Internet Sectoral Overview | Number 2 June, 2019 Year 11

Privacy and personal data

Protection of personal data: basis, concepts and application[1]

By Laura Schertel Mendes[2]

The collection, processing and use of immense amounts of personal information are indisputable aspects of contemporary society. The interest of the State and other private organizations in this type of information stems from the multiple benefits that can be obtained from processing data: targeted advertising, links with customers, and risk assessments. In relation to the digital environment, this situation is even more striking, since many Internet business models are based on the processing of personal data, enabling the financing of various services through the monetization of this data.

From the point of view of individuals, ubiquitous computing (Mattern, 2008) is made even more significant by the ways in which all realms of life are marked by the processing of personal data. This is due to the numerous electronic devices that are part of our day-to-day lives and continually store all kinds of personal information. Therefore, apart from the opportunities made possible by computerized and interconnected daily life – expansion of forms of personal and public communication, social mobilization, and circulation of knowledge, among others – risks emerge for individuals, such as increased monitoring and surveillance, discrimination, unwanted exposure, and formation of comprehensive personality profiles (Hartmann & Wimmer, 2011).

In this context, data protection legislation, i.e., the legal framework for individual protection in relation to the processing of personal data and information by third parties, is currently at the center of economic, social and political discussions around the world.

Intense data processing by the public and private sectors, beginning in the 1970s, led to the evolution of the right to privacy, including a dimension of personal data protection, particularly the control of individuals over the flow of their information in society. The creation of data protection rules, which are currently starting to be developed, rests on the principle of accountability. It is understood that the effectiveness of data protection not only results from expanding control by individuals, but also from making the entire chain of data processing agents accountable for information processing risks, since these agents have greater means to implement technical and organizational measures to protect the personal information of data subjects. Consequently, the most recent laws, particularly the European

[1] This text is initially based on a study carried out in the book *Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental* (Privacy, protection of personal data and consumer protection: general outlines of a new fundamental right) (Mendes, 2014) and seeks to update the data protection model proposed in the Brazilian General Personal Data Protection Law, approved in 2018 (Law No. 13709/2018).

[2] Professor in civil law at the University of Brasília (UnB) and professor in the master's degree program in constitutional law of the Brazilian Institute of Public Law (IDP). Holds a PhD in private law from the Humboldt University of Berlin.

Laura Schertel Mendes
University of Brasília (UnB) and Brazilian Institute of Public Law (IDP).

General Data Protection Regulation (GDPR), have started to include new mechanisms such as impact reports, codes of conduct, certifications and governance programs, in addition to standards that encourage implementation of the privacy by design concept (Bennett & Raab, 2018).

General Personal Data Protection Law in Brazil

Until the enactment of the General Personal Data Protection Law (LGPD) in 2018, Brazil did not have general regulations on this matter. Several sectoral laws[3] formed a "regulatory patchwork," which prompted much criticism, either due to the weak protection of personal data subjects, or for the legal uncertainty to which companies that had data processing as one of the pillars of their business were subjected.

Proponents from the Brazilian academic community (Mendes & Doneda, 2016; Bioni, 2014) and from different sectors (Manifesto, 2018) have long defended the creation of a general law, able to provide a coherent system of rules and minimum parameters for processing data in the country. Therefore, the approval of the LGPD can be viewed, in part, as the result of internal recognition of the national academic community and stakeholders. External factors also decisively contributed to the approval process of the law, such as the General Data Protection Regulation going into effect in Europe in 2018, and events related to the Cambridge Analytica company, regarding the use of Facebook data for microtargeting in the U.S. electoral campaign of 2016, in violation of data protection rules[4].

The enactment of the LGPD in Brazil instituted a general data protection system for the first time in the country, consolidating and complementing the regulatory framework of the information society. The Brazilian law inaugurates an *ex ante* data protection model, based on the idea that given the widespread automated processing of data in the information society, there is no longer data that is irrelevant. Since personal data is a form of representation of individuals in society, any processing of data can affect their person and, therefore, has the potential to violate their basic rights. This is why the legal protection of personal data within the framework of the LGPD takes place horizontally and is applied to all economic sectors, as well as the public sector.

Since the LGPD is based on a broad concept of personal data, in principle all data processing – done by both the public and private sectors – is subject to this law. Its scope of application also includes the Internet. Exceptions are justified on an individual basis, whether based on a fundamental right (for example, freedom of information, in the case of exceptions for journalistic activities) or for being relevant to the public interest (such as exceptions for public safety and national defense).

[3] Throughout the evolution of personal data protection rules in Brazil, various documents have addressed the topic, such as the Civil Code (Law No. 10406/2002), Credit Rating Law (Law No. 12414/2011), Access to Information Law (Law No. 12527/2011) and Brazilian Civil Rights Framework for the Internet (Law No. 12965/2014).

[4] The penalty applied by the Information Commissioner's Office of the United Kingdom to the parties involved can be found at: <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>

Another innovation in the law is the idea that data processing must be supported by a legal basis. These bases are varied, but examples include consent, performing a contract, the legal duties of controllers, processing by the public administration, and legitimate interest. These levels will be examined in detail below.

Conditions of legitimacy for personal data processing

One of the core assumptions of the LGPD is that data can only be processed if there is a regulatory basis authorizing it. Processing will only be legitimate if it fits within at least one of 11 hypotheses, such as consent of the data subject. For consent to be valid, it must be free, informed, clear and for a specific purpose.

Another relevant authorization hypothesis is personal data processing to fulfill an obligation established by law, regulation, or to perform a contract to which the data subject is a party, whether when processing is necessary for implementing a public policy or in the general exercise of responsibilities or powers conferred by law.

When personal information is essential for performing a contract, its collection or processing shall be authorized. For example, it is necessary for e-commerce companies to obtain the consumer's credit card information and address for payment and delivery of products, without which it is not possible to perform the purchase and sale agreement.

With regard to processing personal data in accordance with the legitimate interests of controllers or third parties, the balance between these interests and the rights of data subjects should always be considered. If carrying out a specific purpose with personal data processing has the potential to affect the fundamental rights and freedoms of a data subject, this legitimate interest would not be considered grounds for authorizing the data processing.

Assessing whether the conditions for processing data are legitimate should also consider whether the principles of the LGPD are being followed, such as free access, security, transparency and quality. The law seeks to address contemporary aspects of data protection and reflect new demands. Examples of this are the principle of no discrimination through personal data processing, which looks at the discriminatory potential of using data or automated decision-making mechanisms that use personal data, and the principle of prevention, which is the basis for developing privacy-related measures in design.

Another feature is the principle of purpose, which links the processing of personal data to the objectives that gave rise to and justified its collection. The application of this powerful principle endeavors to ensure contextual privacy and prevent data from being used afterwards for purposes that are incompatible with the original intent that initially permitted its collection. The LGPD also makes express reference to the principle of good faith, which is fundamentally important in personal data protection, primarily due to the mass nature of various data processing mechanisms and the opaqueness intrinsic to these operations. This principle broadly guides the relationships between data subjects and processors, whether duties such as transparency are already minimally outlined or need to be established.

For consent to be valid, it must be free, informed, clear and for a specific purpose.

(...) data subjects should have free access to their data; must be able to correct wrong and outdated data; and must be able to cancel data that has been improperly stored or where consent has been revoked.

Procedures to ensure personal data protection

Apart from legitimacy conditions, the LGPD contains a number of procedures aimed at providing greater security and strengthening the guarantees of data subjects.

The basic rights attributed to data subjects by various national laws and international treaties for controlling the flow of their data are known by the acronym "ARCO", short for: access, rectification, cancellation and opposition. In light of the control paradigm, it is understood that data subjects should have free access to their data; must be able to correct wrong and outdated data; and must be able to cancel data that has been improperly stored or where consent has been revoked . Other relevant rights are those attributed to data subjects in relation to decisions made solely on the basis of automated processing of personal data, such as those intended to define an individual's personal, professional, consumption and credit profile.

In this second stage of the model for application of the law, it is the responsibility of processors to observe, apart from the rights provided for in the LGPD, the obligations established for all those who process data. Among these is an obligation for controllers, not processors, to fulfill: hire a data processing officer. This officer will be responsible for receiving complaints from data subjects, communicating with the national supervisory authority, and guiding employees so that the organization complies with the data protection rules.

Another important obligation, until then not comprehensively covered in Brazil's legal system, is in reference to processors keeping records. "Article 37. The controller and processor shall maintain records of data processed by them, especially when based on a legitimate interest" (Law No. 13709/2018). The LGPD also establishes that controllers and processors are obligated to adopt technical and administrative security measures to protect data from unauthorized access, accidental or illegal destruction, loss, alteration and transmission, or any other form of inadequate processing.

The information security chapter is a fundamental pillar of the LGPD and introduces at least three important innovations to the Brazilian legal system in terms of the obligations of data processors. First, the law requires them to adopt measures that ensure the integrity, confidentiality and availability of the data being processed. Second, in the event of a security incident, such as leakage of data, the controller is required to notify the data protection authority, which can stipulate the adoption of mitigation measures or widespread disclosure to the public. Third, there is an obligation that fits within the concept of privacy by design, since such measures will need to be observed from the design stage to execution of the product or service.

Monitoring, application of sanctions and compensation

The third stage of the data protection model involves the liability of controllers or processors should damages occur as a result of personal data processing. In the LGPD, this liability is established in both civil and administrative terms.

The civil liability of controllers or processors first takes into account the nature of the data processing activity, which is limited by the LGPD to hypotheses that have a legal basis, encompass strictly necessary data, and are tailored and proportionate in relation to its purpose.

Given these limitations, together with the fact that the law, as a rule, assumes that data will be deleted once processed and that the risk intrinsic to the processing of personal data will be considered, the LGPD seeks to limit processing hypotheses to those that are useful and necessary, ensuring that even these can be subject to restriction if they constitute a risk to the rights and freedoms of data subjects.

One of the main principles of this regulation is to reduce the risk intrinsic to the processing of personal data in order to protect data subjects.

The law also has specifications as to the liability of certain agents. In the case of processors, they will only be liable for acts that violate the law, or the instructions provided by the controller; in the last situation, joint liability between the controller and processor will apply. In the other hypotheses, only the controller is liable.

With respect to administrative liability, the LGPD establishes a number of sanctions that, in case of violation of the law, should be applied by the national data protection authority. These sanctions range from a warning or a fine of up to 2% of the company's revenue in Brazil to a partial or total ban on performing activities related to personal data processing. As a parameter for determining sanctions, the law requires considering the adoption of internal mechanisms and procedures for safe and adequate processing of personal data, in addition to implementing best practices and governance policies, and corrective measures.

When applying the administrative sanctions of the LGPD, the supervisory authority should take into account the legal criteria that inform whether a particular processing of data is irregular. This is the case when the processing fails to comply with the law or does not provide the security expected by data subjects, considering any relevant circumstances: how the processing is done; expected outcome and risks; and data processing techniques available, among others.

Therefore, the third level of the data protection model interacts directly with the first two: In the case of noncompliance with the processing legitimacy conditions or personal data protection procedures, processors will be subject to administrative sanctions and payment of compensation to data subjects. The objective of this stage is to make the rules in the LGPD effective, whether through compensation for any moral or material damages caused by failure to comply with the law or through the application of administrative sanctions aimed at curbing the behavior prohibited by the law.

(...) in the case of noncompliance with the processing legitimacy conditions or personal data protection procedures, processors will be subject to administrative sanctions and payment of compensation to data subjects.

[5] The rights of data subjects are primarily established in Article 18 of the LGPD: "Article 18. The data subject has the right to obtain from the controller, in relation to the data processed by the controller, at any time and upon request: I -confirmation of the existence of the processing operation; II – access to the data; III – rectification of incomplete, inaccurate or outdated data; IV – anonymization, blockage or erasure of data that is unnecessary, excessive or not processed in compliance with the provisions of this Law; V – portability of data to other service providers or suppliers of product, upon express request, and observing business and industrial secrets, in accordance with the regulations of the supervisory authority; VI – erasure of personal data processed with the consent of the data subject, except in hypotheses under Article 16 of this Law; VII – information about public and private entities with which the controller shared data; VIII – information about the possibility of denying consent and the consequences of such denial; IX – revocation of consent under the provisions of § 5 of Article 8 of this Law". Available at: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>

On the one hand, the legal system for data protection is essential for guaranteeing the self-determination of citizens in relation to the flow of their information and to ensure legal certainty for companies and organizations that process personal data. However, it will not always be sufficient to prevent violations being committed by lawmakers themselves.

Next steps: constitutional protection and institutional strengthening

The General Personal Data Protection Law is a major step forward in building a personal data protection system in Brazil, an essential step in strengthening the trust of citizens in the services offered in the information society and encouraging constant innovation in these services. However, it is also crucial to fortify the constitutional protection of personal data in the Brazilian legal system.

On the one hand, the legal system for data protection is essential for guaranteeing the self-determination of citizens in relation to the flow of their information and to ensure legal certainty for companies and organizations that process personal data. However, it will not always be sufficient to prevent violations being committed by lawmakers themselves. The LGPD is not able to protect citizens from other laws that may be passed by the legislative branch of government that violate their privacy, by allowing, for example, processing of abusive data, legitimization of surveillance practices, or discrimination produced through the processing of personal data. Imagine, for example, a law that authorizes the use of racial data as input for an algorithm created to identify tax debtors, or one that legitimizes unrestricted surveillance of the population by the government without any justification. In such situations, the mere existence of a General Personal Data Protection Law and a national supervisory authority would not be sufficient to safeguard the rights of citizens.

In this context, the Brazilian Constitution has two important mechanisms for protecting citizens against improper processing of personal data: the material right to the protection of personal data, and the instrumental guarantee of this right, linked to *habeas data* action. Based on these experiences and institutional experience related to data protection in Brazil, it is now possible to recognize a fundamental right to personal data protection – so-called informative self-determination – as a material dimension of *habeas data* supported by the inviolability of intimacy, private life and human dignity, under the terms of the Constitution.

Apart from strengthening the constitutional protection of personal data, effective implementation of the General Personal Data Protection Law will depend on the creation of a personal data protection authority bolstered by the support of three elements: sanctioning power, expertise, and autonomy. Without building this regulatory architecture, it will not be possible to achieve the primary objective of the law, which is to strengthen society's trust in information and communication infrastructure and, consequently, ensure rights, expand innovation and enable more competitiveness among the services that use personal data in a legitimate and transparent way.

In recent decades, it has been clearly shown that the existence of administrative personal data protection bodies is essential for implementing the law and the culture of privacy in Brazil. In the words of Bennett and Raab (2006): "The existence of vigorous supervisory authorities has been regarded as a *sine qua non* of good privacy protection inasmuch as laws are not self-implementing and the culture of privacy cannot securely establish itself without an authoritative champion."

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.

Interview II

Joana Varon
Executive Director of Coding Rights.

I.S.O._ Why is it important to protect personal data? Why might it be problematic that a third party has a history of my purchases, medical information, sexual orientation or religion?

J.V._ Data protection means being able to choose who has access to our information and under what circumstances, i.e., deciding what to share and knowing how the data is being used by companies, governments and other organizations. This control is important for ensuring rights, not only of privacy, but also of freedom of expression, development of our person, and even equality and for fighting discrimination. This is because, as personal data is gradually used to feed decision-making processes, whether automatically (through algorithms) or manually, transparency and control of our data become more important, so as to know whether we are being discriminated against through profiling practices, done on the basis of information that is available about us.
For example, when you provide your Individual Taxpayer Registration Number to obtain discounts at drug stores, the list of medications associated with this data may contain sensitive information about your health. It is possible that this information will be used in a discriminatory way by health insurance companies, changing the deductible amount according to the profile. In like manner, our online shopping history says a lot about our purchasing power and personal preferences. Through this information, it is possible to target advertising that is compatible with our tastes, tempting us to buy something we don't need, as well as allowing for charging higher prices or limiting access to credit for certain profiles. Data about sexual orientation, in a society that still has a bias against diversity, can also be used for purposes of segregation, for example, restricting job opportunities. In the project <http://chupadados.com>, we present stories about everyday uses of our personal data and some of the implications this has in our lives.

I.S.O._ What does it mean to "accept the terms of use" of an application or website? By doing so, what are we consenting to? What are the rights of users?

J.V._ Every term of use or privacy policy has different implications. An application can be more or less careful in how it handles data and, consequently, privacy and security. The problem is that most of the time we just click on the "Accept" button, without reading the content, and also because it was not designed in a way to facilitate reading it. We end up consenting to something without even knowing what it is. If the person responsible for developing the application is not at all concerned about our privacy or whether use of the data is part of the business model, it is very likely that the data will be shared with third parties or used for profiling.

I.S.O._ How can our personal data be used to "feed algorithms? What are the implications of this?

J.V._ Algorithms are increasingly being used in our day-to-day activities, in countless opportunities when we transfer decision-making processes to computers. They decide what to show when we do a Google search or whether the next post on our social network timeline will be an airline or baby clothing ad. They indicate whether your finger is really yours in the biometric recognition system of the bank or, in some controversial facial recognition tests conducted during this year's Brazilian Carnival festivities, whether a person passing in front of a camera is someone in the police's database. Soon, they will replace us in the driving of vehicles.

Algorithms are nothing more than a sequence of programmed steps for performing a task. The examples above illustrate algorithms that optimize data analyses for making decisions. The problem is that the decisions are not always optimal. Depending on how the algorithms are programmed, the databases organized, and the steps of the process assessed, the outcomes may reinforce asymmetries, prejudices and inequalities. The book *Algorithms of Oppression*, by Safiya Umoja Noble, demonstrates how search engines strengthen racist and macho practices, suggesting pejorative terms as an automatic supplement to the searches entered. The same thing happens with facial recognition technologies, which tend to signal false positives for women's faces, especially black women[7]. This occurs because the people who design these algorithms replicate the predominant power structures in society.

I.S.O._ What can we do to use social media, applications and service platforms and, at the same time, protect our personal data?

J.V._ The first step is to be aware that these technologies work by processing our data, often making money from it. We can opt for applications and services that, among other aspects, feature privacy and security as values of the product offered; ensure protections, such as the use of cryptography; promote minimization of the information collected and stored over time; do not share data with third parties, unless legally ordered to do so; are open source; and do not require authentications with a real name or another form of identification.

In the case of social networks and other services not guided by these concerns, but which we nonetheless need to use, it is advisable to engage in identity management, i.e., assess what type of personal data we want to associate with each of our profiles. It is also recommended that we check the privacy settings and adjust them to minimize data collection and storage. At the same time, it is also increasingly suggested that we ensure autonomous ways to manage personal data – for example, have the content in other locations, not only in social networks.

Depending on how the algorithms are programmed, the databases organized, and the steps of the process assessed, the outcomes may reinforce asymmetries, prejudices and inequalities.

[7] In a public hearing in the Chamber of Deputies on April 3, 2019, critical studies on the use of these technologies for public security were listed. To learn more, go to <https://medium.com/codingrights/bem-na-sua-cara-a-ilus%C3%A3o-do-reconhecimento-facial-para-seguran%C3%A7a-p%C3%Bablica-47c708b34820>.

When a product considers "privacy by default", it is released with the most protective privacy settings as the default, i.e., you have to choose to have your data saved or stored, which is the opposite of the current logic.

I.S.O._ What do the concepts "privacy by design" and "privacy by default" mean? How can developers adopt these principles to develop applications that protect user privacy?

J.V._ Since the predominant logic underlying the development of many technologies today, mainly (but not only) for the Web, is the logic of data capitalism, most products and services, as a rule, have settings that enable massive data collection and storage. When a product considers privacy by default, it is released with the most protective privacy settings as the default, i.e., you have to choose to have your data saved or stored, which is the opposite of the current logic. Privacy by design is an even broader concept, which means that products and services take into account privacy concerns from the moment they start being developed. This is the case for services developed by collectives and groups that follow what was previously called cypherpunk logic, which emphasizes strong cryptography and protection of privacy. Examples are Signal, a messaging application that is an alternative to highly invasive products such as WhatsApp, and Tor, which is a browser that respects user anonymity.

I.S.O._ What techniques are recommended to keep personal data protected?

J.V._ There is no single recipe – it depends on who we are and what, when, where and with whom we are communicating. There are different means of protecting both our communication and personal data. In general, the techniques are associated with practices that focus on data protection (for example, the use of cryptography), minimization of the amount of data collected or stored, and identity management (i.e., the act of separating our different profiles among various online identities).
On the other hand, there are situations where we have no choice, since our data is required, for example, to access public services. In all cases involving the management of our data, we may use transparency tools to learn what is being done with the information, such as *habeas data*, and occasionally demand corrections or even compensation for misuse. It is essential that the General Personal Data Protection Law (LGPD) also go into effect with a provision for a data protection authority to inspect practices in both the public and private sectors.

Domain Report

The dynamics of the registration of domains in Brazil and the world

The Regional Center for Studies on the Development of the Information Society (Cetic.br) carries out monthly monitoring of the number of domain names registered in the 16 largest country code Top-Level Domains (ccTLDs) in the world. Combined, they exceed 101.3 million registrations.

In May 2019, the domains registered under .tk (Tokelau) reached 23.7 million, followed by Germany (.de), China (.cn) and the United Kingdom (.uk), with 16.2 million, 11.7 million and 9.7 million records, respectively[8]. Brazil continues to occupy the seventh place on the list, with 4 million registrations under .br. With 1.9 million registrations, Spain (.es) ranked 16th, as can be seen in Table 1.

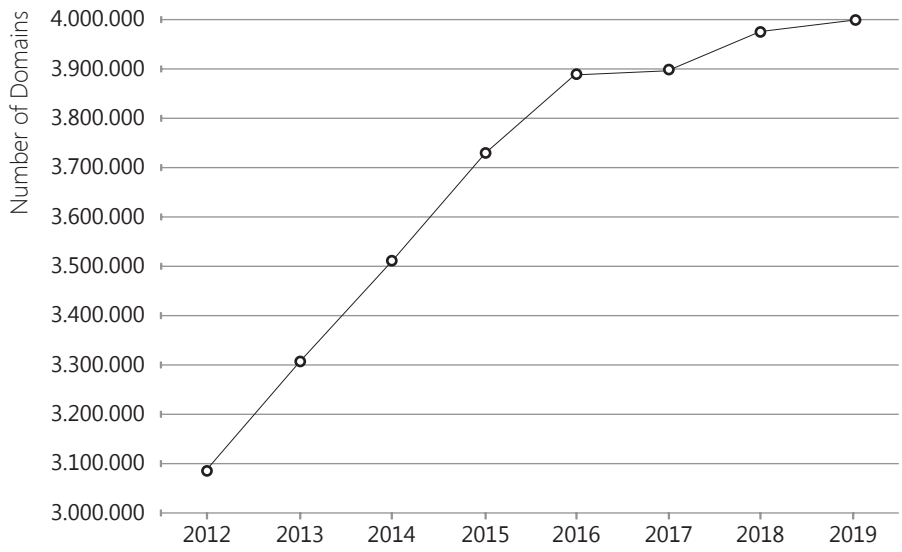
Table 1 – REGISTRATION OF DOMAIN NAMES IN THE WORLD – MAY 2019

Position	ccTLD	Domains	Ref.	Source
1	Tokelau (.tk)	23.704.267	May-19	research.domaintools.com/statistics/tld-counts
2	Germany (.de)	16.224.416	May-19	www.denic.de
3	China (.cn)	11.719.947	May-19	research.domaintools.com/statistics/tld-counts
4	United Kingdom (.uk)	9.778.572	May-19	www.nominet.uk/uk-register-statistics-2018
5	Netherlands (.nl)	5.852.144	May-19	www.sidn.nl
6	Russia (.ru)	5.014.569	May-19	www.cctld.ru
7	**Brazil (.br)**	**4.040.132**	**May-19**	**registro.br/estatisticas.html**
8	European Union (.eu)	3.582.957	May-19	research.domaintools.com/statistics/tld-counts
9	France (.fr)	3.377.847	May-19	www.afnic.fr/en/resources/statistics/detailed-data-on-domain-names
10	Italy (.it)	3.197.556	May-19	www.nic.it
11	Australia (.au)	3.187.548	May-19	www.auda.org.au
12	Canada (.ca)	2.831.137	May-19	www.cira.ca
13	Poland (.pl)	2.616.373	May-19	www.dns.pl/english/zonestats.html
14	Switzerland (.ch)	2.215.837	Apr-19	www.nic.ch/reg/cm/wcm-page/statistics/index.html?lid=em*
15	United States (.us)	2.054.778	May-19	research.domaintools.com/statistics/tld-counts
16	Spain (.es)	1.926.092	May-19	www.dominios.es

[8] It is important to note that variations exist among ccTLD reference periods, although it is always the most updated one for each country that is used.

Graph 1 shows the performance of .br since 2012.

Graph 1 – TOTAL NUMBER OF DOMAIN REGISTRATIONS PER YEAR FOR .BR – 2012 TO 2019*



** Data in reference to May 2019.*
Source: Registro.br

In May 2019, the five generic Top-Level Domains (gTLD) totaled more than 172 million registrations. With 141.6 million registrations, the .com ranked first, as shown in Table 2.

Table 2 – MAIN GTLDS – MAY 2019

Position	gTLD	Domains
1	.com	141.602.087
2	.net	13.561.131
3	.org	10.199.035
4	.info	4.740.206
5	.biz	2.033.621

Source: DomainTools.com.
Retrieved from: research.domaintools.com/statistics/tld-counts

WHAT DO YOU KNOW ABOUT METADATA?

IN A LETTER

The information on the envelope is metadata. What goes inside it is content.

IN A PHONE CALL

The time of the call, its length, the geolocation of the devices and the number of participants are examples of metadata. The content is what is talked about.

VISITING A WEBSITE

Metadata include your IP address, the time the website was accessed, the length of the visit, the characteristics of the equipment, and where you are connecting from.
The content is what appears on the screen.

When a lot of metadata is collected about people, their patterns of behavior start to emerge. It is possible to find out where they live, who they meet and what their interests and opinions are, without needing to access the content of their communications.

Source: Adapted from Viera, C. (2017). Retrieved from <https://www.derechosdigitales.org/tipo_publicacion/infografias/>.

WHAT INFORMATION DOES METADATA PROVIDE ABOUT YOU?

Metadata is a set of information that describes specific content.

Source: Adapted from Garay, V. (2015). Retrieved from <https://www.derechosdigitales.org/publicaciones/que-informacion-entregan-los-metadatos-sobre-ti/>.

/Credits

TEXT
MAIN ARTICLE
Laura Mendes (UnB/IDP)
DOMAIN REPORT
José Márcio Martins Júnior (Cetic.br)

EDITORIAL COORDINATION
Alexandre Barbosa
(Cetic.br)
Tatiana Jereissati
(Cetic.br)
Stefania L. Cantoni
(Cetic.br)

ACKNOWLEDGMENTS
Laura Mendes
(UnB/IDP)
Bruno Bioni
(Data Privacy Brasil)
Joana Varon
(Coding Rights)

REVIEW IN PORTUGUESE
Mariana Tavares

TRANSLATION INTO ENGLISH
Grant Borowik, Lorna Simons, Luana Guedes, Luisa Caliri
(Prioridade Ltda.)

GRAPHIC DESIGN AND LAYOUT
Comunicação NIC.br

PUBLISHING OF ENGLISH EDITION
Grappa Marketing Editorial

The Internet Sectoral Overview is also available in Portuguese at cetic.br/publicacoes/indice/panoramas/

STRIVING FOR A BETTER INTERNET IN BRAZIL

CGI.BR, MODEL OF MULTISTAKEHOLDER GOVERNANCE

www.cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK