REFERENCES

Bennett, C. & Raab, C. (2006). *The governance of privacy*: *Policy instruments in global perspective*. Cambridge: MIT.

Bennett, C. & Raab, C. (2018). Revisiting 'the governance of privacy': Contemporary policy instruments in global perspective. Paper presented at the Privacy Law Scholars Conference, Berkeley, CA, June 1-2. Retrieved on 16 May 2019 from https://ssrn.com/abstract=2972086.

Bioni, B. R. (2014). A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. *Direitos e novas tecnologias*: XXIII National Meeting of Conpedi, 1, 59-82.

Hartmann, M. & Wimmer, J. (2011). Einleitung. In J. Hartmann & J. Wimmer (Eds.), *Digitale Medientechnologien*: Vergangenheit – Gegenwart – Zukunft (pp. 21). Wiesbaden: VS.

Manifesto pela aprovação da Lei de Proteção de Dados Pessoais. (2018). São Paulo. Retrieved from https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais.

Mattern, F. (2008). Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In Roßnagel, A. et al. *Digitale Visionen*: Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlin: Springer.

Mendes, L. S. (2014). *Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva.

Mendes, L. S. & Doneda, D. (2016). Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, v. 9.

Interview I

I.S.O._ In your view, who are the main actors and what are the dynamics that make up the ecosystem of governance and regulation of personal data?

B.B._ On the one hand, there are data subjects, i.e., citizens who own the information linked or corresponding to them – for this reason, referred to as personal data. There are also agents who process this data – the organizations that collect and manage information, such as the private and public sectors. There is a subdivision within these agents: controllers, i.e., those who determine how the data will be processed. In some situations, they outsource part of the data processing. In these cases, operators come into the picture, for example companies contracted to provide data storage services, such as cloud computing. Among this constellation of actors, there are also regulatory agencies. In this regard, a key element of the new Brazilian General Data Protection Law (LGPD) is the creation of a national personal data protection authority. The mission of the new body will be to manage this agenda, and it will join up with other regulatory agencies that bear this responsibility within their respective sectors, such as the National Consumer Secretariat. A big challenge is to promote synergy between these regulatory bodies, and the role of the future national authority in coordinating the application and oversight of the LGPD with the other actors will be essential. Finally, there are organizations for the protection of diffuse and collective rights. In general, citizens lack ability on an individual level to efficiently protect their own rights. For this reason, nongovernmental organizations emerge to protect rights on behalf of groups, in addition to other bodies, such as the Public Defender's Office, the Public Prosecutor's Office and consumer protection bureaus. In the future, these bodies are increasingly likely to be involved with a personal data protection agenda.

Bruno Bioni
Independent consultant in personal data privacy and protection. Founder of Data Privacy Brazil.

Brazil already has sectoral personal data protection laws, such as the Consumer Protection Code, the Brazilian Civil Rights Framework for the Internet, the Credit Rating Law and the Access to Information Law. Through the creation of a general law, we will have a more complete regulatory system and a personal data protection legislation.

I.S.O._ In your opinion, what are the main points of the new LGPD?

B.B._Brazil already has sectoral personal data protection laws, such as the Consumer Protection Code, the Brazilian Civil Rights Framework for the Internet, the Credit Rating Law and the Access to Information Law. Through the creation of a general law, we will have a more complete regulatory system and a personal data protection legislation. The LGPD, in itself, is important because, unlike these other laws, it is designed to deal exclusively with personal data protection. As such, it lists ten principles that must guide any type of personal data processing. If these ten principles are not fulfilled, the personal data processing operation will be considered illegal.

There is now a broader set of legal bases for addressing personal data protection, which are authorizations and hypotheses established by the LGPD that legitimize data processing. This law is important because it goes much further than consent, which is the only legal basis in Brazilian sectoral laws. The LGPD adds another nine legal bases.

One in particular is legitimate interest, which can be used as a basis for organizations in situations where it is not possible to obtain consent, either because there is no point of contact with data subjects or because it would not be advisable to seek such authorization. This could occur, for example, in bank fraud prevention activities. It is within the legitimate interest of a bank to prevent fraud; at the same time, as the holder of a checking account, it is to my benefit and within my legitimate expectation that the financial institution will process my personal data without my consent to generate a behavioral profile that serves as a criterion for identifying possibly fraudulent financial transactions and, thereby, create a system that prevents fraud. This is a typical case of application of legitimate interest where there is greater flexibility for authorizing the processing of personal data.

Also worth noting is the relationship between the law and important compliance tools, promoting the existence of documents through which public and private sector organizations can demonstrate their compliance with the LGPD. Nowadays, the main tool is the personal data production impact report, which indicates the flow of data processed by the organization and points out the respective legal bases, as well as actions taken to comply with the law. It is important to view this compliance tool as a document through which organizations report on their compliance with the law, in relation to each of the ten principles of the LGPD. It is not enough for organizations to say they use personal data responsibly; they need to document this process so that, in the future, they can prove their compliance with the LGPD.

I.S.O._ What has the impact of the General Data Protection Regulation (GDPR)[6] been in Latin America?

B.B._ Overall – and this is not a prerogative of the GDPR – it has extraterritorial application, i.e., the law follows the data, regardless of where the person processing that data is located. For an organization in Latin America that wants to access the European market through the sale of products or services, if it involves processing personal data, the GDPR applies. This has a significant impact in Latin America and in Brazil's particular situation, since many local organizations interface, to or lesser or greater extent, with the EU market.
Another impact is with regard to the free flow of information, which is linked to how countries exchange personal data. This goes both ways, i.e., how Brazilian companies are able to bring data collected from people located in the European Union and how European companies can transfer data collected from people in Brazil. For this reason, it is referred to as bilateral movement. In most personal data protection laws – including the GDPR and LGPD – there is a free flow of information when one country recognizes that the other has an adequate level of personal data protection. In the future, something that will become a topic of much discussion is the convergence between the Brazilian and European regulations, so that this free exchange of data can occur. This is why personal data protection laws have a direct relationship with foreign trade agendas: In a situation where a number of products and services depend on processing and transferring personal data to enable global operations, these laws will have an important impact.

I.S.O._ In your opinion, are national laws sufficient to ensure the privacy and protection of personal data? Do other necessary mechanisms exist?

B.B._ The code of the law, in itself, does not guarantee actual compliance with the provisions. From the perspective of a toolbox for modulating behavior in society, law and legislation are just one of the tools. There are other possible tools, such as the market itself, since it shapes a number of social behaviors. A major change would be organizations viewing personal data privacy and protection as a competitive advantage and matter of reputation. Once there is a group of organizations that openly recognize that effective protection of their consumers' information is a strength, the market will become an instrument for molding behavior.
Social norms are another tool, i.e., how society itself curbs certain behaviors, regardless of the legislative branch and the market. This is linked to a cultural aspect: In countries or environments where a personal data protection culture

It is not enough for organizations to say they use personal data responsibly; they need to document this process so that, in the future, they can prove their compliance with the LGPD.

[6] The General Data Protection Regulation is a regulation in EU law on data protection and privacy applicable to all individual citizens of the European Union (EU) and European Economic Area (EEA). It also regulates the export of personal data outside the EU and EEA.

(...) the law is only one of the tools and, on its own, is not sufficient to ensure respect for personal data privacy and protection. It must be coordinated with economic interests, i.e., the market, cultural aspects, i.e., social norms, and technology. Then it will be possible to talk about efficient protection of personal data.

exists, society demands best data protection practices from the public sector – as a regulator or major stakeholder in processing data – as well as from the private sector.
Finally, there is the technology, i.e., how it can reinforce or neutralize our ability to control information that concerns us. A classic example is cryptography, which strengthens control over our data, especially by keeping secret the content of communications between senders and recipients, wherein can be found a significant amount of personal information. There are also technologies that work in the opposite direction, such as facial recognition, which enables not only identifying a certain person in a crowd, but also recognizing emotions and behavioral aspects through facial expressions. Therefore, the law is only one of the tools and, on its own, is not sufficient to ensure respect for personal data privacy and protection. It must be coordinated with economic interests , i.e., the market, cultural aspects, i.e., social norms, and technology. Then it will be possible to talk about efficient protection of personal data.

I.S.O._ There has been much discussion about the use of personal data by major companies such as Facebook and Google. In general terms, how does the private sector collect and use our data?

B.B._ The first point is that the LGPD and, in general, personal data protection rules, extend far beyond the ecosystem of the Internet, particularly when you consider organizations whose business models are based on the use of personal data for targeted advertising and content, among others. Traditional sectors of the economy, such as the automotive industry, health sector and electric power industry, are increasingly investing in the use of their consumers' data and target audience to optimize the provision of services and more accurately model products before launching them on the market. Therefore, in general terms, it can be said that a large part of the private sector collects and uses our personal data to be more competitive and efficient in its economic activities.
Something that appears to be a trend is recognition by the private sector that personal data protection is a value, especially in reputational terms. An issue addressed by the LGPD is the right to data portability, which permits owners, along with their data, to migrate to competing services. Within this possibility, a scenario is emerging where personal data protection is viewed as a competitive advantage, which is a big window of opportunity for the private sector to recognize the value of this message of protection and responsible use of data as a business strategy.

I.S.O._ And what is happening in the realm of Internet service providers?

B.B._ Most business models nowadays are based on behavioral advertising. Consumers or users of a service do not pay for it in cash, but "swap" their data so that this business model is monetized by the incorporation of behavioral advertising on social networks or search engines, for example. This is an ecosystem that is largely impacted by any personal data protection law. It will be no different in Brazil. From now on, we need to observe the behavior of these actors. In this scenario, as in the European Union, we have a role, as professional associations, to call on these actors to think about best practices so that the reputation of the sector is responsive to personal data protection rules. This means, for example, thinking about how technologies can generate interoperable standards within this multitude of players so that, once you've chosen what you want to be done or not to be done with your data, this decision is achievable and generates an auditable trail throughout the online media ecosystem. The big dilemma, specifically in the Internet realm, is that when you use these platforms, various actors are following, monitoring and collecting information about your habits in order to create a quite accurate behavioral profile of you. It is not coincidental that a certain ad follows you in the various environments you frequent on the Internet. Therefore, the question that arises is being able to develop technologies capable of scaling the ability of data subjects to have greater control and understanding of how their data is trafficked in these environments, and how it will come back to them, whether as targeted content or advertising.

Consumers or users of a service do not pay for it in cash, but "swap" their data so that this business model is monetized by the incorporation of behavioral advertising on social networks or search engines, for example.