LEXOLOGY

Market Intelligence

Digital Transformation

Ricardo Barretto Ferreira, Lorena Pretti Serraglio, Juliana Gebara Sene Ikeda, Sylvia Werdmüller von Elgg Roberto, Isabella da Penha Lopes Santana Azevedo Sette Advogados

Published December 2021

Brazil

Ricardo Barretto Ferreira da Silva was co-founder and managing partner of two renowned law firms (CFF and BKBG) (1975–2004 and 2004–2016, respectively) before becoming a senior partner and head of TMT legal practice at Azevedo Sette Advogados. Ricardo is an attorney with experience in corporate, tax, M&A, intellectual property, technology, media, telecommunications, privacy and data protection.

Lorena Pretti Serraglio is a senior associate at Azevedo Sette Advogados and coordinator of privacy and data protection projects. She acts in the areas of technology, media and telecommunications, focusing on digital law and data protection. She is a consultant to the Special Data Protection Commission of the Federal Council of Brazilian Bar Association.

Juliana Gebara Sene Ikeda is a senior associate at Azevedo Sette Advogados. Juliana coordinates projects to structure technology companies in Brazil and assists clients with the preparation of legal opinions, contracts and memos in the areas of digital law, privacy and data protection.

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.

Isabella da Penha Lopes Santana is an associate member of the technology, media, and telecommunications team at Azevedo Sette Advogados.

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

In Brazil, 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.

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 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 Programme (TransformaGov), which aims 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 Brazilian 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 especially stimulated by the covid-19 pandemic. Furthermore, the Latin American Economic Outlook 2020: Digital Transformation for Building Back Better report, produced by the Organisation for Economic Co-operation and Development 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 scheduled to be held in November 2021, the National Telecommunications Agency (ANATEL) will auction radio frequencies in the 700MHz, 2.3GHz, 3.5GHz and 26GHz bands and grant authorisations to exploit the Personal Mobile Service, aiming to expand telecommunications services with fourth-generation technology (4G) and, in addition, implement fifth-generation technology (5G) in Brazil. The 5G, expected to be offered in July 2022, will ensure the requirements necessary to enable the concepts of Ultra Reliable Low Latency Communications, massive Machine-Type Communication and enhanced mobile broadband, 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 new platform that relies on blockchain technology, called b-Cadastros, which enables the databases 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, eg, 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 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 addition, 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, in progress in the House of Representatives, establishes principles, rights, duties and governance instruments for the 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.

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. In any case, 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 ideally reduce costs.

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. 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 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, with professionals who can address how the technology works and what are the benefits and consequences 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 (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.

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. From this perspective, it is important that companies are really aware about new IT techniques – such as blockchain, 5G and 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 its possible consequences.

In the past two decades, organisations have been concerned with the issues above and the only development (besides new technologies) is that local laws are now establishing further requirements in connection with these services, especially regarding data protection and security issues. We believe that in view of the consolidation of these news 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 (to avoid additional charges); service levels; data protection, data portability and backup; compliance with applicable laws; warranties and liability; penalties; and business continuity and disaster recovery. These issues are mostly solved within a commercial context. For example, 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). This 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.

Furthermore, the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014) establishes principles, guarantees, rights and obligations for the use of 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 the 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 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 Brazilian General Data Protection Act (Law No. 13,709/18 (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 or 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 are 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 on the operations of personal data processing. Also, the international transfer of personal data is only allowed through the legal mechanisms provided by 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, since 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, bringing 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 the digital transformation in a legitimate way.

8 What do organisations in your jurisdiction need to do from a legal standpoint to move software development from (traditional) waterfall through Agile (continuous improvement) to DevOps (continuous delivery)?

There is no immediate required action from a legal standpoint 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 covers this kind of progress without any legal impediment.

However, considering the need for more flexibility, effective communication and processes management that move software development to DevOps, from a legal standpoint, 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 using the potential of digital technologies to promote sustainable and inclusive social and economic development, with innovation, as well as increased competitiveness, productivity and employment and income levels in the country.

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, with respect to citizens' rights; education and professional training on

advanced technologies and the work of the future; the regional integration in 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; 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 also essential to consider the relevance of data governance in the 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, to guarantee the compliance with data protection rules and the security of information, which is essential to keep the efficacy of the companies' strategies, as well as achieve higher commercial values of data.

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. The development of IoT and smart cities also benefit from digital transformation (especially through public-private partnerships) and 5G technology tends to be increasingly boosted by digital transformation effects in society. Furthermore, a study, entitled Digitisation, Resilience and Business Continuity, organised by Deloitte, presents some considerations about the future of digitisation in Brazil due to the effects of covid-19, demonstrating that the Brazilian 'new normal' will have high impacts on health, education, the judiciary and the government.

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, and keeping up with its evolution, which requires a lot of intersectoral work to develop fast responses, especially during the recent coronavirus crisis. The covid-19 pandemic caused organisations to move quickly to the home office system, which was a major challenge.

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

Some of the essential qualities and skillsets are great legal knowledge, protecting the business from obscure complexities and contributing to the digital transformation governance; some level of technical knowledge, understanding basic aspects related to new technologies that allow digital transformation; an organised and strategic planning of digitisation (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 someone who can establish an efficient and continuous communication with all the agents involved in the digital transformation journey.