The fundamental right of confidentiality and integrity of IT systems in Germany: a call for “IT Privacy” right in Brazil?

Cecília Alberton Coutinho Silva

Received: 31 July 2021 / Accepted: 12 September 2021 / Published online: 13 October 2021
© Springer Fachmedien Wiesbaden GmbH 2021

Abstract The fundamental right to confidentiality and integrity of IT systems was recognized by the *Bundesverfassungsgericht* (BVerfG) in Germany and responds to the growing need to recognize new rights that are able to properly protect the individual as new technologies continue to develop. In the said scenario, this paper will seek to answer the question: Starting from the premises set by the BVerfG in the ruling rendered on February 27th, 2008, are there similar grounds to sustain the existence of an IT Privacy right in Brazil, regarding the Brazilian juridical scenario, mainly as to data protection? To that end, the paper is divided into four main parts to: (i) assess the fundamentals of the decision rendered by the BVerfG in the case mentioned; (ii) present the privacy and data protection legal scenario in Brazil; (iii) point out how information security is provided for in Brazilian legislation; and (iv) validate whether the premises adopted by the BVerfG are also coherent in Brazil, considering the legal landscape presented. The research is based on a hypothetical-deductive method, through inquiry and bibliographic analysis, grounded both in Brazilian and European doctrine. Lastly, the research concludes in the sense that the Brazilian and German Constitutional Legal Orders are different, not only relating to the way in which new fundamental rights are acknowledged, but also in regard to the privacy and data protection legal culture, which directly impacts the feasibility of a fundamental right to confidentiality and integrity of IT systems.

Keywords Information technology · Fundamental right · Cybersecurity · Data privacy · Brazil

Cecília Alberton Coutinho Silva (✉)

Faculty of Law, Pontifical Catholic University of Rio Grande do Sul (PUCRS), Porto Alegre, Rio Grande do Sul, Brazil

E-Mail: coutinhocecilia1@gmail.com

1 Introduction

New technologies have been shaping the last and the current century more strongly than any other time before¹ [14, p. 15]. With that, data can be made instantly available anywhere, anytime, and by anyone as it can be sent to any part of the globe over computer networks at virtually no cost, excluding the costs stemming from building and using networks [3, p. 58].

And it is not just technology itself that, through devices that increase individual and collective intelligence, such as algorithms, big data, artificial intelligence, and cloud computing, potentialize the processing of personal data and, at the same time, impact the individuals' rights as data subjects. Information technology systems also provide an image that accurately reflects the personal interests and inclinations, the economic situation, as well as the physical and psychological state and behavior of their users. With that, those who gain access to the information technology system may, in a sense, have access to the “externalized brain” or even the “externalized psyche” and to much other important information about the affected personality [8, p. 337], as is the case for a broad personality profile of the person in question, for instance.

In this context, as of February 27th, 2008, the German Federal Constitutional Court (*Bundesverfassungsgericht* or BVerfG) has annulled provisions of the North-Rhine Westphalian Act on the Protection of the Constitution, giving rise to a new fundamental right (*Grundrecht*), thereafter known as the right to confidentiality and integrity of IT systems (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*) or, in short, the “IT Privacy” right (*IT-Grundrecht*, *Computer-Grundrecht* or *Grundrecht auf digitale Intimsphäre*).

The North-Rhine Westphalian Act provisions allowed the government to conduct online surveillance of personal computers, which, according to the BVerfG, were unconstitutional due to the fact that they did not sufficiently respect the individual's right to confidentiality of data stored on information technology systems and the integrity of information technology systems themselves. The ruling by the BVerfG represents the empowerment of the fundamental rights guaranteed under the German Fundamental Law (*Grundgesetz* or GG) and became one of the most important decisions rendered by the Court related to data protection.

That said, this brief paper aims to answer the following question: Starting from the premises set by the BVerfG in the ruling rendered on February 27th, 2008, are there similar grounds to sustain the existence of an IT Privacy right in Brazil, regarding the Brazilian juridical scenario, mainly in terms of data protection? To this end, the paper is divided into four main parts to: (i) assess the fundamentals of the decision rendered by BVerfG in the case mentioned; (ii) present the privacy and data protection legal scenario in Brazil; (iii) point out how information security

¹ “Some of the most salient examples of innovation are information and communication technologies, biotechnology or new materials. Though technologies are often relevant in their transformed shape of an ‘end-product,’ opening up new opportunities for customers by using new gadgets, technological innovation in its fundamental outfit can be understood as a significant shift in production techniques that triggers economic productivity” [14, p. 15].

is provided for in the Brazilian legislation; and (iv) validate whether the premises adopted by BVerfG are also coherent in Brazil, considering the legal landscape presented. To properly develop those topics, the research is based on a hypothetical-deductive method, through inquiry and bibliographic analysis, grounded both in Brazilian and European doctrine.

Lastly, the research concludes in the sense that the Brazilian and German Constitutional Legal Orders are different, not only relating to the way in which new fundamental rights are acknowledged, but also in regard to the privacy and data protection legal culture, which directly impacts the feasibility of a fundamental right to confidentiality and integrity of IT systems.

2 The rise of the fundamental right of confidentiality and integrity of IT systems

The culmination of the recognition of data protection in Germany occurred with the decision of the Federal Constitutional Court on the issue of the population census that was carried out in Germany in 1983 (*Volkszählungsurteil*). This decision established the fundamental right to informational self-determination (*Grundrecht auf informationelle Selbstbestimmung*) and was a milestone in the development of data protection laws around the world.

Following said trend, on February 27th, 2008, the German Federal Constitutional Court (*Bundesverfassungsgericht*) annulled provisions of the North-Rhine Westphalian Act on the Protection of the Constitution (NRW-VSG), which allowed the government to conduct online surveillance and secret investigations of personal computers of people that have allegedly committed criminal offenses (*Online-Durchsuchung*) and also to monitor all the online behaviors of suspected individuals in the internet, giving rise to a new fundamental right, in a way, decurrent of the mentioned informational self-determination right, the fundamental right to guarantee the confidentiality and integrity of technical and informational systems (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), which were exemplified by the BVerfG as being “*Personalcomputer*”, “*Telekommunikationsgeräte*” or “*elektronische Geräte, die in Wohnungen oder Kraftfahrzeugen enthalten sind*”² [10, p. 365].

The provisions of the NRW-VSG allowed certain public authorities comparatively comprehensive rights to use “spyware” to, among other activities, oversee emails, secretly access an individual’s information technology system, search data stored on those systems, and monitor online communications, including computers’ hard disk data, in order to protect the State’s constitutional order in the face of growing rates of criminality, notably organized crime and terrorism. However, the provisions only drew attention from the moment when the Minister of State, Wolfgang Schäuble [13, p. 117], decided to propose, at the federal level, the adoption of the same provisions

² Free translation: “Personal computers,” “Telecommunication devices,” or “Electronic devices present at home or in automobiles.”

of the North-Rhine Westphalian law that authorized remote monitoring of suspects' computers.

Thus, the Court ruled that the provisions of the NRW-VSG were unconstitutional, because they did not sufficiently respect the *individual's right to confidentiality of data stored on information technology systems and the integrity of information technology systems themselves*. In other words, the Court understood that unjustified online surveillance violated the right to a "guarantee of confidentiality and integrity of information technology systems," which was considered to be part of the fundamental right to privacy and to the free development of the personality as protected by Articles 1³ and 2⁴ of the German Fundamental Law (German constitution, *Grundgesetz* or "GG").

According to the BVerfG, the need to establish a fundamental right regarding computers was justified, because telecommunications secrecy, the right to inviolability of the home, and previous rulings of the Court no longer guaranteed computer users sufficient protection against state intervention, namely, surveillance. As a result, the fundamental right shall apply not only to personal computers, but also to laptops, business computers, cell phones, and electronic diaries.

So, the fundamental right to confidentiality and of integrity of IT systems rises as a reflex of the fundamental right to informational self-determination, which, in itself, integrates the *general right to personality* [12, p. 84]. The German general personality right (*das Allgemeine Persönlichkeitsrecht*) has been developed by the BVerfG since the 1950s and is derived from the combination of art. 1 par. 1 (dignity of the person) and art. 2 par. 1 (general freedom of action) of the *Grundgesetz*. With that, the combination of the mentioned provisions guarantees everyone the possibility to develop their own personality; in other words, instead of guaranteeing merely the protection of image or intimacy, the general personality reaches matters related to autonomy and self-determination [5, p. 220], which are of the utmost importance when dealing with privacy and data protection rights.

Yet, as exempted by the BVerfG, the fundamental right to guarantee the confidentiality and integrity of technical and informational systems is not absolute, which means that computer spying, the invasion of computers and servers to extract information, shall be allowed only when: (i) specific legislation is published to regulate the requirements for restricting the fundamental right's scope of application, compliant to the principle of legal reserve, which requires the issuance of a special law for the right to be restricted, and (ii) the legal text is sufficiently clear, precise, and proportional to the end that it aims to achieve, also encompassing the characteristics of adequacy (*Geeignetheit*), necessity (*Erforderlichkeit*), and proportionality in

³ Art 1 (1) *Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.* (2) *Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.* (3) *Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.*

⁴ Art 2 (1) *Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.* (2) *Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.*

the strict sense (*Verhältnismäßigkeit im engeren Sinne*). In this context, intervention would be permitted in cases of concrete danger to assets protected by law, as it is the case, for instance, to monitor the planning of terrorist acts, provided there is a court order in that sense, or for preventive purposes as well as criminal investigation and/or prosecution.

Then, the fundamental right at hand fills one of the most important gaps not covered by the right to informational self-determination⁵. As a result, the right to guarantee the reliability and integrity of technical and informational systems is intended to protect the system as a whole (and, therefore, the confidence in its use) and the personal data in a broad sense, which is the reason why, according to the BVerfG, informational self-determination goes beyond the protection of privacy: “*the informational self-determination protects data individually considered, or even a set of data, while the fundamental right to guarantee the confidentiality and integrity of technical-informational systems protects the system itself and the data apprehended in its broadest sense*” [16, p. 798]; BVerfG Ruling of February 27th, [4, p. 200].

Nonetheless, the fundamental right of IT Privacy was not broadly accepted without any controversy, because a part of the German doctrine understood that, although virtual searches can involve a large amount of personal and sensitive data, this would not change in any way the object of the protection of informational self-determination, as ruled by the BVerfG in 1983, which also protects the legal assets involved in virtual searches, as it encompasses protection of the collection, storage, use, and provision of personal data [6, pp. 521–523]. Thus, Eifert sustains that the privacy and integrity of technical informational systems should not be applied parallel/successively with informational self-determination, but as its subspecies [6, pp. 521–523].

In the same sense, Thomas Hoeren defends that “confidential” and “integrity” are characteristics—or virtues—related to people, and not to computer systems, which would make it impossible to recognize the right to confidentiality and integrity of technical and informational systems. In this sense, the author mentions that “*Ein ‘System’ kann nicht vertraulich und integer sein. Vertraulichkeit und Integrität sind personelle Tugenden. Geschützt sein kann nur die Vertraulichkeit der von dem System verarbeiteten Daten sowie die Integritätserwartung der Betroffenen, was die Sicherheit des Systems angeht*”⁶ [10, p. 365]. Adding to that, Hoeren ascertains that the object of protection of the “new” right could be derived both from the German Data

⁵ Informational self-determination gives individuals the power to decide for themselves about the disclosure and use of their personal data. In this sense, in the “*Volkszählungsurteil*” case, it was stated that “*he who, with sufficient security, cannot glimpse what personal information related to him exists in certain areas of his social environment, and he who cannot estimate to a certain extent what knowledge a possible interlocutor has of his person, may have his freedom considerably restricted*.” In other words, as a right of defense (right to non-arbitrary intervention), the right to informational self-determination consists of an individual right of decision, whose object (of the decision) is data and information related to a particular person/individual [22, p. 31].

⁶ Free translation: “A ‘system’ cannot be confidential and with integrity. Confidentiality and integrity are personal virtues. Only the confidentiality of the data prepared by the system as well as the maintenance of the integrity of those affected with regard to the security of the system can be protected.”

Protection Law (*Bundesdatenschutzgesetz*) and from the right to informational self-determination (*Recht auf informationelle Selbstbestimmung*) [10, p. 365].

Notwithstanding the criticism and the fact that the arguments referred to here may be valid, it must be conceded that the proclamation of the fundamental right to guarantee the confidentiality and integrity of technical informational systems marks the entry of the German constitutional law into the “*Online Age*”, as the BVerfG strengthened the individual’s rights by expanding and adapting traditional “offline” fundamental rights to accommodate new emerging technologies and technical means, and represents a considerable advance in the search for the protection of the rights of the personality, and, consequently, in the reaffirmation of fundamental rights [16, p. 806]. In that sense, it shall be highlighted that technical informational systems have acquired a growing importance in people’s daily lives and, thus, by assigning those systems the status of a fundamental right, said guarantee shall only exceptionally be relativized [11, p. 306].

Unlike the *Volkszählungsurteil*, which was ruled upon in a scenario of fears of State control or surveillance over the individual, the most recent decision is taken in a reality where not only the State is the focus of concern, but also private entities. This is because, in the modern information society, individuals are increasingly exposed to business models, equipment, and computer programs that, at all times, collect data and information related to their personality [16, p. 795].

Therefore, the fundamental right to guarantee the confidentiality and integrity of technical informational systems updates the protection of the personality in line with the technological reality of the 21st century, and the decision of the Federal Constitutional Court of Germany draws attention to the importance that the use of computer systems has recently acquired for the development of an individual’s personality, something that was previously unpredictable. As a considerable portion of the population gains access to computers and these begin to play a prominent role in their daily lives, which goes way beyond the mere use of social media, for instance (which, alone, is likely to grow to 3.29 billion users⁷ in 2022), new possibilities open up, but at the same time, new risks to the individuals’ personality compete with these possibilities.

In sum, computer systems are not protected by the fundamental right recognized by the German Court *per se*⁸, but only insofar as their confidentiality and integrity imply relevance to the personality [8, p. 364]. However, the question that arises—and forms the object of analysis of the present paper—is whether such a right could also be recognized in Brazil, considering the country’s legislation. To that end, it is relevant to, *first*, present the current Brazilian legal framework regarding privacy and data protection (as per item 3, below), *second*, refer to how information security

⁷ “Social media is used by billions of people around the world and has fast become one of the defining technologies of our time. Facebook, for example, reported having 2.38 billion monthly active users and 1.56 billion daily active users as of March 31, 2019 (Facebook 2019). Globally, the total number of social media users is estimated to grow to 3.29 billion users in 2022, which will be 42.3% of the world’s population [7]” [2].

⁸ In this regard, however, there is additional protection by other fundamental rights, such as art. 12 and 14 of the GG. However, it is still necessary to develop a concept of property protection based on information technology systems.

is provided for in the country (as per item 4, below), and, *third*, to consider whether there is an “IT Privacy” right in Brazil (as per item 5, below).

3 Privacy and data protection regulations in Brazil

The Brazilian Federal Constitution protects privacy rights in articles 5, X and XII⁹, stating that they are fundamental rights of any individual, but does not expressly mention an autonomous data protection right. In spite of that, the Brazilian doctrine already considers data protection¹⁰ as being an implicitly positive fundamental right¹¹ [15, p. 36, 19, 22, p. 290].

Adding to that, in May 2020, in a historic judgment on Action of Unconstitutionality No. 6,387, regarding the Provisional Measure No. 954, which authorized telephone companies to share personal data with the Brazilian Institute of Geography and Statistics (“IBGE,” in Portuguese), the Brazilian Supreme Court (“STF,” in Portuguese), by a majority, recognized data protection as a fundamental and autonomous right, which represents an important landmark in the privacy and data protection culture in Brazil. In the same sense, the Proposal for Constitutional Amendment No. 17/2019, which was recently approved by the Brazilian National Congress and whose main goals are to include (i) item XII-A in art. 5 of the Brazilian Federal Constitution, is turning data protection into positive law; and (ii) item XXX in art. 22 of the Brazilian Federal Constitution, to establish the exclusive competence of the Union to legislate and oversee compliance on the matter.

The Brazilian Constitutional scenario, thus, is continuously evolving and moving towards a very positive future as to the recognition of data protection as a fundamental right stemming from informational self-determination. With no exemption, privacy and data protection in Brazil are also provided for in other laws and regulations, which follow the general protection of the private life of the individual

⁹ Article 5. All are equal before the law, without distinction of any kind, guaranteeing Brazilians and foreigners residing in the country the inviolability of the right to life, freedom, equality, security, and property, in the following terms: (...) X—intimacy, private life, honor and people’s image are inviolable, the right to compensation for material or moral damage resulting from their violation being ensured; (...) XII—the secrecy of correspondence and telegraphic communications, data, and telephone communications is inviolable, except, in the latter case, by court order, in the hypotheses and in the form that the law establishes for the purposes of criminal investigation or criminal procedural instruction.

¹⁰ “(...) a proteção aos dados decorre da inviolabilidade da intimidade e da vida privada (art. 5º, X). Mesmo sem uma previsão expressa, “é possível extrair-se da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais (...)” [15, p. 290]. Free translation: “data protection stems from the inviolability of intimacy and private life” (art. 5, X). Even without an express provision, “it is possible to extract from the Federal Constitution a real fundamental right to the protection of personal data.”

¹¹ “Ainda sobre o tópico, importa registrar que aquilo que para muitos pode ser considerado um direito fundamental fundado na legislação infraconstitucional em verdade nada mais é—cuidando-se, convém frisar, de direitos fundamentais—do que a explicitação, mediante ato legislativo, de direitos implícitos ou mesmo decorrentes do regime e dos princípios, desde logo originariamente fundados na Constituição” [21, p. 147]. Free translation: “Still on the topic, it is important to note that what for many may be considered a fundamental right based on infra-constitutional legislation is actually nothing more—as regards fundamental rights—than the acknowledgement, through a legislative act, of rights implicit or even arising from the regime and principles, originally based on the Constitution.”

as a fundamental right foreseen in the Brazilian Constitution, as is the case in the following examples.

The *Brazilian Civil Code* (Law No. 10,406/2002) provides that “*the private life of the natural person is inviolable, and the judge, at the request of the interested party, will adopt as mandatory measures to prevent or terminate an act contrary to this rule*” and states that the private life of the natural person is inviolable as an inherent personality right (as per art. 21). In the same sense, the *Brazilian Consumer Defense Code* (Law No. 8078/1990) dedicates Section VI to disciplining the protection of consumers’ data, guaranteeing that consumers must have full access to their information (as per art. 43).

Beyond that, the *Telecommunications Act* (Law No. 9,472/1997) regulates consumers’ rights to privacy in relation to telecommunications services¹², the *Bank Secrecy Act* (Complementary Law No. 105/2001) ensures the confidentiality of financial data, allowing disclosure only upon a judicial order issued for the purposes of conducting or investigating illegal acts, and the *Information Access Act* (Law No. 12,527/2011) governs the use and processing of data by the Public Administration and establishes rules and procedures by which individuals may request details of the information collected by the public administration.

The *Internet Act* (Law No. 12,965/2014) and Decree No. 8,771/2016 regulate the processing of personal data collected through the internet by internet and connection services providers and, to that end, regard personal data protection as a principle (as per art. 3, III¹³), determine that users have the right to obtain clear and complete information on the connection register and access register (as per art. 7, VI¹⁴), and establish general guidelines on the processing of personal data (as per art. 7, VIII); also, the *Internet Act* provides for the access to registration data by police authorities, which is also the object of the *Money Laundering Law* (Law No. 9,613/1998), the *Law on Criminal Organizations* (Law No. 12,850/2013), and of the *Brazilian Code of Criminal Procedure*.

¹² The Fixed Switched Telephone Service Regulation (Resolution No. 426/2005) of the National Telecommunications Agency (“ANATEL”) requires, in art. 22, that “all data referring to provision of services, including phone records,” shall be retained by fixed telephone service providers (such as Vivo and NET) “for a minimum of five years” without a precise description of which data is included, or by whom it may be used and for which purposes. There are no specific security rules regarding the storage of this data: art. 23 only establishes the rule that it is the providers’ responsibility to protect the confidentiality of the data.

¹³ Article 3. The discipline of internet use in Brazil has the following principles: (...) III—protection of personal data, in accordance with the law; (...).

¹⁴ Article 7. Access to the internet is essential to the exercise of citizenship, and the user is guaranteed the following rights: (...) IV—clear and complete information contained in the service provision contracts, with details on the protection regime for connection records and access records to internet applications, as well as on network management practices that may affect their quality; VII—clear and complete information about the collection, use, storage, treatment, and protection of your personal data, which can only be used for purposes that: a) justify their collection; b) are not prohibited by law; and c) are specified in the service provision contracts or in terms of using internet applications (...) IX—express consent on the collection, use, storage, and treatment of personal data, which must occur in a detached manner from the other contractual clauses.

In turn, the *Wiretap Act*¹⁵ (Law No. 9,296/1996) regulates interception by government authorities in Brazil and establishes that the interception of communications can only occur when authorized by a court order, on request by police authorities and the Public Prosecutor's Office, for the purposes of criminal investigation proceedings. Moreover, the *Wiretap Act* foresees that the interception of telephone communications, of any nature, for evidence in a criminal investigation and in criminal proceedings shall comply with the provisions of the law and will depend on the order of the competent judge of the main procedure within which the investigation is being conducted, under the secrecy of justice¹⁶, which means that interception requested by authorities not expressly designated, such as the Brazilian National Intelligence Agency (“*Agência Brasileira de Inteligência*” or “*ABIN*”), is prohibited¹⁷. However, the provisions stated in the *Wiretap Act* apply only to the *interception of the flow of communications in computer and telematics systems*; in other words, the verification of text messages or the last calls received or made from cell phones seized in the possession of suspects, for instance, is not included under the scope of the *Wiretap Act*.

Also, *Resolution No. 59/2008 of the National Council of Justice* (“*CNJ*” in Portuguese) regulates telephone and telematic interception, reinforces the need in the court order for breach of confidentiality to indicate reasonable evidence of authorship or participation of the targets in the investigated criminal offense, establishes standards for court decisions on the matter, defines the form in which notices to companies of interest shall be submitted, and holds judges responsible for protecting the privacy of intercepted information. *Resolution No. 36/09 of the Public Attorney's Office National Council* (“*CNMP*” in Portuguese) contains similar provisions regarding request forms and the execution of interception. The purposes of said resolutions are to limit the possibilities for abuse when issuing court orders, mitigate risks that may affect secrecy and, hence, success of the investigations, and increase the security of intercepted information. Furthermore, they also establish that members of the Public Attorney's Office and judges shall inform, respectively, the Inspector General of the Public Attorney's Office (“*Corregedoria-Geral do Ministério Público*”) and the Inspector General of the National Judiciary Office (“*Corregedoria Nacional da Justiça*”), on a monthly basis, of the number of ongoing interception operations for statistical purposes¹⁸.

Also, regarding the general regulatory scenario in Brazil, the new Cybercrime Law (Law No. 14,155/2021) was enacted on May 28th, 2021, and provides for a considerable increase in penalties for hacking into computer devices, theft, and

¹⁵ The Wiretap Act regulated art. 5, item XII, of the Brazilian Federal Constitution, which states that “*correspondence and telegraphic secrecy, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner established by law for the purposes of criminal investigation or criminal procedural instruction.*”

¹⁶ Art. 1 of the Wiretap Act.

¹⁷ Art. 2 of the Wiretap Act limits even further the circumstance under which it may occur: it shall not be allowed in case there is no reasonable evidence of criminal responsibility or conspiracy to commit a crime; in case evidence can be obtained by other means; or when the act under investigation is subject to no more than an imprisonment sentence of the type “*detenção*” (common for misdemeanors).

¹⁸ Art. 10 of Resolution No. 36/09 and art. 18 of Resolution No. 59/08.

embezzlement perpetrated electronically or through the Internet. The Law does not create new crimes but rather increases the punishment for offenses already provided for in the Brazilian Criminal Code 1920¹⁹, in response to the significant increase in internet fraud over 2020, which occurred as a result of the home office practices adopted due to isolation measures enforced to deal with the COVID-19 pandemic, involving more sophisticated and widespread schemes.

More specifically, the following regulations can be highlighted: the *Good Payers Registry Act* (Law No. 12,414/2011) creates a ‘good payers’ registry and provides that personal data may be used and disclosed for credit-risk analysis without the need for consent, in order to create the registry, with the exception of sensitive data or data that is excessive or not compatible with the purpose; *Resolution No. 4,893/2021* of the National Monetary Council, which regulates the need for financial institutions to implement cybersecurity policies and the requirements to be observed by those institutions when contracting data storage services, data processing services or cloud computing services; *Resolution No. 4,480/2016* of the National Monetary Council, which regulates the opening and closing of bank accounts by electronic means; *Resolution No. 4,474/2016* of the National Monetary Council, which regulates the digitalization of documents; and the *Medical Conduct Code* (Resolution No. 2,217/2018 of the Federal Council of Medicine), which protects the confidentiality of patients’ information and medical records, subject to limited exceptions, and regulates the use of computer systems for the handling and retention of such data, authorizing the digitalization and electronic storage of medical records.

Nevertheless, the *key statute* that regulates the processing of personal data in Brazil is the *Brazilian General Data Protection Law* (Law No. 13,709/2018 or

¹⁹ According to the new wording of art. 154-A of the Criminal Code, the action of hacking into someone’s computer device, whether or not connected to the Internet, in order to obtain, modify, or destroy data or information without the user’s authorization, or to install vulnerabilities on the device in order to obtain unlawful advantages, is now a crime punishable by imprisonment ranging from one (1) to four (4) years, plus a fine. Previously, the imprisonment penalty for said conducts was considerably lower, ranging from three (3) months to one (1) year of detention. The wording of the offence has been modified to clarify that criminal law applies even if the victim is merely a lawful user but not the owner of the device, a recurrent condition during the home-office period. If the hacking results in economic losses, the penalty is increased by 1/3 to 2/3 (previously, the increase ranged from 1/3 to half). If the hacking results in the acquisition of private electronic communications, commercial or industrial secrets, confidential information, or allows for the unauthorized remote control of the hacked device, the penalty is even higher: confinement, ranging from two (2) to five (5) years of imprisonment plus a fine (previously, it was from six [6] months to two [2] years and a fine).

²⁰ The crime of embezzlement, set forth in art. 171 of the Criminal Code, entails a penalty that ranges from one (1) to five (5) years of imprisonment and a fine. The new law includes, in § 2-A, that if the fraud is committed with the use of information supplied by the victim or by a third party fraudulently induced by social networks, telephone contacts, electronic mail, or similar means, the penalty of imprisonment is augmented, ranging from four (4) to eight (8) years and a fine. If such crimes are perpetrated with the use of a server located abroad, the penalties are increased by 1/3 to 2/3. Supposing that the crime targets the elderly or vulnerable victims, the penalties are increased by 1/3 to the double.

“LGPD” in Portuguese), which is the first²¹ specific legislation on the subject in Brazil. The LGPD was signed into law on August 14th, 2018, and entered into force on September 18th, 2020, with the exception of the administrative sanctions, which became effective as of August 1st, 2021, due to Law No. 14,010/20.

The text of the LGPD follows the worldwide trend of strengthening personal data protection, guaranteeing a series of rights to data subjects, as well as imposing important obligations on processing agents. The purpose of the LGPD, hence, is to boost economic and technological development in Brazil, providing greater legal certainty to operations involving the processing of personal data. That said, the LGPD replicates key points of the General Data Protection Regulation (Regulation No. 2016/679 or “GDPR”) that took effect on May 25th, 2018, and applies to any processing operation carried out by a natural person or a legal entity of either public or private law, irrespective of the means, the country in which its headquarter is located, or the country where the data are located, provided that: (a) the processing operation is carried out in the national territory; (b) the processing activity is aimed at the offering or provision of goods or services, or at the processing of data of individuals located on Brazilian territory; and/or (c) the personal data being processed were collected in the national territory (as per art. 3 of the LGPD).

The LGPD does not apply, however, when the processing of personal data is done: (a) by a natural person exclusively for private and non-economic purposes; (b) exclusively for journalistic, artistic, or academic purposes; (c) exclusively for purposes of public safety, national defense, state security, activities of investigation, and prosecution of criminal offenses; or when the personal data (d) has its origin outside the national territory and is not the object of communication, shared use of data with Brazilian processing agents, or the object of international transfer of data with another country that is not the country of origin, since the country of origin provides a level of personal data protection adequate to that established in the LGPD (as per art. 4 of the LGPD)—so, when the personal data is only in transit throughout the Brazilian territory, it should not be considered processing.

The regulatory body responsible for the enforcement of data protection rules in Brazil is the National Data Protection Authority (“ANPD” in Portuguese), which comprises a board of directors, a National Council for Personal Data and Privacy Protection, an internal affairs office, and an ombudsman office. It has powers to apply administrative sanctions and issue guidelines for LGPD compliance. Even though the ANPD has powers to enforce LGPD’s sanctions, other regulatory bodies have been using LGPD as a legal basis for the enforcement of data subjects’ rights, as is the case with a number of consumer protection bodies (PROCONs, for example), the Attorney’s Office in Brasilia (through a Special Unit for Data Protection and Artificial Intelligence), the National Consumer Secretariat (SENACON), and by lower courts in Brazil.

²¹ In terms of data protection, the LGPD can be considered the first *general* law in Brazil, since it focuses *exclusively* on the theme and can be applied without distinction to *any processing* of personal data (carried out both in digital and offline media), by *any person*, in *any sector*, except for the exceptions set out in the LGPD itself. That is, the LGPD is *general (omnibus law)* regarding the protection of personal data in Brazil [17, p. 409].

4 Information security in Brazil

When it comes to security of information and of technological systems, as opposed to the GDPR²², the LGPD does not determine which *specific* security measures shall be adopted by the controller and the processor, even though said aspect of the Law is to be further regulated by ANPD, according to Ordinance No. 11/2021. With that, it is expected that the ANPD will provide minimum technical standards, taking into account the nature of the processed information, the specific characteristics of the processing and the current state of technology, in order to assist processing agents to comply with the standards of security and secrecy of data provided for in the LGPD.

In spite of that, the LGPD foresees that processing agents shall adopt security, technical, and administrative measures to be able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication, or any type of improper or unlawful processing (as per art. 46), and, also, that said measures shall be complied with from the conception phase of the product or service until its execution. Beyond that, the LGPD states that processing agents or any other person that intervenes in one of the processing phases commit themselves to ensure the security of the information as provided in the LGPD regarding personal data, even following the conclusion of the processing in question (as per art. 47). Consequently, it is expected that companies will start to incorporate protective measures as to their systems by design to any new technology or product, in order to place the security of processed personal data at the center of all development.

Adding to that, the Internet Act and Decree No. 8,771/2016 already mentioned provide for information security in Brazil by referring to security and confidentiality standards for records, personal data, and private communications, specifically referring to strict control over access to data, definition of responsibilities, access authentication mechanisms (i.e., dual authentication to ensure the individualization of the person responsible), and the use of record management solutions through techniques that guarantee the inviolability of data, such as encryption or equivalent protection measures (cf. art. 13 of the Decree).

In this sense, companies will be required to implement, for example, an information security policy, which should include the set of standards, definitions, practices, security measures, responsibilities, and penalties applicable to all employees of the company who may use the company's information technology infrastructure in order to minimize the risk of loss or breach of any IT asset; that is, companies will have to make sure that all security measures are being taken to protect corporate information against possible threats of data leaks and security incidents, especially

²² The GDPR foresees in art. 32 that the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

considering that, under the LGPD, the systems used for processing personal data shall be structured to meet the security requirements, standards of good practices and governance, general principles provided in the LGPD, *and other regulatory rules* (as per art. 49).

So, pursuant to the nonrestrictive provision previously stated and until further regulation, technical security measures shall be adopted in compliance with international standards, which include the: (a) GDPR; (b) Directive on Security of Network and Information Systems (Directive 2016/1148 or “NIS”); (c) Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act); and (d) technical market standards, related to the Privacy Information Management System (“PIMS”) and to *Personally Identifiable Information* (“PII”) (i.e., ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701), since it is likely that the ANPD will follow the international trend when regulating the matter.

Among the most important technical market standards, the following are deemed the most important: (a) ISO/IEC 27001, which is the standard and international reference for information security management; (b) ISO/IEC 27002, which establishes a set of good practices necessary for the purpose of ensuring information security (i.e., access control, human resources security, physical and environmental security, and asset management); and (c) ISO/IEC 27701, which specifies requirements and provides guidance for establishing, implementing, maintaining, and continuously improving a PIMS in the form of an extension of ISO/IEC 27001 and of ISO/IEC 27002 for privacy management in the context of an organization. For storage and/or processing of personal data in cloud services, ISO/IEC 27018, which establishes the code of practice for protecting PII, should be consulted.

Without exemption and in addition to the international standards presented, there are two regulations in Brazil that, albeit being specific to the entities they apply to, shall be considered when assessing the information security legal landscape the country relies on. The *first* is Resolution No. 4,658/2018 of the Brazilian Central Bank (“Bacen” in Portuguese), which establishes obligations only for financial institutions and other institutions authorized by Bacen to operate. The Regulation foresees that drafting and enabling public access to a cybersecurity policy is mandatory and reflects the three fundamental guidelines provided for in the main foreign regulations mentioned for compliance purposes, namely, the confidentiality, integrity, and availability of the data and information systems used. The *second* is Decree No. 10,222/2020, which approves the National Cyber Security Strategy (“E-Ciber”) and establishes cybersecurity guidelines and rules to be followed by bodies and entities of the federal public administration in Brazil. Therefore, considering that the ANPD was created as part of the federal public administration itself (as per art. 55-A of the LGPD), it will be directly affected by such parameters, which involve, for example, the strengthening of cyber governance actions (i.e., controls for the processing of information with restricted access, adoption of national encryption solutions, use of cybersecurity certification, etc., as per item 2.3.1 of E-Ciber). In sum, even if Resolution No. 4,658/2018 of the Brazilian Central Bank and E-Ciber Decree do not apply broadly to all processing agents subject to Brazilian legislation, they provide

important instruments and guidelines on how the subject will be further regulated in the country.

5 “IT Privacy” right in Brazil?

The IT *Grundrecht* emerged as a byproduct of a juridical assessment conducted by the BVerfG based on the *general right of personality* and the *principle of human dignity*, according to which said fundamental right was also a *special implicit right of personality*, in the same sense as informative self-determination. That is, the decision followed the dynamics in the sphere of the *evolution of information technologies* and the need for adequate regulatory reactions to the effect of protecting fundamental rights, including in the area of personal data protection [9, p. 93]²³, which ended up confirming the insufficiency of a right to informative self-determination and, in any case, did not simply replace other rights, such as privacy [22, p. 33].

That said, in order to recognize an IT Privacy right in Brazil—or even to discuss said possibility—at least those same elements shall be taken into consideration. Yet, when it comes to discussing privacy and data protection in Brazil, one needs to take a step back and understand that Brazil, as opposed to Germany, does not have the same tradition regarding the protection of personal data and does not rely on a privacy culture that is as strong as that in Germany, because, even though Brazil does count on specific legislation on the matter, the laws themselves are comparatively recent.

With that, if on the one hand the fundamental right to confidentiality and to IT integrity systems, as seen, was construed by the BVerfG based on elements that have been long developed and discussed in the country, at least since the 1980s, as is the case with the right to informational self-determination, on the other, in spite of the fact that Brazil already has a regulatory scenario on privacy and data protection, the country still lacks enforceability and general culture on the matter, which makes it difficult at this point to recognize an IT Privacy right in Brazil.

Beyond that, another aspect that would add to the difficulty in affirming the emergence of an IT-related fundamental right for the purposes of data protection is that, as opposed to the German constitutional order, which protects several legal assets under the guise of a single—but broad—concept named the general personality right (*das Allgemeine Persönlichkeitsrecht*), in Brazil, those assets, or legal rights, are protected separately (in articles of the Federal Constitution or infra-constitutional legislation, such as the title of the rights of personality in the Civil Code) [5, p. 220]. In other words, the Brazilian Constitutional Order does not provide for the same unity as does the German, which is important for the full protection of the person and the most diverse aspects of personality based on human dignity [5, p. 220] and impacts the way a fundamental right such as of the confidentiality and integrity of technical and informational systems would be interpreted and recognized in Brazil.

²³ To legally protect personal data also belongs to the legal protection of autonomy; that is, a realization of the protection of human dignity and the protection of personality, especially in the form of the protection of informational self-determination [9, p. 93].

In spite of that, Brazil adopts an open fundamental rights system²⁴ [21, p. 147], which allows for the recognition of fundamental rights not expressly provided for in the Constitution ([1], p. 105)²⁵, by means of assessing, case-by-case, whether the right at hand directly relates, or not, to the person's dignity [20, p. 116], or by identifying how essential a given right is to the purpose of enforcing human dignity [18, p. 115]. And so, in relation to the rights of personality in Brazil, as enshrined in the current Civil Code, these could already be deduced from a general clause of protection of the personality anchored in the general right of freedom and in the principle of dignity of the human person [21, p. 47], in the same way that occurs with the right to a name, already established by the Brazilian Supreme Court²⁶. Therefore, there would be grounds to defend the recognition of an IT Privacy right in Brazil, because the same risk identified in Germany on the possibility to monitor the behavior of users and to enter technological devices to access the communications storage can also be seen in Brazil, and Brazil is beginning to assign more and more importance on information security.

6 Closing remarks

All that said, the research responds to the initial question presented, which is, “Starting from the premises set by the BVerfG in the ruling rendered on February 27th, 2008, are there similar grounds to sustain the existence of an IT Privacy right in Brazil, regarding the Brazilian juridical scenario, mainly as to data protection,” affirmatively, as it has been demonstrated that, even though Germany has a more evolved privacy and data protection legal background, the current gaps that

²⁴ “A abertura do sistema de direitos fundamentais (...) abrange tanto a previsão expressa de uma abertura a direitos não enumerados quanto a dedução de posições jusfundamentais por meio da delimitação do âmbito de proteção dos direitos fundamentais, a inclusão dos direitos de matriz internacional, bem como a dedução de normas de direitos fundamentais de outras normas constitucionais, tudo a demonstrar que as possibilidades da abertura do catálogo constitucional de direitos fundamentais são múltiplas e complexas” [21, p. 147]. Free translation: “The opening of the fundamental rights system (...) encompasses both the express provision of an opening to unlisted rights and the deduction of fundamental legal positions through the delimitation of the scope of protection of fundamental rights, the inclusion of rights of an international nature, as well as the deduction of fundamental rights norms from other constitutional norms, all to demonstrate that the possibilities of opening the constitutional catalog of fundamental rights are multiple and complex.”

²⁵ According to Alexy ([1], p. 102), “uma norma de direito fundamental atribuída é uma norma para cuja atribuição é possível uma correta fundamentação referida a direitos fundamentais. Se é possível uma correta fundamentação referida a direitos fundamentais para a norma que se acaba de apresentar—algo que aqui se pressupõe—, então, ela é uma norma de direito fundamental.” Free translation: “An assigned fundamental rights norm is a norm for the attribution of which a correct foundation referred to fundamental rights is possible. If a correct foundation referring to fundamental rights is possible for the rule just presented—something that is assumed here—then it is a rule of fundamental law.”

²⁶ See the judgment handed down in Extraordinary Appeal No. 248.869-1, ruled in July 8th, 2003 by Justice Maurício Corrêa, where it was once again stated that “the right to a name is inserted in the concept of human dignity and reflects its identity, the origin of their ancestry, the recognition of the family, which is why the state of affiliation is an unavailable right.” Free translation of: “o direito ao nome insere-se no conceito de dignidade da pessoa humana e traduz a sua identidade, a origem de sua ancestralidade, o reconhecimento da família, razão pela qual o estado de filiação é direito indisponível.”

exist in the Brazilian regulatory framework, which is the case, for instance, for the non-applicability of the LGPD for the purpose of investigation and prosecution of criminal offenses (as per art. 4, III, “d”), may allow room for the recognition of an IT Privacy fundamental right, due to the potential state of surveillance they are prone to generate, especially by means of technological devices.

Beyond that, even though the main goal of the research was not to investigate precisely and in depth the right to personality (in Germany, the general right to personality or “*Allgemeines Persönlichkeitsrecht*”) and the requirements that must be fulfilled in order to recognize the existence of a fundamental right, one can also infer that the fundamental right to the confidentiality and integrity of technical and informational systems was deduced from the general personality clause in Germany, but it is also linked to the dignity of the human person in the context of the right to information and the protection of personal data. Thus, the IT Privacy right may be recognized in Brazil, in the same way as the informational self-determination right. Overall, these circumstances reveal, as defended by Sarlet [20, p. 120], how much the problem of the material opening of the catalog and the argumentative resource for the principle of human dignity is still far from being exhausted when the impact of new technologies on human life and dignity and life in general is taken seriously.

References

Cited Literature

1. Alexy R (2015) Teoria dos direitos fundamentais, 2nd ed. Malheiros
2. Appel G, Grewal L, Hadi R et al (2020) The future of social media in marketing. *J Acad Mark Sci* 48:79–95. <https://doi.org/10.1007/s11747-019-00695-1>
3. Betkier M (2019) Privacy online, law and the effective regulation of online services, 1st edn. Intersentia, Cambridge
4. BVerfG, Urteil des Ersten Senats vom 11. März 2008 - 1 BvR 2074/05 -, Rn. 1–185, http://www.bverfg.de/e/rs20080311_1bvr207405.html
5. Cunha AS (2021) A privacidade como direito guarda-chuva na Alemanha e nos Estados unidos e seu reflexo nos modelos de proteção de dados. In: Ody LFW (ed) *Direito Comparado Brasil-Alemanha: temas de direito privado em estudos originais e traduzidos*. Faculdade de Direito da UFRGS, Porto Alegre, pp 213–240
6. Eifert M (2008) Informationelle Selbstbestimmung im Internet: Das BVerfG und die Online-Durchsuchungen. *Neue Z Verwaltungsr Ver Mit Verwaltungsrechtsprech* 27(5):521–523
7. eMarketer (2018) Social Network Users and Penetration in Worldwide. Retrieved from <https://tinyurl.com/ycr2d3v9>
8. Hoffmann-Riem W, Ribeiro PH (2020) A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da informação. *J Contemp Priv Law* 23(7):329–365 (<http://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/771>)
9. Hoffmann-Riem W (2021) Teoria geral do direito digital: transformação digital: desafios para o direito, 1st edn. Forense, São Paulo
10. Hoeren T (2008) Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme? *Multimed Recht* 6:365–366 (https://www.itm.nrw/wp-content/uploads/grundrecht_auf_integritaet.pdf)
11. Hornung G (2008) Der verfassungsrechtliche Schutz der “Vertraulichkeit und Integrität informationstechnischer Systeme”. *Comput Recht* 24(5):299–306. <https://doi.org/10.9785/ovs-cr-2008-299>
12. Hornung G, Schnabel C (2009) Data protection in Germany I: the population census decision and the right to information self-determination. *Comput Law Secur Rev* 25(1):84–88. <https://doi.org/10.1016/j.clsr.2008.11.002>

13. Hornung G, Schnabel C (2009) Data protection in Germany II: recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Comput Law Secur Rep* 25(2):115–122. <https://doi.org/10.1016/j.clsr.2009.02.008>
14. Krlev G, Anheier HK, Mildemberger G (2019) Social Innovation—What is it and who makes it? In: Krlev G, Anheier HK, Mildemberger G (eds) *Social Innovation: comparative perspectives*. Routledge, New York, London, pp 3–36
15. Mendes GF, Branco PG (2021) *Curso de Direito Constitucional*, 16th edn. Saraiva, São José dos Campos
16. Menke F (2019) A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira* 5(1):781–809. ISSN: 2183-539X. http://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf
17. Parentoni LN, Lima HCS (2020) Protection of personal data in Brazil: internal antinomies and international aspects. In: Pereira de Lima CR (ed) *Comentários à Lei Geral de Proteção de Dados*. Almedina, Coimbra, pp 399–431
18. Reis J (2018) *Interpretação constitucional e direitos fundamentais*, 2nd edn. Saraiva Educação, São José dos Campos
19. Ruaro RL, Rodríguez DP (2010) O direito à proteção de dados pessoais na sociedade da informação. *Revist Direito Estado Soc* 36:178–199 (http://direitoestadosociedade.jur.puc-rio.br/media/8ruaro_rodriguez36.pdf)
20. Sarlet IW (2019) *Dignidade (da pessoa) humana e direitos fundamentais na Constituição Federal de 1988*, 10th edn. Livraria do Advogado, Porto Alegre
21. Sarlet IW, Marinoni LG, Mitidiero D (2021) *Curso de Direito Constitucional*, 10th edn. Saraiva, São José dos Campos
22. Sarlet IW (2021) *Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados*. In: Mendes LS, Doneda D, Sarlet IW, Schertel L, Rodrigues OL Jr (eds) *Tratado de Proteção de Dados Pessoais*. Forense, Rio de Janeiro, pp 21–59

Further Reading

23. Hoffmann-Riem W (2008) Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme. *JuristenZeitung* 63:1009–1022