public Administration.

2 What are the most noteworthy recent developments affecting organisations' digital transformation plans and projects in your jurisdiction, including any government policy or regulatory initiatives?

There are several noteworthy recent developments affecting organisations' digital transformation plans and projects in the Brazilian jurisdiction.

First, we have seen the creation of the digital portal, gov.br, courtesy of Decree No. 9,756/2019, which offers digital public services and guarantees identification of every citizen accessing these services. Furthermore, Law No. 13,989/2020, which provides for the use of telemedicine (long-distance patient and clinician contact) during the crisis caused by the coronavirus pandemic, and establishes that the Federal Council of Medicine may regulate telemedicine after the pandemic. Under Law No. 14,063/2020, provision is made for the use of electronic signatures in interactions with public entities, acts of legal entities and in health issues and on software licences developed by public entities, reducing the bureaucracy of electronic signatures in documents to expand access to digital public services. Also, Resolution No. 1/2020 from the Brazilian Central Bank institutes the payment arrangement 'PIX' and approves its regulation, disciplining the provision of payment services related to instant payment transactions and the instant payment transaction itself, under the arrangement. Law No. 13,709/18 (the General Data Protection Act (LGPD)), formalised by Law No. 14,058/2020, brings legal responsibilities for the agents that process personal data, including by digital means; and Law No. 14,075/2020 extends the use of digital social savings account to receive social benefits from the federal government. These are just some of the initiatives that have been particularly stimulated by the covid-19 pandemic. Furthermore, the Latin American Economic Outlook (LEO) 2020: Digital Transformation for Building Back Better report, produced by the Organisation for Economic Co-operation and Development (OECD) and other entities, points out that 'digital transformation is the key in accelerating the recovery of Latin America and the Caribbean from the crisis caused by covid-19', and this may incentivise the transformation further.

Also relevant, in a bidding procedure in November 2021, the National Telecommunications Agency (ANATEL) auctioned radio frequencies in the 700MHz, 2.3GHz, 3.5GHz and 26GHz bands and granted authorisations to exploit the Personal Mobile Service, aiming to expand telecommunications services with 4th generation technology (4G) and, in addition, implement 5th generation technology (5G) in

Brazil. The 5G is already being offered in the country's capitals and is expected to ensure the requirements necessary to enable the concepts of ultra reliable low latency communications (URLLC), massive machine-type communication (mMTC) and enhanced mobile broadband (eMBB), which, in turn, will serve different business models and applications, including IoT devices, in areas such as public safety, telemedicine and smart cities.

The Federal Revenue along with the Serpro (Federal Service of Data Processing) launched a platform that relies on blockchain technology, called b-Cadastros, which enables the data bases of social security number (CPF), national register of legal entities (CNPJ), and other registers to be shared with public entities and the entities associated to them. The platform allows the participants of the blockchain network to receive only the composition of bases that may interest them; for example, they may choose to receive only the CPF base or the CPF and CNPJ bases, or any other composition necessary for their activities, through its own infrastructure or provided by Serpro. Consequently, it will improve data protection and enable lower costs.

Finally, Resolution No. 333/2020 of the National Council of Justice (CNJ) institutes ethics, transparency, and governance in the creation and use of artificial intelligence (AI) in the judiciary. It establishes that court decisions that support AI must preserve ethical values. In continuance, Bill No. 21/2020 creates the legal framework for the development and use of AI by the government, companies, various entities and individuals. The text is in progress in the Senate now and establishes principles, rights, duties and governance instruments for AI. The bill establishes that the use of AI will be based on respect for human rights and democratic values, non-discrimination, plurality, free enterprise and data privacy.

Photo by windwalk on Shutterstock

QUESTIONS

3 What are the key legal and practical factors that organisations should consider for a successful cloud and data centre strategy?

Before creating and/or implementing any cloud and data centre strategy, it is essential to understand the technologies and the current IT environment of the organisation. After mapping the issues in the current environment, the company must establish its goals within the context of a new structure, and it must maintain the software and hardware control systems updated, as well as frequent monitoring of IT resources, provide precise information for legitimate purposes, and preferably invest in international data security certifications. In any case, in order to have a successful cloud and data centre strategy, organisations shall consider the risks, costs, and technologies involved. The idea is to mitigate all risks (including, without limitation, legal risks, such as potential breaches of data protection regulation), as well as maximise the use of new technologies, and preferentially reduce costs.

> "To reduce legal and business risks associated with digital transformation projects, it is recommended that companies review existing internal documents."

Specifically regarding legal factors, it is important to have in mind that any cloud and data centre strategy has its concerns. Despite all its advantages, organisations must take into consideration cybersecurity issues in general. These organisations need to adopt and implement serious security procedures, such as security training. They also need to be aware that the stored data can be compromised or breached. Cloud computing services are not regulated by any specific law, although they are subject to the regulations set forth in the Civil Code (Law No. 10,406/2002) concerning the performance of the services and liability of the service provider. Notwithstanding the above, both technologies are subject to the provisions of the General Data Protection Act (13,709/2018), which ensure the security and confidentiality of all personal data of individuals and legal entities and imposes administrative sanctions and penalties in the event of non-compliance with the law. Data centre and cloud providers offer different levels of security protection, and in any case, such protection is not total. There are always warranty disclaimers and limitation of liability provisions. This is why the contracts between such organisations and their IT providers for data centre and cloud services need to be well negotiated and reviewed.

Therefore, to reduce legal and business risks associated with digital transformation projects related to cloud and data centre strategy, it is recommended that companies review existing internal documents to analyse if the deployment of the technology is viable, consulting with professionals that can address how the technology works and what the benefits and consequences are for the customers. Companies should also negotiate robust contracts with suppliers, as well as provide audit compliance of suppliers' documents and procedures. Proofs of concept shall be performed on limited terms, to avoid liabilities on the business and eventual inadequate processing of information. Finally, companies must establish additional legal obligations to secure compliance whenever necessary.

4 What contracting points, techniques and best practices should organisations be aware of when procuring digital transformation services at each level of the cloud 'stack'? How have these evolved over the past five years and what is the direction of travel?

IT service agreements, such as data centre and cloud services agreements, have similar relevant contracting points. Furthermore, despite the development of new technologies and new regulation related to this matter (especially involving data protection) in the past five years, main negotiation issues remain the same: due diligence and migration terms; implementation schedules; full description of services (in order to avoid additional charges); service levels; data protection, data portability and backup; compliance with applicable laws; warranties and liability; penalties; and, finally, business continuity and disaster recovery.

Photo by f11photo on Shutterstock

As mentioned above, it is recommended, from a digital transformation point of view, to understand the particularities of cloud service and delivery models before the implementation of a cloud due diligence, procurement and contracting. Following this perspective, it is important that companies are aware about new IT techniques – such as blockchain, 5G, IoT, among others – when procuring digital transformations services, since the legal responses to them heavily depend on the clarity of how these technologies work and their possible consequences.

In the past two decades, organisations have been concerned with the issues above, and the only development (besides new technologies) we had is that local laws are now establishing further requirements in connection with these services, especially regarding data protection and security issues. With the LGPD, the security of data became an obligation for organisations that deal with personal data, through the supervision of a data protection officer (DPO), who must be hired by the organisation to ensure that the processing of data is in compliance with the applicable data protection rules. We believe that in view of the consolidation of these new laws and, as a result, the creation of case law regarding this matter, organisations and suppliers will have solid grounds to negotiate their agreements in the near future.

5 In your experience, what are the typical points of contention in contract discussions and how are they best resolved?

The main negotiation issues related to data centre and cloud services agreements are due diligence and migration terms; implementation schedules; full description of services (in order to avoid additional charges); service levels; data protection, data portability and backup; compliance with applicable laws; warranties and liability; penalties; business continuity, and disaster recovery. These issues are mostly solved within a commercial context. For example, in order to have greater warranties and service levels, the organisation will offer higher compensation to its providers. Penalties can be lower or higher depending on the schedules agreed by and between the parties.
In addition, many issues are technical, such as disaster recovery procedures and all security procedures related to data storage. In this regard, although some local laws may set forth minimum technical requirements, many organisations have their own standards, even stricter than local regulations, in order to avoid security breaches and the possible damage of reputation.

There is no specific rule to solve these contention points. The parties must take into consideration minimum legal standards, but in general, they are free to negotiate them in accordance with their own policies and practices.

6 How do your jurisdiction's cybersecurity laws affect organisations on their digital transformation journey?

Decree No. 9,637/2018 has created the National Policy of Information Security, which expressly establishes that the Office of Institutional Security of the President shall draft and publish a National Strategy of Information Security, in articulation with the Interministerial Committee for Digital Transformation. Later, Decree No. 10,222/2020 approved the National Cyber Security Strategy (E-Ciber), a manifest orientation of the federal government to Brazilian society indicating its intended actions for cybersecurity, in the national and international scenario, within the period 2020–2023. It is the first module of the National Strategy of Information Security. Among its strategic goals, fundamentally based on the transformations caused by the digital revolution, we should mention the strengthening of governance actions in cybersecurity by the public and private sectors, which contemplates initiatives related to people management, compliance with cybersecurity requirements and management of information assets.

Also important is ANATEL's Resolution No. 740/2020, which approved the Regulation of Cybersecurity Applied to the Telecommunications Sector, setting forth conducts and procedures to promote security in telecommunications networks and services and protect critical telecommunications structures, being applicable to collective interest telecommunications services providers, except those deemed small-sized providers as per the relevant regulations (even though some providers might become or cease to be subject to the provisions thereof). Notwithstanding, its principles and guidelines should be complied with by all collective and restricted interest telecommunications service providers, regardless of their size.

In addition, Normative Instruction No. 4/2020 of the Office of Institutional Security of the Republic Presidency sets forth the minimum cybersecurity requirements that should be adopted in the establishment of 5G networks.

> "Decree No. 10,222/2020 approved a manifest orientation of the federal government to Brazilian society indicating its intended actions for cybersecurity."

Furthermore, the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014) establishes principles, guarantees, rights and obligations for the use of the internet in Brazil. Among its provisions, the preservation of stability, security and functionality of the network, via technical measures consistent with international standards and good practices, brings an incentive for cybersecurity in organisations.

Decree No. 8,771/2016, which regulates the Brazilian Civil Rights Framework for the Internet, also provides some security and secrecy standards of registers, personal data and private communications, determining that applications and connection providers (ASPs and ISPs) shall establish strict control over the access to data, provide authentication mechanisms for access to records, create a detailed inventory of access to connection and application access records and use record management solutions by means of techniques that

Photo by ESB Professional on Shutterstock

ensure the inviolability of data (such as encryption or equivalent protection measures).

7 How do your jurisdiction's data protection laws affect organisations as they undergo digital transformation?

The LGPD affects organisations as they undergo digital transformation, since the processes of digitalisation involve a lot of types of personal data processing, such as the manipulation of big volumes of data, storage, sharing and automation of activities. Also, the LGPD applies to any processing operation carried out by a natural person or a legal entity of public or private law, irrespective of the means, the country in which its headquarters is located or the country where the data are located, provided that the processing operation is carried out in the national territory; the purpose of the processing activity is to offer or provide goods or services or the processing of data of individuals located in the national territory; or the personal data being processed have been collected in the national territory. The processing agents – namely the controller, who takes the decisions about the processing of personal data, and the processor, who processes personal data on the controller's behalf – shall keep records about the operations of personal data processing. Also, the international transfer of personal data is only allowed through the legal mechanisms provided by the LGPD, which include level of adequacy; standard or specific contractual clauses; execution of contract; and compliance with a legal or regulatory obligation.

Processing agents must also adopt technical and administrative security measures, able to protect personal data from unauthorised accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing. These measures shall be observed by design (ie, from the initial stage of a product or service to its execution).

Furthermore, the LGPD establishes the obligation of communication about the occurrence of a security incident that may cause risks or relevant damage to data subjects, resulting in a strategy focused on the data subject experience; and the obligation that operational processes and systems used for the processing of personal data are structured, so as to meet security requirements, standards of good practice and other regulatory standards.

All these elements are important to guarantee an efficient governance privacy programme, capable of addressing digital transformation in a legitimate way.

QUESTIONS

"In Brazil, effective governance and best practice for digital transformation constitutes the harmonisation of initiatives."

8 What do organisations in your jurisdiction need to do from a legal standpoint to move software development from waterfall through Agile to DevOps?

There is no immediate action required from a legal point of view in order to move traditional software to DevOps at this moment. In Brazil, software protection laws are in accordance with international standards (provided by the World Trade Organisation and its international treaties). Software registration (for protection purposes) is not mandatory, so there is no bureaucratic issue. Thus, software developers, contractors and users shall enter into specific agreements that cover this kind of progress without any legal impediment.

However, considering the necessity of more flexibility, effective communication, and processes management that move software development to DevOps, from a legal point of view, organisations are recommended to implement internal policies to cope with this development (for example, a policy about software assets management, to ensure the adequate use of third-party software, within its licence scope).

9 What constitutes effective governance and best practice for digital transformation in your jurisdiction?

In Brazil, effective governance and best practice for digital transformation constitutes the harmonisation of initiatives with the purpose of using the potential of digital technologies to promote sustainable and inclusive social and economic development, with innovation, as well as increased competitiveness, productivity, employment and income levels in the country.

Photo by Gustavo Frazao on Shutterstock

To implement this definition, it is necessary to look for: the promotion of the expansion of internet access and digital technologies for the population; incentives for the development of innovative technologies derived from scientific research; increased trust in the digital environment, especially with laws that have well-defined rights; education and professional training on advanced technologies and the work of the future; regional integration in the digital economy; and the stimulation of competitiveness and the presence of Brazilian companies abroad.

In companies, digital transformation governance and best practice can be implemented through the use of planned infrastructure and architecture to prevent security threats and allow the transformation; awareness of employees so that they understand the care that must be taken with regard to customers' data and best practices of the market; the arrangement and negotiation of robust contracts with suppliers, along with constant management of execution risks; updated risk assessments of the management of data and cybersecurity; and effective internal policies covering DevOps.

It is essential to consider the relevance of data governance in digital transformation since companies generate an exponential volume of data and progressively use it in their decision-making. Data governance shall observe the value, cost, risks and constraints of data to analyse, on a case-by-case basis, the impacts of the uses of data in digital transformation.

Also, it is necessary to transform and adapt the processes related to artificial intelligence, big data, and data analytics, in order to guarantee compliance with data protection rules and the security of information, which is essential to maintain the efficacy of the companies' strategies, as well as achieve higher commercial values of data.

Ricardo Barretto Ferreira da Silva
barretto@azevedosette.com.br

Lorena Pretti Serraglio
lserraglio@azevedosette.com.br

Juliana Gebara Sene Ikeda
jikeda@azevedosette.com.br

Sylvia Werdmüller von Elgg Roberto
selgg@azevedosette.com.br

Azevedo Sette Advogados
São Paulo
www.azevedosette.com.br

Read more from this firm on Lexology

QUESTIONS

The Inside Track

What aspects of and trends in digital transformation do you find most interesting and why?

The increasing provision of digital services to citizens fosters investments in telecommunications infrastructure and information security, heading towards the digital inclusion of the population, with trust in digital relations. Accelerated digital transformation brings efficiency, riches and infinite possibilities to companies, and those with greater digital maturity stand out in the market. The development of IoT, artificial intelligence, and smart cities also benefit from digital transformation (especially through public–private partnerships). The arrival of 5G technology in Brazil tends to bring investments in big data, edge computing, AI, and IoT as well, generating effects of digital transformation in society. In addition, the covid-19 pandemic had significant effects on the future of digitalisation in Brazil, the 'new normal' tends to stay, impacting health, education, the judiciary and the government. However, it is common that regulation and innovation do not go together (a clear example is the regulatory scenario of artificial intelligence in Brazil, which has been much debated), and companies and entities must be aware of new technologies to have the ability to understand the speed and the depth of transformations these tools provide.

What challenges have you faced as a practitioner in this area and how have you navigated them?

As practitioners in the area, we faced challenges related to the fast transformation of technologies (which required a fast learning of technical aspects of technologies and the applicable legal grounds), as well as difficulties in addressing legal frameworks to technologies that are not regulated, keeping up with their evolution, which requires a lot of intersectoral work and analysis of legislation from other countries, in order to develop fast responses. Despite the LGPD, many developments of the law depend on complementary regulations of the National Authority (ANPD), so we need to be aware of the best market practices and interpret the principles of Brazilian law.

What do you see as the essential qualities and skill sets of an adviser in this area?

Some of the essential qualities and skill sets are great legal knowledge, not only from Brazil, but also from other jurisdictions. It is also important: (1) to follow the process of creation and discussion of new laws related to technology and digital transformation in Brazil, protecting the business from obscure complexities and contributing to the digital transformation governance; (2) to have some level of technical knowledge, understanding basic aspects related to new technologies that allow digital transformation; (3) to plan digitalisation in an organised and strategic manner (involving the creation of policies, the negotiation of contracts, the management of liabilities and continuous assessment of risks, legal issues and concerns related to the deployment of new technologies); and (4) to have someone who can establish an efficient and continuous communication with all the agents involved in the digital transformation journey.