PRIVACY, DATA PROTECTION AND THE AGE OF ALGORITHMS

by **Fernanda GONÇALES**, UNINTER – Centro Universitário Internacional. City of Curitiba/Brasil.

Technology is part of contemporary life, and because it is an expression of the reality of the information society, it cannot be left out of the law. Far beyond hermeneutics in the interpretation of norms, the law faces a new challenge, technological issues. Algorithms have become an important resource in the development and improvement of products and services. Technology is not averse to law, there is much to be debated, the academic theoretical framework is fundamental to guide the best interpretation and application of the law to specific cases. The general objective of the study is to promote a bibliographic review about the concept of privacy, pointing out its main elements. The article aims at researching the use of algorithms, seeking to understand its impact considering the constitutional right to privacy. The working hypothesis is to verify if the use of algorithms along the current lines, preserves or not the right to privacy. As a conclusion, the study points out that the term privacy, depending on the socioeconomic or cultural context, has different meanings and is far from being a doctrinal consensus on its concept and that the use of algorithms is currently obscure and there is no specific legislation to be. followed in this field.

The history of privacy is deeply intertwined with the history of technology, has long been a definition for the term is discussed, in addition, the idea of what is privacy is changing, as is the mutant comportament to society itself. At the beginning of the century, the publication of a photo without consent could become the subject of a dispute between the photographed subject and the author of the photograph[1], today, nothing more common than we access social networking is and we encounter the publication of intimate known and strange moments.

The construction of human personality before the world is no longer limited to the individual field, but stems from the relationship between the individual and the others. This interaction permeates the digital means of communication. Therefore, the guardianship of this individual must take place "in relation to others (the meaning of otherness) and to the external world. Today it is known that the human

[1] *Marian Manola v. Stevens & Myers*, New York Supreme Court, New York Times of June 15, 1890. The complainant claimed that while playing at the Broadway Theater, in a role that required her to appear in the flashlight, she was photographed clandestinely and without their consent, by defendants Stevens, and Myers, pleading that defendants should be prevented from using the photograph taken.

being exists only as part of a species that needs other (s) to exist (rectius, coexist)"[2].

Society is fully engaged in a technological information revolution, but it is just beginning to understand its implications, including in the field of law. In the last decades, the way we shop, carry out bank transactions and interact with our peers has resulted in a gigantic accumulation of information about where we are, what we do, what we have and our tastes. With the use of technology, these records are preserved indefinitely in databases, classified, reorganized, combined in hundreds of different ways and used for the most diverse purposes, from marketing notifications, credit analysis and even for evaluating possible love matches.

Concern for privacy varies over time, ethnic and social subgroups, sex and so on. A seemingly simple name and address on a website may not have any implications for most people, but situations of vulnerability profoundly alter the context of privacy, for example, victims of domestic assault and witnesses to crime, certainly do not intend that such data are available for public access.

Without a nucleus of legal meaning for the term privacy, even if there is a legal provision, any law will be inadequate to enforce the right to privacy. Warren and Brandeis[3] point out that social and legal tolerance of public exposure can corrupt a society, diverting attention from important economic and political issues. The authors add that while several strategies, including laws, have been employed to protect privacy interests, the standard must explicitly authorize people to determine the extent to which their thoughts, feelings, emotions and productions become available to the world at large regardless of any economic valuation.

Far beyond hermeneutics in the interpretation of norms, the law faces a new challenge, technological issues.

Algorithms have become an important resource in the development and improvement of products and services. For example, a bank can use data about users' browsing habits on its website to improve the view of the program screen, improving the customer experience, reducing the time between the user logging on to the website and making a payment.

We are going through a moment of transition in human interactions due to the use of technological tools, which demands research from the legal point of view. While several countries have been discussing the right to privacy and data protection since the 19th century, in Brazil the most in-depth studies emerged with the Marco Civil da Internet, in 2014. It is imperative that legal operators understand the application of

[2] M. C. B. MORAES, *Ampliando os direitos da personalidade. Na medida da pessoa humana: Estudo de direito civil-constitucional*, Rio de Janeiro: Renovar, 2010.

[3] S. WARREN, L. D. BRANDEIS, "The right to privacy", *Harvard Law Review*, Cambridge: Harvard Law Review Association, No. 193, 1890.

technology in the context of social relations with the necessary depth.

Technology is part of contemporary life, and because it is an expression of the reality of the information society, it cannot be left out of the law. The judiciary will certainly have to judge demands involving source code, algorithms, SQL injection, phishing, IOT, query among many others. It is in this gap that the research and academic production contribute by improving knowledge for improvement and material evolution of society, enabling, for example, theoretical framework for the effective rules applying to the case or not the design of new public policies aimed at welfare Social.

To Danilo Doneda[4] the law must be able to provide answers to questions brought by technology with attention to the constitutional text. The author very well points out that "The real problem is not knowing what the law should act on, but how to interpret technology and its possibilities in relation to the values present in the legal system […]".

In addition, the instrumentalization and effectiveness of law involves the construction of solid interpretations, the lack of clarity in legal terms creates barriers to formulate policies[5] or even to resolve disputes. The parameters brought by the interpretation and application of the law reflect the legal security that full citizenship demands.

A right that is not able to understand the dynamics between society and technology and the new problems resulting from this relationship loses contact with reality, becoming early obsolete[6].

There is a lot to be researched and produced, the theoretical apparatus is fundamental to guide the best interpretation and application of the law to specific cases. When searching for the biography of the references used in this work, what were found were several philosophers, sociologists and researchers linked to information technology, but few doctrines linked to law, which further reinforces the importance of studies on this matter from a legal perspective.

§ 1 – PRIVACY

As a starting point of this research, and for a better understanding, it is important to address the concept of privacy. The present study does not intend to create a semantic definition in stone, it is much more concerned with highlighting

[4] D. DONEDA, *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2020. Eletronic version.

[5] In England, discontent with the definition of privacy led the Younger Privacy Committee to recommend, in 1972, against recognizing the right to privacy, as proposed in legislation at the time. The main difficulty in enacting statutory privacy protection, said the committee's report, is "the lack of any clear and generally accepted definition of what privacy itself is." Courts would have difficulty dealing with "such a poorly defined and unstable concept". As a result, the legislation was not passed.

[6] Idem 4.

the need for harmonization regarding interpretative limits, from the perspective of the law, for an expression that is truly multifaceted.

Privacy is seen as one of the leading issues of our time and a key aspect of human dignity. The contrast between today's privacy landscape and that of the early 1990s is enormous. The arrival of technology, in the last century, in the daily life of society has created new complexities, intensities and vulnerabilities, highlighting the need for renewed legal analysis that considers the involvement of technology in aspects of privacy.

Traditional ways of conceptualizing privacy do not take into account the aspects and problems that the digital age has introduced[7]. Therefore, there is an urgent need to define the term privacy, under the legal bias and within the current context, that is, within the reality experienced by society mainly with the insertion of the media and technology.

Although there is no doubt about the importance and value of privacy, the understanding of its meaning is not unanimous, depending on the angle of analysis; philosophical, legal, economic, individual or collective, it can take different forms and interpretations.

The different conceptions can be the result of the methodology used, which makes the discussion even more complex. Marcel Leonardi[8] points out that most attempts to draw the meaning of privacy use traditional methods such as the definition *per genus et differentiam*[9], in this sense, a combination of common elements is used, meaning "core", "essence", "core", "axis", "mainspring", "core", "soul", "bulge", which allows differentiating a right, privacy in this case, from other rights, creating a unitary notion. With this technique, we intend to separate concepts allowing us to subsume a certain factual situation to this or that category depending on its definition.

Privacy can be defined much more subjectively than objectively. Privacy is commonly used as a parent term or keyword, which comprises an infinite number of possible interpretations, about which the doctrine[10] uses several other synonyms such as internally, intimate life, secret, secret, confidential, be alone, autonomy *privacy, intimacy, secret, secrecy, modesty, reserve, their privacy, and even "privateness"*[11].

---

[7] D. J. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age,* New York: Harvard University Press, 2004.

[8] M. LEONARDI, *Tutela e privacidade na internet,* São Paulo: Saraiva, 2011. p. 51.

[9] By the close gender and by the specific difference.

[10] The same is true in foreign doctrine, which uses a variety of expressions to refer to privacy. In Germany, there is "die Privatsphäre", separating individual autonomy and social life. Spain prefers the term "Derecho a la intimidad". In the United States, the term "privacy" is used. In France, there is talk of "droit au secret de la vie privée" and "protection de vie privée". In Italy, it refers to the "diritto alla riservatezza" and the "diritto alla secretezza and privacy". In Portugal, it is said to reserve the "intimacy of private life and privacy". (Leonardi, 2011, p. 46)

[11] D. DONEDA, *From Privacy to the Protection of Personal Data*, Rio de Janeiro: Renew, 2020, Electronic version.

Marcel Leonardi[12] mentions that the conception of privacy can be more or less comprehensive, and some related expressions can be included, or not, depending on the line of understanding adopted by the various doctrine scholars, pointing as related to privacy the terms:

> "freedom of thought, control over one's own body, stillness at home, modesty, control over personal information, protection of reputation, protection against searches and investigations, personality development, informative self-determination".

Paulo Mota Pinto[13] states that the term privacy is elastic and trying to define it is practically impossible:

> "[…] If it is true that attempts have been made to define the philosophical, political, sociological or psychological definition of privacy, it does not seem that it was possible to end the concept with the minimum precision necessary for it to serve as the basis for a cohesive legal regime".

The word privacy comprises an entire universe in itself, and it is not a self-explanatory term, it could be said to involve everything that relates to each individual's personal space, aspects of himself, his body, thoughts, desires, fears, whether in the physical world or not, and that the lack of privacy makes the individual vulnerable to the external. Thus, once life alternates within a dynamic of social life, privacy can be represented by individual attitudes and reservations.

The problem surrounding a conception for privacy has two sides; the definition is too broad or too narrow, depending on the terms used, which may include matters considered private or not[14]. The absence of a delimited form can lead to the difficulty of applying the law, making it difficult or impossible to protect it, especially in the face of conflicting rights and interests[15]. In this sense, how to articulate the damage to privacy when there is no definition for the term.

Much of the doctrine that deals with privacy defend its importance, but does not define what privacy is, authors commonly relate it to several other values, including the right to be left alone and respect due to the individual's inviolable personality[16].

Without a sense of what is private, the concepts of limited access do not demonstrate which are the nouns that would imply complete privacy. Daniel Solove[17] points out that not all access to the *self* infringes privacy, only access related to specific

[12] Idem 8, p. 48.
[13] P. M. PINTO, *O Direito à Reserva sobre a Intimidade da Vida Privada*, Boletim da Faculdade de Direito, Coimbra, v. 69, 1993, p. 504.
[14] Idem 8, p. 51.
[15] Idem 8, p. 58.
[16] F. D SCHOEMAN, *Dimensões filosóficas da privacidade,* Cambridge University Press. Kindle Edition.
[17] SOLOVE, D. J., *Understanding Privacy*, New York: Harvard University Press, 2008, p. 26.

dimensions of the *self* or to particular subjects and information. In addition, there is no understanding of the degree of access necessary to constitute a breach of privacy.

According to Arendt's definitions[18] it would be possible to define privacy as the separation between common life, among other equals, and the space of the family.

However, the dichotomy person public space and person family space cannot be considered as the best definition for the term privacy. Lóscio[19] very well points out that privacy is a historical and cultural notion. It is built on the basis of social, economic and political conditions of a specific time and place. In this sense, the construction of the sense of privacy brought by Arendt has a direct connection with the reality experienced back there by Greek society.

Traditionally, privacy has been understood as the right to "be left alone", this understanding is based on the article by Warren and Brandeis dated 1890. This right - the "right to be left alone" – was a "right general protection of the person's immunity, the right to personality"[20].

Marcel Leonardi[21] lists the main ideas for a conception of the term privacy:

> "a) the right to be left alone; b) protection against interference from others; c) secrecy or secrecy; d) control over personal information and data".

For Caitlin Mulholland, the right to privacy, and more specifically, the right to intimacy, alludes to the protection of a person's private or intimate sphere, in the face of external, foreign and unauthorized interference. The author understands that the concept has evolved including in its content situations of protection of sensitive data, of its control by the holder and, especially, of respect for the freedom of personal choices of an existential character[22].

As seen, privacy is a word of many meanings, the problem addressed by the philosophical and legal debate is precisely the imprecision of the concept. But this is not just a quality of privacy, several other terms find the same difficulty, freedom and democracy are examples. Although there are differences between the various authors, two approaches are commonly found in the literature to characterize what privacy would be: the idea of

---

[18] H. ARENDT, *A condição humana* (Trad. R. Raposo), 10st ed., Rio de Janeiro: Forense Universitária, 2007, p. 41.

[19] B. F. LÓSCIO, H. R. Oliveira, J. César de Souza PONTES, *NoSQL no desenvolvimento de aplicações Web colaborativas, 2011*. Available at: https://www.addlabs.uff.br/sbsc_site/SBSC2011_NoSQL.pdf, Accessed on: 29 March 2020, p. 101.

[20] Idem 19.

[21] Idem 8, p. 52.

[22] C.MULHOLLAND, *O Direito de não saber como decorrência do direito à intimidade – Comentários aos REsp 1.195.995*, Civilistica.com. Rio de Janeiro, a. 1, jul-set/2012. Available at: http://civilistica.com/wp-content/uploads/2012/09/Direito-de-nao-saber-civilistica.com-1.-2012.pdf. Accessed on: 29 March 2020.

restricting access, and the notion of control. Thus, given the focus of this project, the perception of privacy will be considered based on these two elements: restriction of access to what is considered private, such as personal information, and the practice of control, in the sense that the choice belongs to the holder whether or not the information.

§ 2 – WHY TALK ABOUT PRIVACY?

In the current configuration of society, in which technology is present in almost all activities, there are certainly many reasons to talk about privacy, but considering that this work deals with privacy with a focus on data protection and the use of algorithms, it is. From this perspective, some reasons will be pointed out about why it became so important to talk about privacy.

There is no doubt that technology made life much easier, shortened distances and provided real-time means of communication. In the 2000s, the relationship with technology underwent significant changes. Charging electronic devices and interacting with them all the time has become commonplace. We have come to trust that the cell phone and its various applications indicate the direction, help us choose lunch or who to date.

Fernanda Bruno[23] points out that technological structures, such as platforms and social networks, have potentiated the individual forms of communication and expression, but, on the other hand, mechanisms for monitoring, capturing, tracking and categorizing data have grown in the same proportion, to "feed strategies for advertising, security, service and application development […]".

Collected and managed data is a powerful weapon, so-called data brokers capture individual information and convert it into scores, classifications and risk calculations for further monetization, resulting in significant legal impacts. In this problem, the algorithms used do not undergo any regulation or inspection. Through the internet it is possible to find large amounts of personal information, reverse phone books and databases of public records. Marketers are extracting this data with considerable enthusiasm, judging by the significant increase in e-waste and targeted mail in recent years[24].

In recent years, the abusive use of data that has resulted in clear breaches of privacy justifies the discussion on the subject, not only to clarify past facts, but to encourage mature discussions on the topic that become concrete policies for the defense of individual and inalienable rights.

Events such as the terrorist attack of September 11, 2001, in the United States, are used as a justification for the development of

[23] F. Máquinas de Ver BRUNO, *Modos de Ser. Vigilância, Tecnologia e Subjetividade*, Porto Alegre: Sulina, 2013.

[24] J. K. PETRESEN, *Understanding Surveillance Technologies s: spy devices, their origins & applications*, CRC Press, 2001, pp. 3-6

systems that go far beyond mere security and have become true surveillance mechanisms.

After the September 11, 2001, attacks, President George W. Bush sanctioned the *USA Patriot Act*[25], which gave the government surveillance powers, supposedly to combat terrorist actions. There was no public information available on what data and information was being collected, nor who would be the target of this capture, until 2013, when documents from the National Security Agency (NSA) were leaked[26]. These documents revealed high-level spying on ordinary citizens.

The book written by Glenn Greenwald[27], originally titled "*No Place to Hide,"* tells the story of one of the biggest complaints about the use of mass personal data for surveillance purposes by the United States government. The Security Agency, authorized by President Bush, has implemented a program for the mass collection of domestic telephone, internet and email records. To understand the size of the problem, I present a summary of what happened in this case.

The person responsible for the leak of the case is Edward Snowden, who worked for the CIA for some years and left the agency in 2009, when he started to work for private technology companies, which provided services to the NSA. In early 2013, he was hired as a systems administrator, in the division located in Hawaii, of Bozz Allen Hamilton, a company that also provides services to the National Security Agency.

While providing services to the NSA, he gained access to documents whose content was related to US intelligence activities. With data and documents gathered, he went to Hong Kong, where he met journalist Glenn Greenwald, with whom he had been in contact for some time, and filmmaker Laura Poitras, to grant the interviews later released by *The Guardian* and *The*

---

[25] About the*Patriot Act*: https://www.justice.gov/archive/ll/highlights.htm.

[26] According to the NSA page: The National Security Agency (NSA) leads the US Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations in order to gain a decision advantage for the nation and our allies under all circumstances. The Central Security Service (CSS), part of NSA, provides timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community. CSS coordinates and develops policy and guidance on the SIGINT and IA missions of NSA/CSS to ensure military integration.
See: https://www.intelligence.gov/index.php/how-the-ic-works/our-organizations/413-nsa.

[27] Glenn Greenwald is a journalist, constitutional lawyer, author of four *New York Times* bestselling books on politics and law, and one of the three founders of *TheIntercept*. Before founding*Intercept*, Glenn wrote for the British newspaper *The Guardian* and for the portal *Salon*. For his reporting on the NSA, he received the George Polk National Security Reporting Award; the Gannett Foundation Award for Investigative Journalism and Supervisory Journalism; the Esso Award for Excellence in Investigative Reporting in Brazil (it was the first foreigner to be awarded) and the Pioneer Pioneering Award from the Electronic Frontier Foundation. Along with Laura Poitras, *Foreign Policy* magazine named him as one of the top 100 global thinkers of 2013. The NSA reports for *The Guardian* received the 2014 Pulitzer Prize in the Public Service category. Adapted text. Available at: https://theintercept.com/equipe/glenn-greenwald-brasil/

Washington Post[28]. Snowden's files demonstrate that the NSA controls phones and user data worldwide with access to the servers of companies like *Google*, *Yahoo, Facebook*, *Skype* and *Apple;* monitoring would be part of the program PRISM[29], which allowed the NSA, which acts mainly in the fight against terrorism, to have direct access to servers of large Internet companies, which made it possible to monitor user behavior on a global scale[30].

For Snowden, the United States government, through the NSA, would be building mechanisms that would allow access to all types of information, from anyone in the world, without prior science and without the possibility of control[31].

§ 3 – AFTER ALL, WHAT ARE ALGORITHMS?

The law arose with the need to regulate life in society, to defend the innate interests of human beings first, then property and everyday aspects. Whenever a social fact becomes relevant, that is, it interferes in the human field, it becomes equally important to the legal world. Each era has its peculiarities, making the legal analysis of the facts increasingly complex and interdisciplinary.

Talking about algorithms with those working in the information security sector, or with data analysis is an easy task. The challenge of investigating technology under the bias of the law is the difficulty in converting technical terms into terms that are understood by those who do not have experience in the area.

It is not possible to investigate whether the use of algorithms affects the right to privacy if we do not understand what algorithms are, how their presence influences all areas of life connected by technology.

The word algorithm is applied in the mathematical and computer sciences. In mathematics, it is associated with calculation processes. "*In their origin, algorithms are logical systems as old as mathematics*"[32]. In computing, it is connected to a set of perfectly defined rules and logical procedures that lead to the solution of a problem in a finite number of steps[33].

Algorithms are used since the solution of simple problems, such as calculating the arithmetic mean of school grades, calculating interest on bank transactions, converting years into days or months, as well as for more complex issues, such as predicting opponent's plays in chess games, diagnoses of diseases such as

[28] After the interview and reports, the US government revoked Snowden's passport accusing him of being a spy. He currently lives in Russia.

[29] Acronym for Sustainable Methods of Project Integration, the program allows the collection of browsing history, download and transfer of files, content of emails and conversations.

[30] *The Guardian. Edward Snowden: the whistleblower behind the NSA surveillance revelations.* 2013. Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Accessed on: 14 November 2020.

[31] Idem 30.

[32] P. V. A REIS, *Algoritmos e o Direito*, São Paulo: Almedina, 2020, p. 58.

[33] A. N. G. M. JOSE, *Algoritmos,* Editora Saraiva. Kindle Edition.

cancer, outline search parameters and results in internet searches, or define, from a combination of physical and psychological characteristics, predictive indicators of attraction between individuals. It is worth remembering that algorithms alone are not the solution to the problem, but the path that leads to the solution. For example, in the case of the algorithms that investigate the presence of cancer, the program, designed from a database, detects the existence of the parameters that characterize the disease, this result combined with the other exams and analyzes is what results in the final diagnosis. In addition, algorithms can be developed merely for data capture, the so-called data mining, or data mining.

Thinking about the practical application of algorithms, Paulo Victor Alfeo Reis[34], describes in a clear and easily understandable way the construction of an algorithm, according to the author, it is initially necessary to delimit the problem to be solved in order to seek the solution. As in the example above, the problem could be defined as; when can the morphological characteristics of an organ or tissue be linked to the existence of cancer cells? The problem definition phase commonly involves more than one area of science, such as health and technology, in the hypothesis.

The elaboration of the sequence of steps, to answer the problem, is carried out in the second phase. The algorithm follows a specific path to achieve compliance between input and output. This procedure map is then translated into some programming language, enabling the computer to understand and execute the commands. This "translation" is performed by programmers, these are the professionals who write the algorithms or parts of them[35].

How Algorithms Change Reality

Society is changing at the pace of each learning algorithm that is produced. The machine learning is recreating science, technology, business, politics and war. Satellites, DNA sequencers and particle accelerators

The use of these technologies generates information continuously at an unprecedented speed. Increasingly, public and private organizations are producing large amounts of data from different sources. However, the mere existence of this information is not very useful, that is, the data needs to be stored and organized so that they can be processed to add value to them.

Social networks, for example, demand the management of large amounts of unstructured data, generated daily by millions of users in search of sharing information, knowledge and interests[36]. It is precisely here that the importance of analyzing these data and using algorithms emerges.

[34] Idem 32, pp.58-59.
[35] Idem 32.
[36] Idem 20.

The use of "behavioral data" is also used for targeted marketing. Several other services use the same technique, cataloging the user's behavior to, from then on, direct an advertising consistent with their inferred profile. The network user is therefore monitored at all times, accumulating a series of (behavioral) data, which are applied to customize the advertising approach[37].

The accumulation of data creates an informational or *profiling* identity, described by Doneda[38], such as that in which "personal data are processed, with the aid of statistical methods, artificial intelligence techniques and others, in order to obtain a 'metadata', which would consist of the synthesis of habits, personal preferences and other records of the person's life".

According to Rodotà[39], from that point on, the physical body is becoming an access way, because the electronic body, the one formed by the set of personal data and which thus results in metadata of the individual, is the one that matters most for questions of security or actions market share. The natural human body, therefore, is equated with any object, subject to remote observation, monitoring and control, using sophisticated computer systems integrated with satellite and radio frequency technologies.

Advances in data-driven innovation offer new opportunities not only for the private sector, but also for the public, however, they cannot override the fundamental rights of the citizen. To ensure that the use of information complies with fundamental standards, the interaction between innovation and economic growth must be carefully analyzed from the point of view of risk and benefits. In other words, it is necessary to question whether the use of data, to effect public rights and policies, outweighs its potential negative effects.

CONCLUSIONS

In the last decades, much has been discussed about the advantages of using data to improve communication, shorten distances and efficiency in the consumption of services and products in general. Not everything is perfect in the technological age, the use of non-transparent algorithms raises obvious concerns because of two fundamental principles such as the right to liberty and the right to privacy.

It is no longer necessary to discuss whether we are for or against technologies in general, but it is necessary to encourage discussion about the limits, such as transparency, consent and the right to object.

---

[37] B. R. BIONI, *Proteção de Dados Pessoais*: *a função e os limites do consentimento*, Rio de Janeiro: Forense, 2018, p. 20.

[38] D. DONEDA, *Da privacidade à proteção de dados pessoais*, Rio de Janeiro: Renovar, 2020. Eletronic version.

[39] S. RODOTÀ, *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

The data itself is not the big challenge, because it exists regardless of its use, but rather, how it is used and to what extent its use can be harmful or beneficial to the individual and society.
Data surveillance has two sides; one of them, apparently, offers speed, security and protection; the other unnecessarily threatens the individual's privacy. In this discussion, the main concern in the use of technology is the existence or absence of clearly defined standards or regulations.

REFERENCES

ARENDT H., *A condição humana* (Trad. R. Raposo), 10st ed. Rio de Janeiro: Forense Universitária, 2007

BIONI B. R., *Proteção de Dados Pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018

BRUNO F., Máquinas de Ver*, Modos de Ser*. *Vigilância, Tecnologia e Subjetividade*. Porto Alegre: Sulina, 2013

CASTELLS M., *A Sociedade em Rede*, 17st ed. São Paulo: Paz & Terra, 2016

DONEDA D., *Da privacidade à proteção de dados pessoais*, Rio de Janeiro: Renovar, 2020. Eletronic Version

FERRAZ JÚNIOR T. S., "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. São Paulo", *Revista da Faculdade de Direito de São Paulo*, 1993

LEONARDI M, *Tutela e privacidade na internet,* São Paulo: Saraiva, 2011

LÓSCIO B. F., OLIVEIRA Hélio Rodrigues, PONTES, Jonas César de Souza, *NoSQL no desenvolvimento de aplicações Web colaborativas, 2011*, available at: https://www.addlabs.uff.br/sbsc_site/SBSC2011_NoSQL.pdf. Accessed on: 29 março de 2020

JOSE A. N. G. M., *Algoritmos,* Editora Saraiva, Kindle Edition

MORAES M. C. B., *Ampliando os direitos da personalidade. Na medida da pessoa humana: Estudo de direito civil-constitucional*, Rio de Janeiro: Renovar, 2010

MULHOLLAND C. *O., Direito de não saber como decorrência do direito à intimidade – Comentários aos Resp 1.195.995*, Civilistica.com, Rio de Janeiro, jul-sept/2012, available at: http://civilistica.com/wp-content/uploads/2012/09/Direito-de-nao-saber-civilistica.com-1.-2012.pdf. Accessed on: 29 March 2020

PETERSEN J. K., *Understanding Surveillance Technologies: spy devices, their origins & applications*, CRC Press, 2001

PINTO P. M., *O Direito à Reserva sobre a Intimidade da Vida Privada*, Boletim da Faculdade de Direito, Coimbra, v. 69, 1993, pp. 479-585

SCHOEMAN F. D., *Dimensões filosóficas da privacidade,* Cambridge University Press. Kindle Edition

REIS P. V. A., *Algoritmos e o Direito*, São Paulo: Almedina, 2020

RODOTÀ S., *A vida na sociedade da vigilância: a privacidade hoje*, Rio de Janeiro: Renovar, 2008

SOLOVE D. J., *Understanding Privacy*. New York: Harvard University Press, 2008

SOLOVE D. J., *The Digital Person: Technology and Privacy in the Information Age,* New York: Harvard University Press, 2004

THE GUARDIAN, *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* 2013, available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Accessed on: 14 November 2020

THE GUARDIAN, *NSA collecting phone records of millions of Verizon customers daily.* 2013, available: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, Accessed on: 14 November 2020

WARREN S., BRANDEIS L. D., "The right to privacy", *Harvard Law Review*, Cambridge: Harvard Law Review Association, No. 193, 1890