Data Protection in Public Sector: Normative Analysis of Portuguese and Brazilian Legal Orders

Marciele Berger Bernardes[1(✉)], Francisco Pacheco de Andrade[1], and Paulo Novais[2]

[1] Escola de Direito, Universidade do Minho, Braga, Portugal
marcieleberger@gmail.com
[2] Escola de Engenharia, Universidade do Minho, Braga, Portugal

Abstract. Considering that information technology penetrates all areas and domains of the public sector, it has to be considered the extension of the required regulation needed for warranting that this phenomenon becomes an advantage and not a threat. In this sense, this study has as aims to discuss certain aspects associated with fair use of emerging and disruptive technologies and (such as Artificial Intelligence, Internet of Things, Big Data) in the public sector. The emphasis may fall upon the treatment of this subject by traditional regulatory instances, such as Data Protection Regulation-GDPR, in the sense of enhancing the capacity of Governments to ensure privacy, data protection, and the protection of citizens.

Keywords: Data protection in public sector · General Data Protection Regulation · General data protection Law-Brazil

1 Introduction

The introduction of collaborative innovations in urban environments requires an interdisciplinary look. The governmental and technological structures and human beings (living complex organisms under constant evolution) are now integrated by instruments collecting data. These are connected by different sources, under the principle that (non) governmental and private beings interact and exchange information for a better, more sustainable life, with fewer costs and more participated. The fact is that, besides that, cities became massive centers of data collection. So the challenge is clear: how to consider the enormous amount of data produced while respecting the main principles of the fundamental rights to privacy and intimacy? Furthermore, more importantly, how to ensure that the administrations shall use ICTs while placing citizens in the center of these processes, respecting legal security and the person's digital sovereignty.

For answering these questions, this study was divided into three items. First, we presented a review of the literature on Smart Cities, data protection, and privacy. Second, it was presented the normative profile of data protection in both Portuguese and Brazilian contexts. Finally, by a combination of theoretical and practical implications, the research questions in this study were answered. It was suggested the way

Á. Rocha et al. (Eds.): WorldCIST 2020, AISC 1160, pp. 807–817, 2020.
https://doi.org/10.1007/978-3-030-45691-7_76

followed by traditional regulatory instances, such as the General Data Protection Regulation- GDPR, in the sense of enhancing the capacity of Governments to ensure privacy, data protection, and the protection of the citizens.

2 Smart Cities, Data and Privacy: Challenges and Prospects

Unquestionably, street sensors allow to enhance public security levels, and access to high-speed Internet for all populations and the integration between government, corporations, and civil society allow to create a city more accessible for everyone. In the same measure, people are aware that many speeches on the subject are marked with an optimistic view, so often not very critical towards new technologies.

Thus being, difficulties arise as it has to be recognized some emerging concerns that urban centers must face when turning to digital environments. Among the main risks identified by doctrine, it must be considered the issues related to privacy and trust. - It must be considered the potential to create new forms of social regulation with the erosion of privacy and the potential of creating systemic vulnerabilities in the whole infrastructure and the security of data, instead of producing a stable and trustable structure for the citizens.

As it may be noticed, one of the great subjects of debate around Smart Cities is related to the dilemma between the fundamental rights of privacy and publicity and the more and more generalized context in which private data are used as an instrument of municipal public management. Reflecting on this scenario, Edwards [1] points out that cities congregate three central challenges to personal privacy, namely Internet of Things - IoT), Big Data, and cloud computing. The potential impact in the implementation of applications and smart citie's platforms makes it convenient to make a review of the main characteristics of these technologies.

Internet of Things refers to the connection of objects that may be read by machines exclusively identified through the Internet. In the cities, some examples of these are street lights, temperature sensors, noise sensors, sensors of rain and air quality, traffic lights, security cameras, public transportation, and citizen's cellphones. According to the authors, the main elements characterizing the Internet of Things is that data are collected from these objects and sent to citie's platforms or applications to be stored and processed.

Big data is a product of the Society of Sharing (or Informational Society). It is related to the accelerated technological development and with the economic model arising out of it. In a simplified way, big data may be translated as the set of techniques and tools for manipulating and storing a significant volume of data. Among its main characteristics, it may be mentioned: volume, a great quantity of data generated, variety, data from different sources and with different structures, and speed, being that many services depend on fast processing or even of real-time processing.

New tools of Big Data in smart cities were made possible thanks to the widespread use of devices and sensors, based on technological structures, which allow cities to become important data collecting centers.

So, it is worth to refer that, in the context of smart cities, Big Data includes all actions and communications in digital platforms. From the more simple ones (as the

use of cellphones, laptops or even the recognition of patterns in traffic, using historical data, the forecast of quantities of electrical energy in different days and schedules, using the flows of data in real-time, and the forecast of the use of public transportation), to the detection of public security problems, arising out of monitoring through security cameras.

Concerning cloud computing, it is a "new modality of services provision, through the use of internal and external servers, allowing omnipresent access to a wide range of services and resources," that is to say that it includes the infrastructure for the storing and processing of data. Among its essential non-functional requirements for smart cities, Kon and Santana [2] point out the cloud of things (storing and processing of data from sensors in an environment of cloud computing) and sensing as a service (infrastructure in charge of the provision of data from the sensors to applications as services in the cloud).

Based on this, mainly considering the almost instantaneous possibility of storing, processing, and distributing information, new theories arise on the better grounding of decisions based on data analysis by governments. Thus, decisions may have a better grounding, and so lead to a "radical increase in the efficiency of processes and allocation of resources. Including the detection of failures and fraud".

Meanwhile, as it was noticed by Pierre Lévy [3], "to digitalize an information is just to translate it in numbers". And this leads to legal reflection related to the object of this research. That means that we must consider that the (wrong) use of technologies may create unbalances or even violations of rights. By the way, it is worth to refer that the previous warning and the consent of the citizen – holder of rights – are considered to be the cornerstone of data protection and privacy. However, they may become weakened in the context of Smart Cities.

The imminent risk of this was already pointed out by Lawrence Lessig [4] when he clarified that depending on the use; such devices make possible a permanent and tendentially integral control of the persons: "The struggle in this world will not be on the government. It will be to warrant that essential freedom is preserved in this environment of perfect control".

In the face of this dilemma, some issues arise: everyday rights will be (re)negotiated with the State and with the new emerging economic model. So, different questions come to our minds, among which: whose rules to apply to public powers? How should be the consent of the holder of rights? What is the responsibility of public power in the personal database's management? To what sanctions must public powers be subject? In search of answers for these questions, it was considered, in the next item, the normative analysis in Portuguese and Brazilian legal orders.

3 Portugal and Brasil: Normative Profile of Data Protection

Professor Ernesto Valdés [5], in work under the title "Privacy and Publicity," reasons on different situations in which it is alleged that there is a violation of the private sphere, according to social norms.

Still in the North American scenario, it is worth remembering the news of 2013, according to which National Security Agency – NSA intercepted domestic telephonic

calls and collected its data, through the Internet. NSA also intercepted calls of non-American persons and even from other country's governments. These revelations on surveillance arose form documents of the North American government, revealed by Edward Snowden (ex NSA agent), concerned with the collection of data by the American government.

This kind of issue requires clear policies and contínuos deliberative processes and updating. In the age of Big Data, as cities and administrations use more and more data to generate operational and political advances, it must be considered the security of data and the rules on warranties of anonymity. Thus being, it is required an analysis of the legal solutions identified in the European Union (Portugal) and Brazil in order to face possible threats to privacy in smart cities.

From this perspective, we must refer to the work of Schönberger [6], who points out four different generations of data protection laws in Europe. The first generation reflected the technological framework of the time and aimed at controlling technology, regulating the authorizations for the creation of databases. One of the critical points in this period was the 1970 Hesse (german state) data protection law. The normative motivation occurred as a reply to the alleged technological threat, characterized by generality and abstraction, which has lead to a quick mismatching in front of the quick multiplication of data processing centers.

The second wave of the European normative has as exponent the french law on data protection (1978) being its main characteristic a change of paradigm: the focus was not anymore on providers and went to citizens. Citizens were supposed to identify the undue use of their personal information and to propose its protection. The main obstacle was that citizens were forced to choose between social exclusion and the provision of their data.

In the 1980s, arises in Europe, the third generation of laws, focused on the citizen, but with a sophisticated guardianship based on the right to informational self-determination. As an example of this, we may refer to the Norwegian Law on Data Protection. Finally, the fourth generation, referred by Schönberger [6], tried to overcome the disadvantages of the individual focus, stating that data guardianship may not restrict individual choices of the citizens: laws are required to enhance the collective pattern of data protection.

In the context of the European Union, we must refer to the European Directive 95/46/CE, created with a double aim: to support the creation of a normative mark of data protection and the free circulation of data among the member states. It is still to be referred that, as a result of the transposition of such Directive, it was issued in Portugal the Data Protection Law (Law n.º 67/98).

As the years went by, the reffered norms became clearly not enough to assure the needs of data protection, as the reality was quickly changing, also in the different Member States of the EU, and modernization and a unique legal act was required in order to "reinforce the fundamental rights of the persons in the digital age (…) thus ending with fragmentation and the costly administrative charges". This scenario of

normative mismatching and of technological evolution lead to the approval of Regulation (UE) n.º 2016/679 General Data Protection Regulation-GDPR[1], concerning the protection of individuals in what concerns personal data processing and the free circulation of data.

According to Ronaldo Lemos [7], this framework evidences the role that Europe is performing to become a regulatory superpower (not just considering data protection but also subjects such as Intellectual Property and Competition Law). Furthermore, as the Author refers it, two primary and visible effects of the Regulation are visible. The first one is a macro aspect. The fact that Europe implemented such a Regulation enhanced the adoption of data protection laws in other countries, such as Brazil. The second one is a micro aspect. "Every Corporation working with data will have to take into account GDPR – even if they do not have a siege in Europe."

Considering that the focus of this paper falls upon a comparative analysis of the Portuguese and Brazilian scenarios, it is convenient to do a brief review of GDRP (now the main rule for data protection in Portugal). And of the Brazilian Data Protection Law (whose contents were inspired in the European model).

3.1 General Data Protection Regulation (GDPR)

Following logic Viktor Schönberger's [6], on the different generations of data protection laws in Europe, above referred, it is believed that GDPR may be classified as the fifth generation of European Legislation on Data Protection. It must be clarified that the said study is from 1997, and thus it could not have foreseen the appearance of the European Regulation. Yet, in a recent study by Schönberger and Kenneth [8] it was stated that data are for Informational Society as fuel was for Industrial Society. The authors have warned that there is a risk of the outcome of what they called the "Barons of the Big Data" in the 21st century, as it happened with the "Barons of Rubber" in the XIX century, who dominated railroads, metallurgy and telegraphic networks in the United States.

So, for these authors, in the age of Big Data (in which it is not possible to foresee the extent of technological evolution), the challenge is to develop measures that allow transactions of data. Thus, thinking analogically, Schönberger and Kenneth suggest a strategy of identification of general principles for a regulation of the subject. in order to ensure the safeguard of minimal rights.

Given this context, GDPR starts to show itself, having as legal support the following instruments. The Treaty on the Functioning of the European Union - TFUE (article 16); the Chart of the Fundamental Rights of the European Union (articles 7 and 8); the Convention 108 of 1981, "the first international instrument legally binding adopted in the domain of data protection"; the European Convention on Human Rights - ECHR (article 8); the Treaty of Lisbon, "providing a more solid base for the

[1] GDPR came into force on the 25th may 2016 and became fully applicable on the 25th may 2018. It expressly revoked Diretive 95/46/CE and, being an European Regulation, it is mandatory and directly applicable in all EU State Members, thus replacing Portuguese Data Protection Law in all that is not compatible with tghe Regulation. (articles 94. º and 99 of GDPR).

development of a more efficient and clear system of data protection"; the Directive 95/46/CE –"concerning data protection."

Out of these arose GDPR, which has gone through, until its full applicability, important temporal steps. 2012 (in January, it was presented the initial proposal of Regulation of data protection by the European Commission). 2014 (in March, the European Parliament approved its version of the Regulation). 2015 (in June, the Council of the European Union approved its version and, in December, the Parliament and the Council reached an agreement); 2016 (in May, the Regulation was approved). 2018 (after two years, GDPR became fully applicable all over the European Union on the 25th of May 2018).

It may be said that GDPR had several aims[2]: the harmonization ("being the Regulation directly applicable in all Member States, there is not the need of a national legislation in each Member State"); the expansion of reach (" the Regulation is applied to all the organisations acting within the European Union […] and also the ones with siege outside of EU but that monitor and/ or offer services and goods to individuals in the EU"); the unique schema/ "one-stop shop" (a new concept o fone stop shop "means that the organizations will have just to deal with one only supervising authority, […] making it simpler and cheaper for corporations making business in the EU").

GDPR also presentes new concepts and some other, already existing, were considerably revised. It is to be noted, among others, the following ones: personal data (article 4, nr.1, GDPR); special category of data (article 4 nrs. 13,14,15 and article 9 GDPR); vilation of personal data (article 4, nr. 12, GDPR); pseudonimisation (artigo 4, nr. 5, GDPR); right to the erasure of data "right to be forgotten" (article 17, GDPR); privacy by design (article 25, nr.1 GDPR); privacy by default (article 25, nr. 2 GDPR), right to the portability of data (article 20, GDPR) and thw agentes of the treatment ("Responsible for the treatment" and "Subcontracor", article 4, nrs. 7 and 8, GDPR).

So, it will be subject to GDPR, every person "natural or collective person, public authority, agency or other organism receiving communication of personal data, regardless of being or not a third party" (article 4, no. 9, GDPR). Concerning the range of its application, GDPR states possibilities for material application, focusing on all those who treat personal data by means totally or partially automatized, including all public and private entities (article 2 GDPR). The range of territorial application includes those residents in Europe and corporations processing data of persons located in the European territory (article 3 GDPR). Besides that, the possibilities of exclusion of the application of GDPR are mentioned in article 2 nr. 2 GDPR.

It must be said that GDPR was built considering certain principles, such as lawfulness, loyalty, transparency", "limitation of purpose", "data minimization", "accuracy," "limitation of conservation" and "integrity and confidentiality" (article 5 GDPR).

All this keeps a deep connection with the rights of the holders of data for the exercise of the subjective right of data protection, present in chapter 3 GDPR. 1) the right to be informed – access to information on the processing. 2) the right of access –

[2] That, in a general way, were built on the base of the argument that it is up to the European Union to ensure that "the fundamental right to data protection, established in the Chart of Fundamental Rights of the European Union is applied in a coherent way (…), specially in a world society characterised by quick technologial changes".

access to personal data stored by the controller. 3) the right to rectification – correction of any nonconformity concerning the processed personal data (article 16, GDPR). 4) The right to erasure or "right to be forgotten" – exclusion of data stored or processed (article 17, GDPR); 5) The right to portability – transfer of data to another (article 20, GDPR); 6) The right to the objection of treatment – temporary restriction to the processing of personal data (article 4 nr. 24 GDPR).

GDPR also provides a modernized framework of compliance based on responsibility concerning data protection. It was thus included a new figure of the Data Protection Officer[3]. For this aim, DPOs assumed a central role in the normative framework, as participants of the system of data governance.

It must be noted that GDPR does not define what authority or public organism are, leaving this task for the national legislator in each member state of the EU. For this purpose, the Portuguese Proposal of Law nr. 120/XIII, in article 12, nr. 2, assumes as public entities: a) the State; b) the autonomous regions; c) the local authorities; d) the independent administrative entities and the Bank of Portugal; e) the public institutes; f) the institutions of public higher education of foundational nature; g) the public enterprises on legal public form; h) the public associations.

Besides that, DPO must be selected in accordance to his legal and specialized knowledge in terms of data protection (article 37 nr. 5, GDPR), without forgetting the capacity to perform the functions referred by article 39 (computer skills), evidencing the multidisciplinary character of this figure. He may perform several tasks referred on article 39 nr. 1, GDPR, consisting of supervision and monitoring of the internal application, ensuring respect for data protection norms.

For exercising this function, DPO must be independent and can not receive instructions of the controller or processor in what the performance of his tasks is concerned. He can not be dismissed or penalized for performing his tasks, and he may perform other functions within the Corporation (provided that there is no conflict of interest). Still, the DPO may be an internal collaborator or an external agent, hired as a services provider (articles 37 nr. 6 and article 38 nr. 6 GDPR).

The efficacy of the GDPR is still bound to the creation/designation of an entity, namely the Independent Control Entity (article 51, GDPR), with several attributions (article 57 GDPR), having even the power to investigate and imposing sanctions (article 58 GDPR). For the prosecution of these functions, they must act with total independence. Furthermore, GDPR brought along a new paradigm: it allowed the relationship between authorities of control, through the cooperation in trans-border treatment (article 56 GDPR). In Portugal, the role of the "Authority of Control" is in

[3] According to the Working Group of Article 29 [9], the concept of DPO is not new, since the "Directive 95/46/CE3 did not oblige any organization to designate a DPO but still the practice of designating a DPO was being developed in several member states along the years.". Furthermore, the referred Working Group mentions that the main aims of DPO are to "ease the conformity through the implementation of responsibilization instruments (for instance, making it viable evaluations of data protection impact, and making or audits)" and also serving as "intermediaries between the interested parties, for instance, authorities of control, the data holders and the entrepreneurial units within an organization".

charge of CNPD – National Commission for Data Protection, following article 3 of the Proposal of Law 120/XIII.

Once occurring a treatment in violation of personal data – for instance, not complying with the basic principles of treatment (not having the consent of the client, or violating the holder's rights) sanctions will be applied (article 82 GDPR). The Regulation includes a list of staggering financial sanctions. The most significant alteration was the establishment of higher sanctions for the responsible for the treatment and the subcontractor not complying with the established rules. Some violations are subject to sanctions that go to 20 million euros or, in the case of a Corporation, to until 4% of its annual business volume (article 83 nr. 5 GDPR).

At last, it is convenient to remind that GDPR does not arise out of nothing, to safeguard "as in magic" all the individual rights of data protection. However, instead, it evidences the long road taken by the EU towards the guardianship of these rights, each day threatened by technological transformation and, so, requiring permanent normative updating. Regardless of the Regulation's impact, all the EU member states already had legislation directed to the treatment of data. The Regulation was an opportunity to revise and to uniformize the treatment of data according to the principles of data processing and especially "limitation of purposes."

3.2 Brazilian General Data Protection Law (GDPL)

The road towards the approval of the Brazilian General Data Protection Law [10] was not supported neither in a wide normative framework, nor in an updating of previous legislation on data protection. Considering the total absence of legislation, data protection in this country was promoted based on constitutional interpretation (article 5 § 2 CF/88) and in co-related legislation (Law on Access to Information - Law nr. 12.527/11 and "Marco Civil da Internet – Civil Mark for Internet" – Law nr. 12.965/14).

In front of this, it was presented the Brazilian GDPL, whose way until approval went through the following: 1) 2010 (Draft Law elaborated by the Ministry of Justice through the public debate). 2) 2012 (presentation of the Project of Law nr. 4.060/12 by the Chamber of de Deputies). 3) 2013 (presentation of the Project of Law nr. 330/13, by the Federal Senate). 4) 2015 (new draft elaborated by the Ministry of Justice went to public debate). 5) 2016 (Project of Law nr. 5.276/16 was sent to the National Congress); 6) 2018 (The General Data Protection Law was approved on the 14th August 2018 and, after 18 months, it will get into force and thus will be applied in the whole Brazilian territory).

It may be affirmed that the brazilian GDPL had a Strong influence of the european model, starting with basic concepts, such as: personal data; sensitive personal data; anonimised data; treatment agent, article 5 GDPL.

Other subjects were inspired in GDPR, such as the right to be forgotten "elimination of personal data" (article 18, GDPL). Data protection, since the conception ("it determines the adoption of security, technical and administrative measures, adequate to protect personal data, from the phase of the conception of the product or the service to its execution"), article 46, §2, GDPL.

From this perspective, GDPL is applied to any operation of data treatment performed by natural or legal persons (of public or private law), according to any of the following requirements. 1) data collected and treated in Brazil; 2) data having as holders individuals located in Brazil; 3) data having as purpose the offering of products or services in Brazil (article 3 GDPL). The possibilities of exclusion of GDPL application are mentioned exhaustively in article 4: a natural person for personal private purposes; aims exclusively related to journalistic, artistic or academic purposes; public security; data "in transit."

Just as its inspiring model, GDPL is based on a series of principles directed towards the treatment of data, such as: "finality, adequation, need, free access, quality of the data, transparency, security prevention, non-discrimination, responsibilization and accounting" (article 6 GDPL).

GDPL assumes consent as a "free, informed and unequivocal manifestation, from which the holder agrees with the treatment of its personal data for a determined purpose" (article 5 XII GDPL). Besides that, two possibilities are established for the consent of the data holder: (i) written consent or (ii) by any other mean demonstrating the will of the data holder, such as a checkbox of the privacy policy (article 8 GDPL).

In front of that, GDPL establishes the following individual rights: the right to be informed; the right to rectification; the right to the portability of data; the right of access; the right to the exclusion of data; the right of the revocation of consent (article 18 GDPL).

It is also included in GDPL, the figure of the Data Protection Officer (DPO), who must be indicated by every data controller. The "identity and contact data must be disclosed publicly, clearly and objectively, preferably in the electronic site of the" (article 41 §1 GDPL).

As it happened with the European model, the corporations willing to adopt a broader pattern of protection of data must strongly consider the to hire a Data Protection Officer. Besides that, some critical practical aspects were not considered in GDPL. Such as: the qualification required for the DPO (technical and/or legal), the need of certification and the possibility of accumulating functions.

As well as GDPR, the efficacy of GDPL in Brazil is bound to the creation of an entity responsible for auditing and ensuring the compliance with the Law. Fot that, the figures of "National Authority on Data Protection (ANPD)" and of the "National Council of Privacy and Data Protection" were established in articles 55-A to 58-A of GDPL[4].

ANPD was projected as a Federal Local Authority, bound to the Ministery of Justice. Its regulation and organizational structure would be regulated by Presidential Decree. Within its attributions, it may be referred the elaboration of orientations for the National Policy of Data Protection. But also the supervision of the compliance to the law and application of sanctions, the fulfillment of requests by holders of rights against controllers; lawyering; advocacy; to publicize regulations and procedures for the protection of personal data and the elaboration of reports on the impact of personal data protection.

[4] Wording given by Law nº. 13,853 of 2019.

Besides that, there are four main pillars on which ANPD would act, and these still are considered in GDPL: security of data, treatment of incidentes, reparation of damages, and sanctions.

Thus being, in case of non-compliance with the GDPL, ANPD would be the entity responsible for the application of administrative sanctions. Among these sanctions, there is the possibility of warnings, fines, or even the total or partial prohibition of activities related to data protection. Fines may go up to two percent of the billing of the private law legal person, or entity's group in Brazil, in the last exercise, excluding the tributes and limited, in total, to fifty millions of reais per infraction (article 52, GDPL). Still, there is the possibility of daily fines to compel the entity to end with such violations.

From the above exposed, it may be said that GDPL keeps many similarities with its inspiring model, GDPR. Many challenges must be transposed for adequate data protection in Brazil. However, it must not be forgotten that the referred Law inaugurates a new era in the guardianship of the rights of the citizen and inclusion of Brazil in an international eco-system – a new regulation of information and data.

Final Considerations

As it was seen, smart cities launches new challenges to human rights, such as the scale of privacy and intimacy that may be harmed[5] by the distortion of the use of the technology for an "intelligent" policing.

As it was analysed, EU is assuming the iniciative of adequation to this new scenario, from its historic efforts and recently by the approval and entrance into force of the General Data Protection Regulation, a concrete opportunity for citizens to regain some data sovereignity, mainly through the concern with the guardianship of the fundamental rights, serving this as a norm for the Portuguese State and as an inspiring model for the creation of the Brazilian GDPL

However, one thing is the theoretical debate on smart cities (use of data for improving and enhancing governance and participation) and the normative prevision (Law on Data Protection, Law on Access to Information, …), and another issue is its practical application.

Acknowledgments. This work has been supported by FCT Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2019.

References

1. Edwards, L.: Privacy, security and data protection in smart cities a critical EU law perspective. Eur. Data Prot. Law Rev. **1**(2), 28–58 (2016)

[5] The above listed is justa n example but, it may be thought as an alert for the fact that, in smart citie's programmes, the debate goes beyond the "mere" use of data. As Teresa Moreira and Francisco Andrade say [11]: These Technologies bring along the risk of an intensive use of personal data. We are confronted with a real threat of constant treatment of personal data, which leads us to the overwhelming perspective of a progressive transformation of persons into electronic persons, while object of constant monitoring (or surveillance) by a growing number of informatic applications.

2. Kon, F., Santana, E.: Cidades Inteligentes: Conceitos, plataformas e desafios. In: 35º Jornada de Atualização em Informática, Porto Alegre, Brasil (2016)
3. Lévy, P.: Cibercultura. In: Paulo, S. (ed.) Tradução Carlos Irineu da Costa, vol. 34 (1999), p. 92
4. Lessig, L.: Code Version 2.0, p. 4. Basic Books, New York (2006)
5. Valdés, E.: Privacidad y publicidad, vol. 1, pp. 223–244. Doxa, New York (2006). ISSN 0214-8876
6. Schönberger, V.: Desenvolvimento Geracional da Proteção de Dados na Europa. In: Agre, P., Rotenberg, M. (eds.) Tecnologia e Privacidade: The New Landscape, pp. 219–242. MIT Press, Cambridge (1997)
7. Lemos, R.: A GDPR terá um efeito viral. In: Meio e Mensagem. (2018)
8. Schönberger, V., Kenneth, C.: Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. In: Paulo, S. (2013), p. 130
9. European Union. REGULATION (EU): 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=pt
10. Moreira, T.C., de Andrade, F.P.: Personal data and surveillance: the danger of the "homo conectus". In: Intelligent Environments (Workshops), pp. 115–124 (2016). Brazil, Lei Geral de Proteção de Dados Pessoais (GDPL). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm