INTERNATIONAL JOURNAL OF DIGITAL AND DATA LAW

REVUE INTERNATIONALE DE DROIT DES DONNÉES ET DU NUMÉRIQUE

Vol. 7 - 2021

ISSN 2553-6893

IMODEV
LES ÉDITIONS

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article
n'engagent que leur auteur.

The statements published in this article
are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

THE RIGHT TO EXPLANATION IN BRAZILIAN DATA PROTECTION LAW

by **Renato L. MONTEIRO**, Lawyer, Director of Data Privacy Brazil;
Caio V. MACHADO, Lawyer and Social Scientist, Collaborator at IMODEV (Brazil), Director of Instituto Vero
and **Leoncio SILVA**, Social scientist, BCL Candidate at the University of São Paulo

Brazil has passed a few, but highly relevant, laws related to the internet and similar modern technologies. On the one hand, the country seems to have been quite innovative in approving some key legislation that has been protective of online liberties. On the other, it seems that Brazil always lags behind on certain key issues. The most notable of these laws has been Law nº 12.965, approved in 2014, the *Marco Civil da Internet*, known in English as the Brazilian Internet Bill of Rights, which established a number of individual and collective online liberties. The law has been much praised for its innovative approach to internet regulation and the fact that it is highly averse to the criminalisation of the internet and highly protective of internet liberties, with a strong focus on the protection of freedom of speech and privacy.

In 2018, Brazil took a step towards regulating data protection in a general sense. Propelled by the establishment of the European General Data Protection Regulation (GDPR) in the same year and the Cambridge Analytica scandal, the Brazilian Congress approved a data protection Law that had been debated in Congress for almost ten years.

The Brazilian Law nº 13.709, called *Lei Geral de Proteção de Dados,* or simply the LGPD (General Data Protection Law), was approved in Congress in 2018, but that was not the end of the discussion and there was turbulence involved in its coming into force. Since Data Protection and Privacy culture are still very underdeveloped in Brazil, many Brazilian companies, political groups and even civil society organisations failed to recognise the urgency in quickly applying the Law. Moreover, since there was little protection already in place in the country, adaptation meant heavy costs for businesses and organisations.

For these reasons, even after its approval, there was intense resistance to the LGPD, and there were many manoeuvres to attempt to postpone its application. First, it was scheduled to come into force 18 months after the approval of the Bill. This later became 24 months. With the COVID-19 pandemic in 2020, a group of Congressmen tried to push the implementation of the

Law back yet another year[1]. Even the Executive Power stepped in, trying to postpone the Law via Presidential Decree. These multiple struggles caused enormous uncertainty, so that people could not really affirm the applicability of the Law. Fortunately, today, it seems that issue has been mostly settled. The Law came into force in September 2020, and its penalties will be applicable from August 2021[2] – an odd solution, which hints at a gradual application.

At a first glance, one might think that the LGPD is an attempt to copy the European statute. Indeed, the pieces of legislation have many similarities, and they have been inspired by the same set of principles and rights that underpin privacy and data protection. However, one must note that the Brazilian Law also has many peculiarities, most interestingly, for this discussion, a strong basis to support the existence of a Right to Explanation.

The LGPD's text includes elements that provide a strong case for the Right to Explanation in the Brazilian Legislation. This Right can be defined as the right of an individual or collective to demand that the operator of an automated decision system provide an explanation as to why the automated system has produced a determined output. In other words, it is an entitlement to know and understand the reasoning and criteria that are encoded within a system's algorithm.

Such a Right also entails extra-legal obligations, affecting the ethical and technical spheres of automated decision-making. In order to conform with this obligation, developers need to take measures to ensure that the data subject has substantial means of requesting and understanding the explanations, which means adapting designs, interfaces and even policies.

Also, emerging technologies and their great potential for the automation of a large number of activities that can affect individual and collective rights have raised the issue of the establishment of an informational due process.

This article presents, in Part I, the relevance of this new Right in the context of massive data processing, indicating the relevant statutes and revealing the legal arguments for the existence of a Right to Explanation in Brazil; it also argues why emerging technologies demand an informational due process for protecting individual and collective rights. Part II presents legal precedents for the Right to Explanation in the context of consumers' rights and discusses the development of data protection in the courts, culminating in recent decisions that have recognised informational self-determination as a fundamental constitutional right. Part III argues that the interpretation of the LGPD and relevant court

[1] R. MACHADO, *Proposta adia para 2022 a vigência da Lei Geral de Proteção de Dados Pessoais*, Agência Câmara Notícias, 2020: https://www.camara.leg.br/noticias/626827-proposta-adia-para-2022-a-vigencia-da-lei-geral-de-protecao-de-dados-pessoais/ accessed on 8 December 2020.

[2] Editorial, 'Lei Geral de Proteção de Dados entra em vigor' (*Senado Notícias*): https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor, accessed on 8 December 2020.

decisions leads to the conclusion that data protection law should be seen within a procedural justice context and proposes a framework for procedural due process in automated decision-making.

§ 1 – The Concept of Data Protection in the LGPD

A) An Extensive Concept of Personal Data

Brazilian legislation has long upheld privacy as a value, and it is even protected in the Brazilian Constitution of 1988, in Article 5º. However, unlike many European countries that had this discussion in the late 70s and 80s, data protection in Brazil did not appear within the scope of privacy until the 2000s. This means that although privacy is an established right in Brazil, privacy in terms of data protection is a fairly new concept in Brazilian legal culture. The right for Data Protection in Brazil has largely stemmed from the same framework of fundamental rights, which includes a set of individual liberties and human dignity that forms the core elements of informational self-determination.

There were no general laws governing the custody of data, except sectoral rules which might have been created for one reason or another, such as Labour obligations as to the privacy of workers or confidentiality arrangements in the financial markets. Personal data had no clear legal status in Brazil and was not even considered as a property right, which were the earlier forms of data regulation that came into force around data protection.

With the expansion of the internet and the growing need to govern personal data, Brazil drew closer to the European discussions, understanding that data protection resulted from the right to privacy and self-determination. Privacy became increasingly understood as a personality right that set limits on data collection established contractually due to a growing need for data protection as a form of privacy. For these reasons, there are strong similarities between the legislative approaches recently adopted in the Brazilian and European laws.

One of the key similarities is the definition of Personal Data, a core element of data protection legislation. Both the GDPR and the LGPD consider Personal Data as "information related to an identified or identifiable person"[3]. The term "identifiable" provides considerably wide scope for legal protection, governing not only information that is directly linked to an individual, but also any information that could *potentially* be attributed to an individual, or that, combined with other pieces of information, could be related to a natural person.

At this point, the LGPD goes a step further and widens the scope of personal data that is defined by the European statute. The

[3] "Art..5º For the purposes of this law, it is considered:
I Personal data: information related to an identified or identifiable natural person" (Translated by the authors).

Brazilian Law has an additional provision in the context of anonymised data, which, in the first instance, would not come within the scope of personal data; it asserts that anonymised data can also be considered to be personal data if they fall within the scope of data used for the behavioural profiling of a natural person[4]. For example, data related to a group or clusters, or that are non-identified, are deemed to be personal data if they are processed for the purpose of creating a behavioural profile of a natural person.

This expansive approach adopted by both statutes raises the issue of the boundaries of personal data, which initially were conceived only as the information collected directly from the individual. However, a close reading of the definition suggests that the method of data collection is not part of what constitutes personal data in the eyes of the LGPD. This is an important observation, because it changes the focus from the flow of data from the individual to the processor, to the mere fact of holding information *about* the individual and the impact that the use of such data can have on the individual.

It must be remembered that both statutes provide the data subject with a series of rights and protections regarding the processing of personal data. Most relevant provisions include the principle of transparency, the right to be informed, the right to access the data and the right to know the criteria used in automated decision-making.

The right to be informed and the right to access are considered basic elements for data protection. Since the first legal instruments of data protection, legislation has established some essential elements regarding the data subject's right to know about the processing of their data, the purpose of the treatment and the type of data used. Together, they could be called a "right to know". They represent the central element that allows the data subject, the person, to have control over the data processing, common to the first privacy and data protection regulations, through which the regulator aims to ensure openness and transparency in order to discourage agents from acting in violation of certain norms and to prevent unfair use. Furthermore, openness and transparency allow correction of personal data[5] and opposition to certain types of processing.

[4] "Art. 12º. Anonymised data will not be considered personal data for the purposes of this law, except when the process of anonymisation by which the data were submitted became reverted, by own means, or when, with reasonable efforts, it could be reverted.
§ 1º The settlement of what should be considered as reasonable must take into account objective factors, like the cost and time required for reverting the anonymisation process, according to the available technology, and the exclusive use of own means.
§ 2º Also considered as personal data, for the purposes of this law, would be those used for generating a certain natural personal behavioural profile, if identified." (Translated by the authors)

[5] For a presentation of the main regulatory approaches in early data protection regulations see: Collin Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States,* Cornell University Press 1992, pp. 153–192.

A type of right to access, developed in earlier data protection legal instruments, appeared in the Brazilian legal system in the federal Constitution, in a procedural right called *Habeas Data*. In Art. 5°, LXXI, the Brazilian *magna carta* dictated that the Judiciary would grant *habeas data* to ensure knowledge of information related to an individual on public entities' archives or databases. This constitutional right may be seen as an outcome of the democratisation process of the 80s, following Latin American dictatorships. Initially focusing on individuals' rights infringements by public authorities, courts' decisions extended to include other databases, such as consumer protection databases controlled by data brokers, since these could be seen to be in the public interest[6]. Two years after the 1988 Constitution, consumer law, through the Consumer Protection Code (Federal Law 8.078/90), recognised that consumers have the right to access and correct their data with help from consumer organisations. Further regulation in 2011, which will be further discussed in this article, set rules for consumer databases and credit scoring methodologies. However, there was no general provision for people to know how their data were used, beyond sectorial laws. Transparency has become very important in the context of legal instruments like the Internet Bill of Rights, but it is the LGPD that has definitively filled this gap within the Brazilian legal system. The regulation established such rights and requirements for notification in Art. 18° and Art. 9°.

EU directives and the GDPR later introduced some new provisions for the effective control of data and established a new model for regulation. Both European documents have recognised some new rights for the data subject, such as the right to know the criteria of automated decision-making and the revision of such decisions. In addition, they created enforcement mechanisms based on authorities with enforcement powers supervising data processing according to the terms of the regulation.

Brazilian regulators followed this model, although there are relevant differences between the two statutes. The current paper focuses on new rights in the context of automated decision-making. The European regulation, for instance, on Art. 22°, establishes the right for an individual not to be subjected to solely automated decisions. The Article prescribes exceptions where the data subject cannot oppose the treatment of their data. When the processing comes under such exceptions, the Article established the right for human revision. As can be seen, the equivalent European Article restricts automated decision-making, providing data subjects with the right to object to the processing.

Brazilian Law, on the other hand, in Art. 20°, merely prescribes the right to a revision, with no requirements for human oversight or restrictions on automated decision-making. There is no right to object to the processing *per se*. It is important to note that, despite firm constraints, the GDPR Art. 22°, paragraph 2, lists generous

[6] *RExt n 673707/2015 MG.*

exceptions which make it possible for the controller to make automated decisions, so that the two regulations may lead to similar outcomes.

Based on a systematic analysis of the provisions for control and revision of automated decisions, combined with the transparency obligation provided by both regulations (in Art. 13°, 14° and 15° in the GDPR and Art. 9° in the LGPD), some authors have argued for the existence of the right to an explanation[7]. The argument for the existence of the Right is reinforced by authorities' recommendations and guidelines for Explainability in algorithmic decision-making[8]. In the Brazilian case, it is possible to make a strong case for Explainability, since Art. 20° establishes the principle that the data controller should give the data subject clear and appropriate information about the criteria and procedures used in the decision every time the subject requests it. When the controller refuses to provide such information, the national data protection authority can request an audit of the data processing[9]. The audit will depend on the structural and technical capability of the authority.

The extent and remit of this right, however, will depend on further interpretations by authorities and courts. For instance, the concept of solely automated decision-making may lead to the exclusion of a large number of applications with a minimal human oversight in

[7] B. CASEY, A. FARHANGI, R. VOGL, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, Social Science Research Network 2018, SSRN Scholarly Paper ID 3143325: https://papers.ssrn.com/abstract=3143325, accessed on 27 May 2020; B. GOODMAN, S. FLAXMAN, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'", 38 AI Magazine 50, 2017; M. E KAMINSKI, '*The Right to Explanation, Explained*, Social Science Research Network, 2018 SSRN Scholarly Paper ID 3196985: https://papers.ssrn.com/abstract=3196985, accessed on 27 May 2020; G. MALGIERI, "Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations", 35 *Computer Law & Security Review* 105327, 2019; A. D SELBST, J. POWLES, *Meaningful Information and the Right to Explanation*, Social Science Research Network, 2017, SSRN Scholarly Paper ID 3039125: https://papers.ssrn.com/abstract=3039125; accessed on 27 May 2020.

[8] ICO and ALAN TURING INSTITUTE, *Explaining Decisions Made with AI:* https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence, accessed on 5 June 2020.

[9] "Art. 20º. The data subject has the right to request the revision of decisions made exclusively based in automated personal data processing that should affect his interest, including the decisions intended to define his personal, professional, consumer and credit profiles or aspects of his personality.

§ 1º The controller must provide, when requested, clear and appropriate information about the criteria and procedures used for the automated decision, taking into consideration trade and industrial secrets.

§ 2º When the information described in § 1º is denied based on trade or industrial secrets, the national authority could perform an audit verifying discriminatory features related to the automated processing of personal data." (translated by the authors) which the human plays an almost insignificant role[10]. Even the meaning of 'human revision' depends on further developments[11].

Furthermore, the meaning of 'personal data' can play an important role in the protection of people's interests and fundamental rights. Since technical developments and the widespread use of information technology have created new business models, with extensive collection and use of personal data, experts have signaled the emergence of risks and harms for privacy and self-determination. Some have called for more stringent control over data processing, beyond data protection regulation, in the face of counter-intuitive inferences about people's characteristics and behaviour, which has the potential to harm people's privacy and right to self-determination. These observations should also apply to the Brazilian context.

An important paper, by Sandra Wachter and Brent Mittelstadt, indicated the limits that exist on current data protection regulations for big data and artificial intelligence[12]. The authors recognised that the expansive concept of personal data contained within the European regulation includes inferences derived from data processing. However, the legal implications of this concept remain unclear. The paper showed that the statistical nature of inferences may inhibit data subjects' ability to control or correct information. For instance, transparency obligations allow subjects to know about the inferences, through the notification duties contained in Art. 13º and 14º, but this does not include inferred data.

In addition, the nature of inferences may present a barrier. If Art. 16º allows subjects to amend incorrect or incomplete data, some precedents have provided a restricted view. The requirement for correction is that the information must be verifiable. It can be argued that one cannot verify inferences about the future. Moreover, for inferences, the regulation gives more protection to intellectual property and trade secrets, thus setting boundaries for data protection rights. For automated decision-making, this can make a big difference.

The authors concluded that current privacy and data protection regulation did not provide sufficient protection for people, but just for the data itself. The development of a more holistic approach to data protection was required, including certain rights in relation to what are considered *reasonable* inferences, *i.e.* the right to control which inferences are allowed to be drawn from data related to a

[10] For a discussion on perspectives on the interpretation of solely automated decisions and human revision see: Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2903469 <https://papers.ssrn.com/abstract=2903469> accessed on 27 May 2020.

[11] In the European context, the Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (2017), from the Article 29 Working Party, suggest that a human intervention must be meaningful.

[12] S. WACHTER and B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI,* 12 October 2018: https://osf.io/preprints/lawarxiv/mu2kf/, accessed on 27 May 2020.

person. It can be argued that privacy and data protection regulations should lay the foundations for an informational due process.

B) The Need For an Informational Due Process

Due process is one of the core notions in democratic societies. It has been incorporated as one of the guiding principles of procedural law, being one of the most basic rights of the individual. Among the democratic countries of the world, law has offered elements of procedural process that can vary according to the interests of the parties involved in a given decision[13]

Using a systematic interpretation, the GDPR and the LGPD have established a framework that goes beyond a simple statement of rights and creates a procedural process for data. There is a discernable structure that starts from the right to know (a duty to notify), the right to make corrections to data, the right to an explanation, the possibility of revision of a decision and auditing mechanisms by independent agents.

The Right to Explanation appears not only as a right giving rise to the need for internet regulation and governance, but also as a corollary of a broader need for procedural justice in the context of widespread digital technological use. Since the beginning of the decade, papers have addressed the possibility for regulation and justice to use the notion of procedural justice in the context of the massive use of big data, profiling techniques and other types of statistical inference making[14].

The idea, however, is not that new. Arthur Miller, in meetings of the Secretary's Advisory Committee on Automated Personal Data Systems of the U.S. Department of Health, Education and Welfare, in 1973, already noticed that procedural justice had a potential role in the field of data protection and privacy law for public policies[15]. As he stated in his early work: "ideals of fair play and due process indicate that any set of rules regulating the handling of personal information should accord the individual […] the right to receive notice and an opportunity to be heard […]."[16]

Automated or semi-automated decisions are becoming much more relevant in several applications and some questions have emerged from studies of algorithms and their social impacts. The main

[13] A discussion about the meaning of due process in the United States can be found in M. REDISH and L. MARSHALL,"“Adjudicatory Independence and the Values of Procedural Due Process", 95 *Yale Law Journal,* 1986: https://digitalcommons.law.yale.edu/ylj/vol95/iss3/1.

[14] D. KEATS CITRON, "Technological Due Process", 85 *Washington University Law Review* 1249, 2008; D. KEATS CITRON and F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, 2014, Social Science Research Network: https://papers.ssrn.com/abstract=2376209.

[15] Ch. JAY HOOFNAGLE, *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418.

[16] A. R MILLER, *Assault on Privacy: Computers, Data Banks and Dossiers,* University of Michigan Press, 1971, p. 237.

problems include the lack of transparency, the impossibility of finding errors, misleading conclusions and the absence of contestability[17].

When people have their rights or their interests affected by a state action in a democratic society within the rule of law, the notion of due process appears as an indispensable instrument for justification. Some authors argue that, in case of informational asymmetries between users and algorithms, due process should be used as a means of increasing confidence and building trustworthy technology. The procedural data due process covers the lawful and legitimate processing of personal data, as opposed to the mere regulation of its collection, use and disclosure[18].

After recognising some of the new risks emerging from big data-oriented decisions, Crawford and Schults[19] argued that a new approach was necessary. In their view, it is important to consider the whole decision process and think about social control, including a right of defence and the possibility of audit from a non-related third party, which might evaluate the severity and impact of an automated decision, just like algorithms in criminal law procedures, on health insurance and credit scoring. Recent events within the so-called 'sharing economy' (or 'gig economy') should be included among those cases. In June 2020, Brazilian Uber drivers staged a strike, demanding transparency on ride-hailing platforms such as Uber, 99Taxi and Cabify. Their complaint included unfair blocking by the platforms, with no meaningful information, and hundreds of cases went to court[20].

Some elements of the procedural process from E.U. and Brazilian regulation remain restricted to some contexts, such as solely automated decisions, and limited by third-party rights related to intellectual property[21]. Although the extent of protection depends on future interpretations by agencies and courts, due process should play an important role in the development of data protection.

[17] V. EUBANKS, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor,* First Edition, St Martin's Press, 2017; C. O´NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Crown Books, 2016: https://www.amazon.com.br/Weapons-Math-Destruction-Increases-Inequality/dp/0553418831, accessed on 27 May 2020; F. Pasquale, *The Black Box Society: The Secret Algorithm That Controls Money and Information,* 2015.

[18] B. BIONI and P. MARTINS, "Devido Processo Informacional: Um Salto Teórico-Dogmático Necessário?", *Jota,* 2020: https://www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020, accessed on 15 July 2018.

[19] K. CRAWFORD and J. SCHULTZ, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, Social Science Research Network, 2013, SSRN Scholarly Paper ID 2325784: https://papers.ssrn.com/abstract=2325784, accessed on 27 May 2020.

[20] R. GROHMANN and others, *The Uprising of Brazilian Food Delivery Riders*, 2020: https://fair.work/en/fw/blog/the-uprising-of-brazilian-food-delivery-riders/#continue, accessed on 8 December 2020.

[21] L. EDWARDS and M. VEALE, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, LawArXiv 2017: https://osf.io/97upg, accessed on 27 May 2020.

§ 2 – Precedents For The Right to Explanation in Brazil

A) Brazil has established instances of algorithmic explainability outside the data protection sphere

Beyond the statutory provisions of the LGPD, other Brazilian laws have laid out elements that support the existence of algorithmic explainability. These provisions come mostly in the context of consumer protection, especially in relation to credit scoring and profiling practices. Before the LGPD, the Consumer Protection Code and the Credit Scoring Law provided consumers with several rights and established limits on the use of databases. Some court decisions gave a more precise interpretation for credit scoring practices, based on these regulations and fundamental rights.

The Law 8.078/90, called *Código de defesa do Consumidor* or CDC (Consumer Protection Code), was passed in 1990[22]. It represented an important step towards a more protective legal system, since it addressed the asymmetries of power that arise from contracts between consumers and businesses. Although the former Civil Code already provided some protection, the procedural costs of accessing the legal system by procedural law made the protection ineffective for consumers.

Information asymmetries are understood to be one of the main sources of consumer vulnerability. One of the main tools the law establishes for consumer protection is transparency. Art. 6º, Section III, sets as a basic consumer right "clean and adequate" information about products and services, including their composition, quality, taxes, price and the risks involved with them. Item IV dictates that consumers must be protected against abusive or misleading advertisements, as well as unfair commercial practices.[23]

The Code also regulates consumer databases and establishes some consumer rights. One of the main targets has been the practices of companies offering "credit protection services". Initially, these services 'blacklisted' defaulting consumers and shared the information with businesses and companies, etc. Since the credit protection services gathered data from a very large number of sources, with little human revision, it was not unusual for people to wrongfully appear among the list of defaulting consumers. These mistakes caused several difficulties for credit access and for exercising people's rights.

[23] "Art. 6º It is a consumer's basic right: III – clear and adequate information about the different products and services, with correct specification for quantities, features, composition, quality, incident taxes on price, as well as the risks that are presented; IV – protection against misleading and abusive propaganda, coercive or disloyal marketing practices, as well as abusive or imposed practices and clauses in the provision of products or services" (translated by the authors)

The Consumer Protection Code, however, goes beyond lists of credit defaulters. Art. 43º regulates the registration of consumers' information, providing protection for every kind of consumer database. The Article guarantees access to the data and states that it must be provided in a clear, true and comprehensible way. The Code also established that the consumer must be informed about any registration in a consumer database that happens without his or her consent. Art. 43º also establishes the right to rectify incorrect information and defines consumer and credit databases as public entities. The Code also limited the length of time for which negative information about a consumer could be held at five years[24].

The Consumer's Law introduced an initial framework for privacy and data protection. The courts have heard several cases regarding access and rectification of personal information, mainly related to negative information about individuals being unfairly classified as a defaulter. However, with computational development, new information became available for databases and the Code was restrained by the concept of consumer databases[25].

In 2011, the Law 12,414/11, called the "Credit Scoring Law", was passed to regulate financial and consumer databases, targetting credit analysis activities such as credit bureaus and their credit scoring methodologies. The Act establishes a stronger framework, setting criteria for the collection and use of personal data for credit analysis. The Act also set principles for data protection that were aligned with a more protective approach and established some concepts, such as sensitive and excessive data, for the purpose of credit analysis. Among the principles, the Act brought transparency obligations. Art. 5º brought subjective rights, such as free access, exclusion from a database, rectification of incorrect data, information about criteria and features used in credit analysis and

[24] "Art. 43 The consumer, withal the provisions from Art. 86º, shall have access to the information from registrations, files, records and personal and consumer data recorded about him, as well as its respective sources,

§ 1° The registration and consumer data should be objective, clear, truthful and in an easily comprehensible language, and should not hold negative information for longer than five years.

§ 2° The opening of a registration, file, record and personal and consumer data should be informed in writing to the consumer without it being requested by him.

§ 3° Consumers should, whenever their data and records are inaccurate, demand immediate correction, and the recorder, within 15 working days, must communicate changes to any recipient of the incorrect information.

§ 4° Databases and registrations related to consumers, credit protection services and similar must be considered as public entities.

§ 5° When a consumer's debt lapses, the Credit Protection Services shall not provide any information that should block or interfere with a new application for credit from suppliers." (translated by the authors)

[25] For a more extensive discussion about the role of credit scoring and consumer rights in the context of Brazilian Data Protection Law, see: R. LEITE MONTEIRO, *Existe Um Direito a Explicacao Na Lei Geral de Protecao de Dados No Brasil*,, Insituto Igarapé, 2018: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf, accessed on 8 December 2020.

the revision of automated decision-making[26]. This framework provides tools for effective control over data, instead of just information rights[27].

These provisions were inadequate for emerging practices enabled by information technologies because they focused solely on financial or consumer databases and there were few enforcement mechanisms. However, they have played an important role in reinforcing informational self-determination in the Brazilian legal system and anticipate some core issues about the Right to Explanation in the courts.

B) Court precedents

Before the Marco Civil and the LGPD, one of the main questions faced by the Judiciary concerned the use of personal data in consumer databases, mostly related to credit protection services that registered individuals as defaulters. Among the provisions of the Consumers Protection Code, Art. 43º, paragraph 1, states that registers of defaults should not last for more than 5 years. The Supreme Court of Justice was called upon to adjudicate on this matter. An important court precedent from 1995 was the understanding that this provision was aligned with constitutional rights such as intimacy, privacy and personality rights such as individual honour and image. Justice Ruy Rosado de Aguiar used the concept of informational self-determination, for the first time in national justice, in a decision to guarantee register exclusion[28].

The development of analysis services evolved into new credit risk models based on information that was in addition to default registers. The Credit Scoring Law of 2011 regulated credit and payment databases that compile financial and consumer information from consumers. However, some questions emerged. One problem involved statistical inferences and the right to access credit scores. The discussion indicated the importance of that regulation for data protection, and, at the same time, the lack of a clear and strong legal provision for personal data.

[26] Art. 5º The registered rights are: I – To obtain register cancellation or reopening, when requested; II – To obtain free access, regardless of justification, to the information about an individual in the databases, including his or her credit history and credit grade or score, and the database manager must maintain a safe system, by phone or another electronic means, for consultation for those registered; III – To request opposition against any incorrect information about an individual in the database and obtain, within 10 days, the correction or cancellation in every database that shared that information; IV – To know the main elements and criteria considered for risk analysis, taking into account commercial secrets; V – To request to the consultant the revision of decisions bases solely on automated means; VI – To be previously informed as to the database manager's identity and about storage and the processing purposes; VII – To have personal data used only for the purpose for which it was collected. (translated by the authors)

[27] The Act was amended by Complementary Law nº 166/2019. The original text just permitted inclusion of consumer and financial information, given subjects' consent but the amendment changed the text to permit inclusion automatically and gave subjects the right to opt out. This Complementary Law also changed the Act to permit data transfers for third parties.

[28] *REsp n 22337 RS 1992/0011446-6.*

Credit scores are statistical inferences about an individual's capacity to manage his or her debts. At the time, some organisations provided such a service without individuals' consent and the judiciary was called to adjudicate on the legality of the practice. According to the Act, databases should only use consumers' financial data after obtaining their consent. The Superior Court of Justice allowed the score[29], as long as it was possible for it to be limited by the principles set by the Law, such as the prohibition on the use of sensitive or excessive data, and to be aligned with consumer protection law, including the provision of information on data sources if it damaged the individual. However, it considered it was not a database and that it did not need individuals' consent.

After the decision, the court edited Súmula nº 550[30], a Brazilian legal instrument for the harmonisation of the court's understanding on a given topic, which stated that credit scoring does not constitute a database, and does not need prior consent, but the individual could ask for information about the data used and the sources of data used in calculating the score. The same court recognised the consumer's right to request access to the data used for the score, subject to the consumer being able to provide evidence of damage due to the score[31].

These initial decisions could lead to the Right to Explanation and constitute a framework for data protection. However, the framework remained substantially restricted. The revelation of criteria used in calculation has been blocked by companies protecting their intellectual property, especially their trade secrets. Furthermore, the courts decided that credit scoring was different to the consumer databases described in the Consumer Protection Code and the Credit Scoring Law. Whereas the regulation for databases provides individuals with access to information as a subjective right, in the context of credit scores, access to information and sources used in the processing require evidence of damage to the consumer.

This framework relied on regulating the databases, and not the data. Such arrangements could not provide data subjects with effective control over information about them. Given the statistical nature of credit scores, and the legal concept of databases set forth by the regulations, it is still impossible for the consumer to fully grasp the usage of the personal data, despite the existence constitutional and legal principles that point towards these protections.

During the last decade, due to the emergence of certain technologies, the rise of widespread data collection and public

[29] *REsp n 1419697 - RS 2013/0386285-0.*

[30] "Súmula 550. The use of credit scoring, a statistical method for risk assessment that does not constitute a database, does not need the consumer's consent, and the consumer has the right to request clarification about the information used and the sources of data considered in the measurement." (Translated by the authors).

[31] *Recurso Especial nº 1304736 RS 2012/0031839-3.*

concerns related to vigilance by the government and tech companies, the notion of privacy was reinvented in terms of the concept of human dignity. The concept of informational self-determination has strenghtened even before the Marco Civil and the LGPD. The regulations introduced and established principles for the fair use of personal data, however, the public debate over the misuse of personal data and scandals such as those concerning NSA and Cambridge Analytica promoted the acceptance that it is possible to deduce the right to data protection from traditional constitutional rights.

In the beginning of 2020, during the COVID-19 pandemic, this question was considered by the Brazilian Supreme Court of Justice. The government enacted the Provisional Measure nº 954/2020, demanding that telecommunications companies transfer user data to the Brazilian Institute of Geography and Statistics. The Measure stated that the data could only be used for official statistics through phone interviews, and consist solely of the name, phone number and address of each data subject.

The Brazilian Bar Association ("OAB") filed a Direct Action of Unconstitutionality against the Measure[32], pleading that it was not formally and materially appropriate to the Brazilian 1988 Constitution. The petition argued that the government could not justify the urgency and relevance demanded for Provisional Measures and that its content violated human dignity from Article 1, section II, and people's privacy, intimacy, honour and image from Article 5, sections X and XII. The Association also argued that a right to informational self-determination could be construed from the Constitution.

Previous decisions of the court interpreted the Right to Privacy from Article 5, sections X and XII, as being tied to the content of communication and to the private or confidential nature of information. The OAB argued, however, for a shift in this interpretation to recognise an autonomous right to the protection of personal data, independent of confidentiality or communication content. The Federal Supreme Court recognised the necessity of updating fundamental comprehension to include informational self-determination according to the new information technology context with widespread data collection[33].

The ministers of the court understand that constitutional law must acknowledge changes in society in terms of granting people rights and shift the focus from the content of data to protecting the data itself, according to the use of the data and the purpose of processing. The use of personal data, therefore, must adhere to the requirements of proportionality, necessity and adequacy. Since the Provisional Measure only mentioned a general motivation for data transfer and did not state specific goals and limits, and also failed

[32] Direct Action of Unconstitutionality is a Brazilian procedural constitutional instrument that could be sued in the constitutional court to identify whether a law or a government act is contrary to constitutional norms or principles.

[33] *ADIn n 6387/2020 DF.*

to demonstrate the need to transfer the whole database, instead of just a small portion of users' data, it was considered inadequate, disproportionate and unnecessary.

Supreme Court Justice Gilmar Mendes, arguing in favour of the existence of a constitutional right to informational self-determination, presented a systematic interpretation grounded on: a) human dignity, a constitutional foundation present in Art. 1º, Section III; b) the renewal of privacy and intimacy provisions from Art. 5º, X and XII and c) the acknowledgment of the *habeas data* as a material instrument for informational self-determination[34].

Although this decision was made before the coming into force of the LGPD, the statute was mentioned by minister Gilmar Mendes, together with the Internet Bill of Rights, as an example of a quasi-constitutional matter, due to the reality of digital questions. Both laws became an important element of the correct interpretation of the Constitution[35].

The judicial decision reinforced the principles of data protection and consolidated a broader notion of personal data, aligned with the LGPD[36], which creates a new condition for the Right to Explanation that should include the making of inferences and automated decisions using emerging technologies. Those technologies should be used by the government, as well as by the judiciary.

It is worth mentioning Resolution No. 332/2020, from the National Council of Justice, an administrative organ of the Brazilian judicial system that sets criteria and norms for the use of artificial intelligence by the court, and which sets out procedures for algorithm accountability and governance, aligned with data protection principles from the LGPD.

The Resolution establishes tests for bias for any artificial intelligence system deployment and sets transparency requirements that include, in Art. 8º, VI, an explanation by a human agent and the possibility of being audited. The Resolution also creates a platform for testing, auditing, training and sharing models of artificial intelligence called Synapses.

§ 3 – The Right to a Due Informational Due Process

Since researchers and civil society organisations have, in the last decades, constantly argued for more effective control over data, it seems that Brazilian legislators and courts have understood that, if

[34] For more information about the role of *habeas data* in the Brazilian Privacy and Data Protection Law, see: L. Schertel Ferreira Mendes, "Habeas data e autodeterminação informativa", 12 *Revista Brasileira de Direitos Fundamentais & Justiça* 185, 2018.

[35] For a discussion of the role of internet laws for constitutional interpretation, see: L. Gill, D. Redeker and U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 2015, Berkman Center Research Publication Series: https://dash.harvard.edu/handle/1/28552582, accessed on 3 December 2020.

[36] B. Ricardo Bioni and others, "A Landmark Ruling from the Brazilian Supreme Court: Data Protection as an Autonomous Fundamental Right and Informational Due Process", 6 *European Data Protection Law Review* 615, 2020.

data protection is to have an impact on people's rights, there must be control over data flows.

The court has decided that *habeas data* should also apply to the databases of private organisations, in the public interest. Informational due process was invoked by Judge Gilmar Mendes for the decision on Direct Action of Unconstitutionality. Even without the LGPD's impact, the courts have established the position that it is not enough that the government informs data collection. It is necessary to assess risks, to strike a balance with the benefits, to initiate a process that seeks proportionality and necessity, and to adopt security measures before any handling of personal data[37].

The analysis of decisions and the LGPD should lead to the conclusion that data protection must be seen within a procedural justice framework. Therefore, transparency obligations should not be regarded as a final goal. The information must be provided as a feature for individual self-determination, within a procedure that permits the control of data processing. In the context of automatic decision-making, the right to an explanation, present in Art. 20º, § 1º, appears as a *sine qua non* condition to challenge those decisions and grant people dignity. The informational due process, thus, may be seen as a principle for automatic decision-making.

Some basic elements for informational due process should now be proposed. Following the classical principles of procedural justice, it is possible to create a framework for automated or semi-automated decision-making.

First, it is important to enforce the need for independent adjudication. It is one of the main principles of unbiasing algorithms. It means that organisations, both public and private, should take steps to ensure the impartiality, representativeness and accuracy of any model prior to deployment.

Second, data subjects should be informed as to whether they wish to have their data used in automated decision-making. They have the right to know about the data used for training the algorithm and its decision-making. Active transparency practices should be implemented and responses should be made to individuals' requirements. In terms of transparency, it is important to note that it is less feasible for the controllers to hide behind intellectual property rights and refuse user requests when dealing with data sources and categories.

Third, the information provided about data processing should be understandable. The individual has the right to an explanation. This right must be bidimensional and go beyond mere information[38]. The processors should strive for data subjects' understanding of criteria, purposes, risks, accuracy, limits and the measures adopted in the development of the model. Information about the criteria

[37] *ADIn n 6.387/2020 DF* (No. 55).

[38] T. MILLER, *Explanation in Artificial Intelligence: Insights from the Social Sciences*, 2018, arXiv:1706.07269 [cs]:
http://arxiv.org/abs/1706.07269, accessed on 14 August 2020.

and procedures involved in decisions can be limited due to intellectual property rights, as long as they are balanced with the impact of such limitations on fundamental rights and liberties. That is why the national authorities played such an important role in developing auditing practices[39].

Several studies have discussed the extent of explanation[40]. Within this procedural framework, the data subject must be provided with the means and capability to challenge a decision. That is why the fourth element of informational due process is to offer the opportunity to appeal. Such an appeal should be effective and based on models' limits, the context of its use and the possible damage caused by the decision-making.

The fifth element of informational due process is revision. There should be the possibility to revise a decision, preferably by a human being and not by another algorithm. The first approved LGPD text for Art. 20º determined that the data subject should have the right of revision by a natural person. However, the text has been changed to withdraw the need for human involvement. The reason for the change was government concern about the costs involved. Such an obligation might have presented a barrier for small firms and startups, and which would inhibit innovation and technology development[41]. The removal of human revision should be understood as an obstacle for the effective protections established by law. If a revision is made by another automatic model, the quality of explanation may be low, generic or simply unrelated to what the consumers's actual requests are [42].

Actually, there are some legislative proposals for regulating automated decisions, especially for high-risk applications. Economic consequences are a relevant dimension for regulating privacy and data protection. Interdictory laws could lead to stagnation and damage entrepreneurial practice. However, the development of a robust and appropriate framework is also important for establishing a trustworthy environment for technology development.

CONCLUSION

[39] CASEY, FARHANGI and VOGL, op. cit..

[40] A. ADADI and M. BERRADA, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)", 6 IEEE, 2018, Access 52138; R. GUIDOTTI and others, *Local Rule-Based Explanations of Black Box Decision Systems*; 2018, arXiv:1805.10820 [cs] <http://arxiv.org/abs/1805.10820> accessed on 30 June 2020; Q VERA LIAO, D. GRUEN and S. MILLER, "Questioning the AI: Informing Design Practices for Explainable AI User Experiences", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,* 2020; CASEY, FARHANGI and VOGL, op. cit..

[41] An interesting discission about the changes in Art. 20º can be found in: A. VERONESE, "Os Direitos de Explicação e de Oposição Diante Das Decisões Totalmente Automatizadas: Comparando o RGPD Da União Europeia Com a LGPD Brasileira", in G. TEPEDINO, A. FRAZÃO and M. DONATO OLIVA (eds), *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro,* 2ª, Thomson Reuters, Revista dos Tribunais, 2020, p. 381.

[42] P. REGINA SILVA, "Os Direitos Dos Titulares de Dados", in Caitlin MULHOLLAND (ed), *A LGPD e o novo marco normativo no Brasil,* Arquipélago, 2020.

The LGPD has established an organised system for data protection, which includes transparency and accountability obligations, as well as auditing and enforcement powers for the national authority. Art. 20º establishes the right to the revision of an automated decision. Furthermore, the data controller has a duty to provide clear and adequate information about the criteria and procedures used in an automated decision. The provision of that information, as a consequence, should enable the revision to be effective, by providing the data subject with significant knowledge about the decision.

The law initially required human revision, but the Article has been changed, to exclude human participation. Moreover, the right to revision for solely automated decisions is a limitation that may exclude a great number of applications. There are reasonable arguments about the risk of slowing down innovation in the technology field but, on the other hand, weakening social control may cause the right to be an ineffective measure.

Courts in Brazil have implemented strong protections for data protection principles such as informational self-determination. In addition, the consequential concept of personal data derived from Art. 12º can represent a strong step towards a new generation of privacy and protection rights that considers not only *ex ante* protections, but also *a posteriori* consequences of data processing for both individuals, and collective rights.

Finally, a five-element test can be derived from informational due process of law practices that lead to a Right to Explanation, which can effectively allow individuals to understand the impact of automated decisions on their life and thus the possibility to challenge them.