Observatório da privacidade e proteção de dados

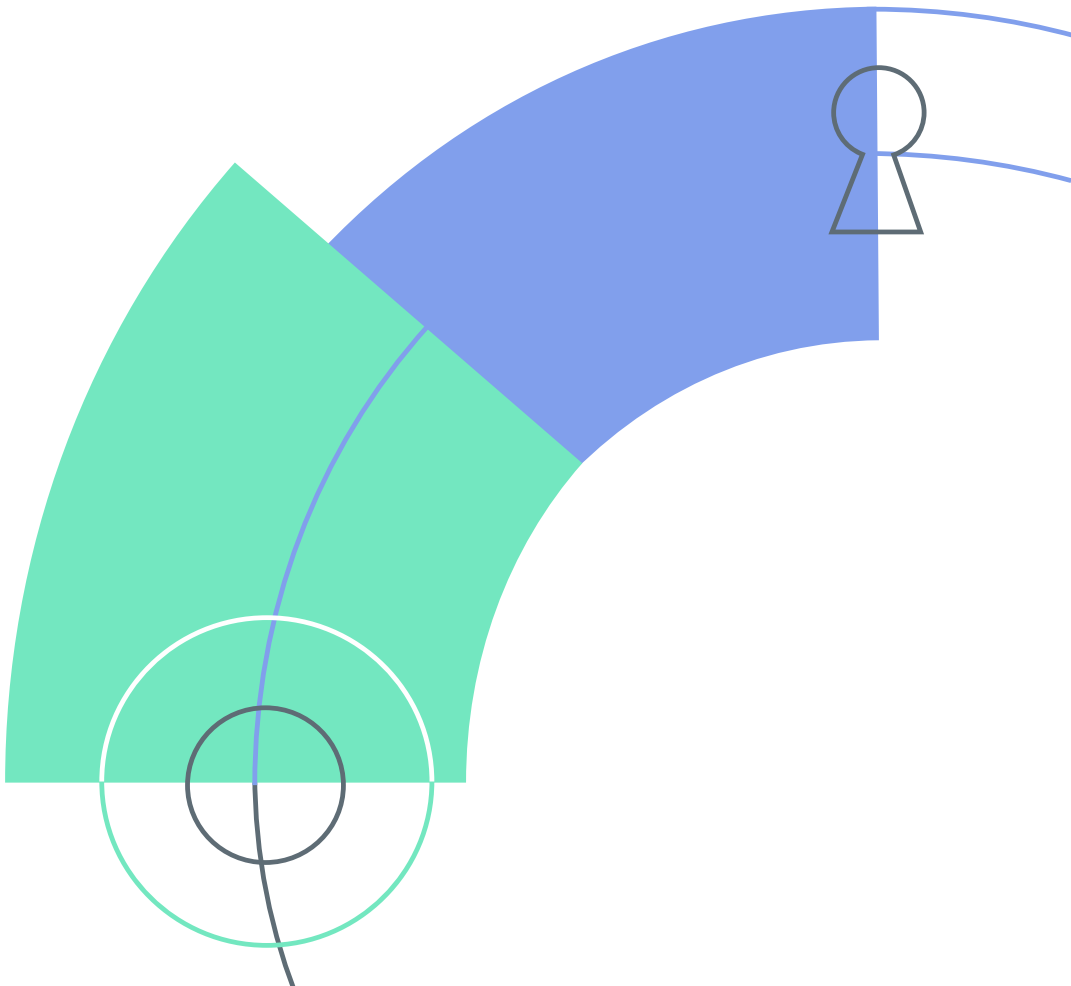
Data Privacy BR RESEARCH

LEGITIMATE INTERESTS UNDER THE BRAZILIAN GENERAL DATA PROTECTION LAW: GENERAL FRAMEWORK AND CONCRETE EXAMPLES

Associação Data Privacy Brasil de Pesquisa

AUTHORS
Bruno Ricardo Bioni
Mariana Rielli
Marina Kitayama

REVIEWER
Aline Herscovici

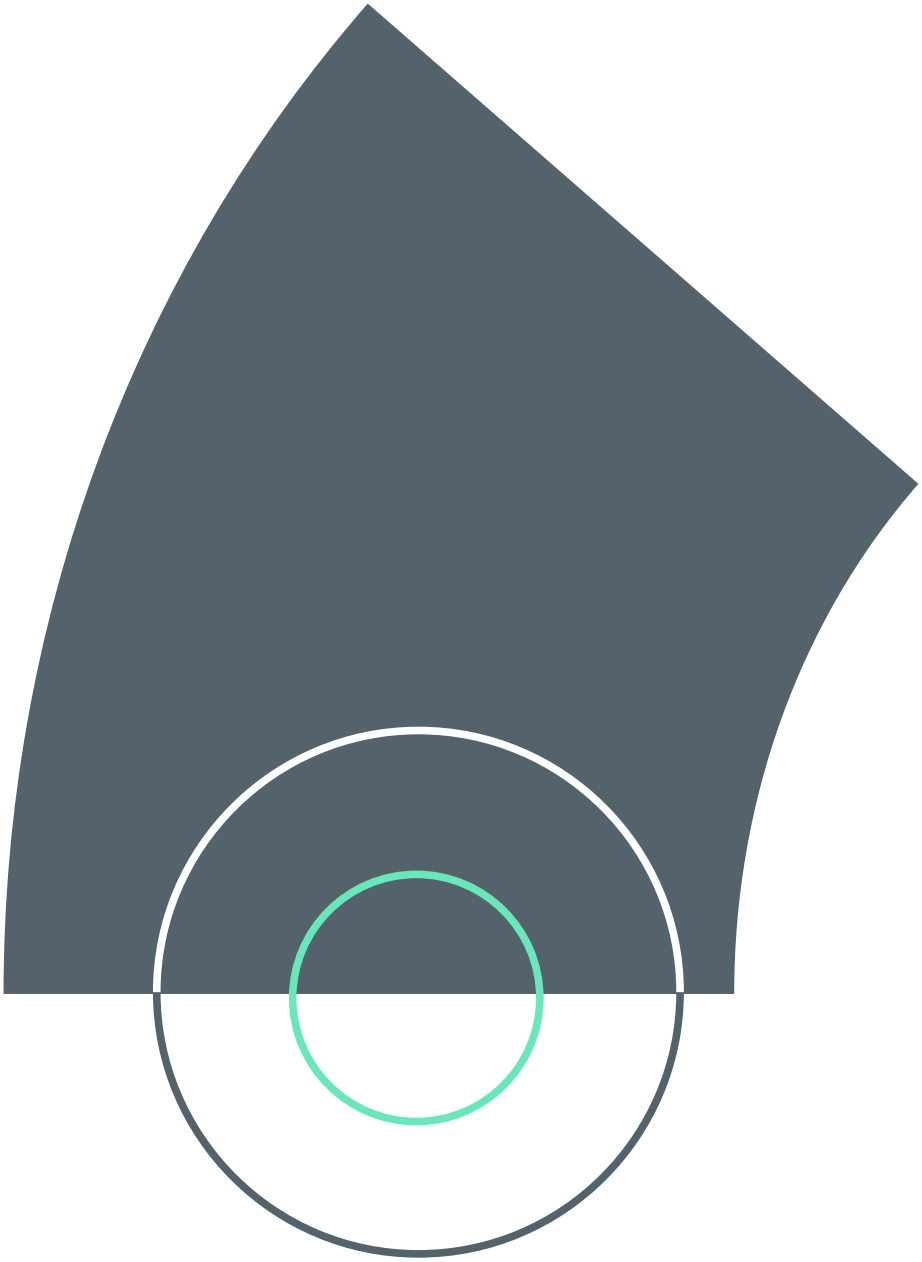


INSTITUTIONAL INFORMATION

Data Privacy Brasil is a space of intersection between Data Privacy Brasil Ensino, a company that provides data protection courses and training, and Associação Data Privacy Brasil de Pesquisa, a non-profit civil association based in São Paulo. The organization is dedicated to research and advocacy on the interface between personal data protection, technology, and fundamental rights. Based on an Ethical Funding and Transparency Policy, the Associação develops strategic research projects, mobilizing knowledge that can help regulators, judges and law professionals deal with complex issues that require in-depth knowledge about how technologies and socio-technical systems affect fundamental rights. The Associação receives funding from international philanthropies such as the Ford Foundation, Open Society Foundations, and AccessNow, as well as domestic funders such as the Comitê Gestor da Internet (CGI.br). For more information, visit www.dataprivacybr.org.

HOW TO CITE THIS PAPER
BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.

PRESS
For clarifications about the paper and interviews, contact the Associação through the e-mail imprensa@dataprivacybr.org



INDEX OF ACRONYMS

ABMED: Brazilian Direct Marketing Association
ANPD: Brazilian Data Protection Authority
CCT: Science and Technology Commission
GDPR: General Data Protection Regulation of the European Parliament and Council of the European Union (in the original, General Data Protection Regulation)
AI: Artificial Intelligence
IP: Internet Protocol
LAI: Access to Information Law
LGPD: Law No. 13.709/2018, Brazilian General Data Protection Law;
LIA: Legitimate Interest Assessment
OCDE: Organization for Economic Cooperation and Development
PL: Bill
PLS: Senate Initiative Bill
PEP: Politically Exposed Person
GDPR: General Data Protection Regulation
RN: Normative Recommendation
EU: European Union
VPN: Virtual Private Network

EXECUTIVE SUMMARY

This paper is the result of the research efforts[1] by the Observatory on Privacy and Data Protection[2], a project conducted by Associação Data Privacy Brasil de Pesquisa[3]. The Observatory is a tool for monitoring and analysis of the debates around the subject of privacy and data protection in Brazil and worldwide[4].

The purpose of the paper is primarily to explore the anatomy of the lawful basis of legitimate interests as provided for by the Brazilian General Data Protextion Law/LGPD. Some primary issues that sparked interest in the elaboration of the paper were: When did the concept of legitimate interests first appear on the legislators' radar and who were the players that raised the debates which culminated in the final version of the text? What were the interests that needed to be harmonized throughout this process and how is this reflected in the interpretation of the lawful basis? Is a proportionality assessment - in European law known as Legitimate Interest Assessment/LIA - required as a type of special registration of data processing operations based on legitimate interests? Are the conditions outlined in Article 10 of LGPD cumulative and do they also govern the application of the legitimate interests of third parties, not just the controller?

The document aims to provide interpretive paths that are both rooted in the Brazilian legal culture and based on a combination of interpretation techniques, in order to understand the legitimate interest lawful basis and some of its most sensitive, and even controversial, aspects. First, the text addresses the rights and duties triggered by the legitimate interest provision for the parties involved - controllers, third parties, data subjects. Then, it moves on to the main consequence of the design of this lawful basis in LGPD: the existence of a ''strengthened argumentative burden'' in relation to data protection principles such as purpose limitation, necessity, transparency, accountability, etc.

---

1 The authors of the paper also had valuable input from experts, who were consulted throughout the writing process. We thank Giovanna Ventre, Daniel Arbix, Karen Duque, Juliana Akaishi, Marcel Leonardi, Giovanna Carloni, Renato Leite Monteiro, Raissa Moura, Paula Zanona, Bárbara Simão, and Luiza Brandão for their time in providing constructive criticism and insights that made this text more robust.

2 See: https://observatorioprivacidade.com.br/

3 See: https://www.dataprivacybr.org/

4 The Observatory as a whole is funded by Google and Facebook, pursuant to the Associação's Ethical Funding Policy, and this phase of the project, which includes the report on the lawful basis of legitimate interest, is funded exclusively by Google. The translation of the report to English was funded by Future of Privacy Forum. We thank the FPF team in the person of Gabriela Zanfir-Fortuna.

The text is interspersed with boxes that summarize each item and provide ''normative recommendations'', which are, at the same time, a suggestion for future guidance by the Brazilian Data Protection Authority and a reference for the ''data processing agents'' (controller and processor as per LGPD) themselves when opting for legitimate interest to support their operations.

The paper also features a two-phase practical exercise. The first part is composed of ten (10) themes/areas, corresponding to sectors in which the legitimate interest lawful basis is most commonly applied (such as labor relations, including background checks, online and offline marketing, analytics, etc). These areas were selected based on conversations with partners who themselves have been dealing with applying legitimate interests, as well as a study of cases that have already been discussed internationally[5].

For each area, there are a few illustrative cases, fictional but loosely based on real examples, that are then followed by a ''thermometer'', an artifice to indicate which phases of the legitimate interest assessment (LIA) tend to be most critical in each of these sectors. The second part of the exercise is a complete and more detailed example of applying a LIA based on a hypothetical case.

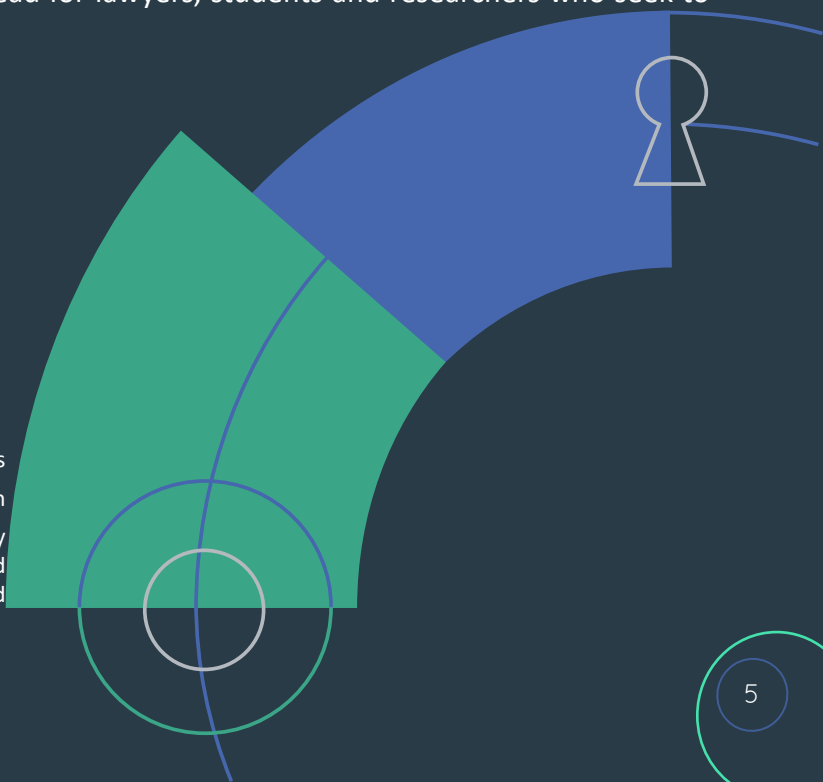
Therefore, this work doesn't limit itself to providing an ''abstract dive'' into the subject, but rather it intends to combine the theoretical substrate of legitimate interests under LGPD with concrete situations.

It is important to emphasize that, at this point in Brazil, with LGPD having come into force a little more than 6 months ago and the National Data Protection Authority having just recently completed its internal structuring, there is no domestic case law or DPA guidance that can be relied upon for interpretation and practice. This paper is a contribution intended to add to the vibrant debate and production of content of the most diverse natures about the legitimate interest lawful basis under LGPD.

One of its central points is that the undeniable European influence on the Brazilian law in general, and on this specific point, cannot divert the focus from the particular choices that resulted in LGPD, nor from the need to balance its provisions with other domestic rules and principles in force, in order to avoid an inadequate ''legal transplant'' of this indeterminate legal concept.

The document's target audience is decision makers at all levels, including members of ANPD, as well as players that carry out personal data processing activities and intend to rely upon legitimate interests as a ground for processing. It is also an interesting read for lawyers, students and researchers who seek to deepen their knowledge on the subject.

We hope you enjoy the reading!



5 To that end, the report ''Deciphering legitimate interests under the GDPR: a report based on more than 40 cases from practice'' by Future of Privacy Forum and Nymity, co-authored by Gabriela Zanfir-Fortuna and Teresa Troester-Falk and researched by Meaghan McCluskey, was the main source of material and inspiration for some of the cases.

FINDINGS AND NORMATIVE RECOMMENDATIONS

Finding no. 1:

Previously an unknown legal concept, upon its introduction during the public debates that preceded the passing of LGPD, the legitimate interest provision was placed on an equal footing with the other lawful grounds for personal data processing, particularly consent, which had been, up until that point, the main (and, in some cases, only) lawful ground adopted by early drafts of the legislation. Following international examples, the final text doesn't establish any hierarchy whatsoever among the ten (10) lawful grounds described in Article 7.

Finding no. 2:

The legitimate interest provision has been the subject of intense dispute. A ''tug-of-war'' has been pulled especially between the third sector (mainly NGOs, research centers and academics) and the private sector to, respectively, restrict and enlarge its scope. In the end, a common denominator was reached, based on a solution brokered mainly by academics, in which this lawful basis would be accompanied by a second provision that set the specific parameters for its application (Article 10). Thus, the Brazilian law innovated by directly providing criteria for the application of an open legal concept and, therefore, potentially bringing greater predictability to its interpretation. From its inception, there was already a concern about the ''side effects'', in terms of legal certainty, of introducing the lawful basis of legitimate interests, something that was partially remedied in the final version of the law.

Finding no. 3 and NR 1:

The adjective "legitimate" is a recurring qualifier throughout LGPD. It comes, for example, with the definition of the principle of purpose limitation (''processing for legitimate, specific, explicit and informed purposes''). In this case, however, it has a more restricted meaning than in the case of a ''legitimate'' interest: it means that the specific data processing purpose should not be prohibited by law or other regulation. In the case of the lawful basis of legitimate interests, on the other hand, this term triggers an analysis of compliance with the conditions described in Article 10 for an interest to be considered legitimate. It is recommended to take into consideration such a distinction in terms of the scope and range of the term.

Finding no. 4 and NR 2:

The provision that the legitimate interest can be of a third party was introduced in the version of the Data Protection Draft Bill submitted to Congress, which then became Bill 5276/2016. Unlike GDPR, the Brazilian law does not provide a definition of third party, nor does it introduce the idea of a ''recipient''. So, it is even more challenging to interpret the scope of the lawful basis of legitimate interests of a third party, something that needs to be urgently addressed by the Brazilian Data Protection Authority (ANPD). Examples of who can be a third party in a data processing operation range from natural persons and legal entities to the wider, more abstract notion of a collectivity. It is advisable to i) treat these categories of third parties differently, as they entail different potential risks for data subjects, and ii) reinforce that, in all cases, the lawful basis must always apply to a concrete situation. In this sense, it is incumbent upon the controller to assess whether the interest of the third party is, in fact, legitimate.

Finding no. 5 and NR 3:

Employing different techniques of legal hermeneutics in order to interpret Article 10, an adequate conclusion is that this provision (i) refers to both the legitimate interests of the controller and of third parties and that (ii) the list of items and paragraphs of the Article imposes cumulative, and not alternative, conditions. This ensures an uniform application of the lawful basis, regardless of who relies on it. It also does not undermine the function of Article 10 as a whole, which is to promote the balancing of the interests of the controller or third parties with those of the data subject. A systematic and teleological interpretation of Article 10 is in line with the very spirit of a general data protection law, which is to establish, as a rule, duties and rights in a horizontal and mostly symmetrical manner.

Finding no. 6 and NR 4:

LGPD was built on the basis of the need to balance the protection of personal data and the data subject's fundamental rights with economic development and innovation, a dichotomy that is also at the core of the legitimate interest provision. In this sense, the law established the possibility for a differentiated regime for small businesses, including alternative procedural matters such as deadlines, to be defined by the Brazilian Data Protection Authority. This differentiated procedure can be applied to legitimate interests, such as for example, by not requiring specific documentation, or by relaxing the components of the Legitimate Interest Assessment. However, it is important to point out that this is an open-ended possibility, so that, in principle, the provisions of the law apply horizontally to all data processing agents.

Finding no. 7 and NR 5:

Relying on legitimate interests as a lawful basis for processing creates a greater argumentative burden regarding the principle of purpose limitation since, in order to avoid its use in a speculative manner, the lawmaker chose to stress that its application results only from a concrete situation. This reinforcement serves the data processing agent itself, as the more clearly their interest is outlined, the easier it will be to assess it, especially in order to analyze whether the amount of processed data is really necessary, as well as what the measures to mitigate the impact on the rights and freedoms of the data subject are. Conversely, the more generic the interest, the more difficult it will be to demonstrate that the data processing agent is not somehow abusing its position.

Finding no. 8 and NR 6:

The idea of ''legitimate expectations'' is directly related to the principle of good faith, to the extent that it is based on a duty of loyalty and non-frustration of the data subject's trust. In addition, another element of the concept of good faith is the prohibition to the ''abuse of rights'', which in this case would correspond to a limitation on the processing of personal data that does not pass the legitimate interest test. In that sense, the interpretation of legitimate interests, particularly in regard to the data subject's expectations, must also take into account the strong influence of the principle of good faith in Brazilian private law, in order to avoid an inadequate legal transplant of the concept. It is important to emphasize that good faith is the "principle of principles" as it stands in the head provision of Article 6, unfolding into the other principles listed throughout the corresponding items. As a result, the best interpretation of the provision is the one that considers that the legitimate expectation of the subject must be *considered* in every case where legitimate interest is applied, even if it does not prevail in the final result of the balancing of interests at stake, since it is not an absolute value.

Finding no. 9 and NR 7:

Unlike other lawful bases, in the case of legitimate interests there is explicit reference to the principle of necessity as a condition for applicability. Necessity, or minimization, is hereby divided into strict sense, which refers to processing the least amount of personal data necessary for a given purpose, and broad sense, which refers to the articulation of safeguards to mitigate the risks to the fundamental rights and freedoms of data subjects. This double duty of care triggers two distinct judgments, one about the least intrusiveness of the data processing, the other about the least harmfulness.

Finding no. 10 and NR 8:

The principle of transparency is one of the norms which best express how informational self-determination is not limited to consent. Its reinforcement as one of the obligatory safeguards for the use of the legitimate interest lawful basis grants not only individual, but also social control over data processing activities throughout their course. This is because while notions such as reasonable efforts may possibly rule out the requirement of full disclosure at the individual level, active transparency measures should be encouraged in order to ensure accountability. It is therefore recommended that the scope of such transparency duties be made explicit by ANPD and, on the part of data processing agents, that it be seen as a measure of their own accountability.

Finding no. 11 and NR 9:

LGPD makes the right to object to data processing conditional on the existence of a "failure to comply with the law". Since the legitimate expectations of the data subject are one of the parameters that must be observed in order to ensure the lawful application of legitimate interests, a possible interpretation is that the right to opt-out could be triggered under the argument that the data subject's trust has been frustrated, which will be contextually balanced with the other interests at stake. Otherwise, such parameters would be too limited in scope. This is an interpretation that avoids an asymmetrical regime between the lawful bases, more specifically in relation to consent, since, in this case, the data subject holds the one-sided right to revoke it at any time. An interpretation that places consent and legitimate interests on an equal footing, as they were articulated in Article 7, is also a matter of internal consistency of the law. Nevertheless, it is reiterated that the right to opt-out is not absolute and may be overruled if the analysis of the specific case reveals that the interests of the controller or of third parties outweigh the legitimate expectations and the rights and freedoms of the data subject. It is also important to point out that, regardless of it being a legal obligation, providing the possibility of opting out of data processing operations should also be seen as a good practice, a safeguard to minimize impacts.

Finding no. 12 and NR 10:

In terms of assessments carried out prior to adopting the lawful basis of legitimate interests, the requirements of Article 10 point out to the obligation to conduct a legitimate interest assessment (without establishing a specific form). A data protection impact assessment, at this point, is not considered mandatory by LGPD, even though ''the Authority *may* require the controller to present a data protection impact assessment when the processing is based on a legitimate interest'' (Article 10, §3º). This interpretation seeks to avoid a "trivialization" of DPIAs, considering it is the data processing activity itself, and not the lawful basis, that defines the level of risk in a given situation.

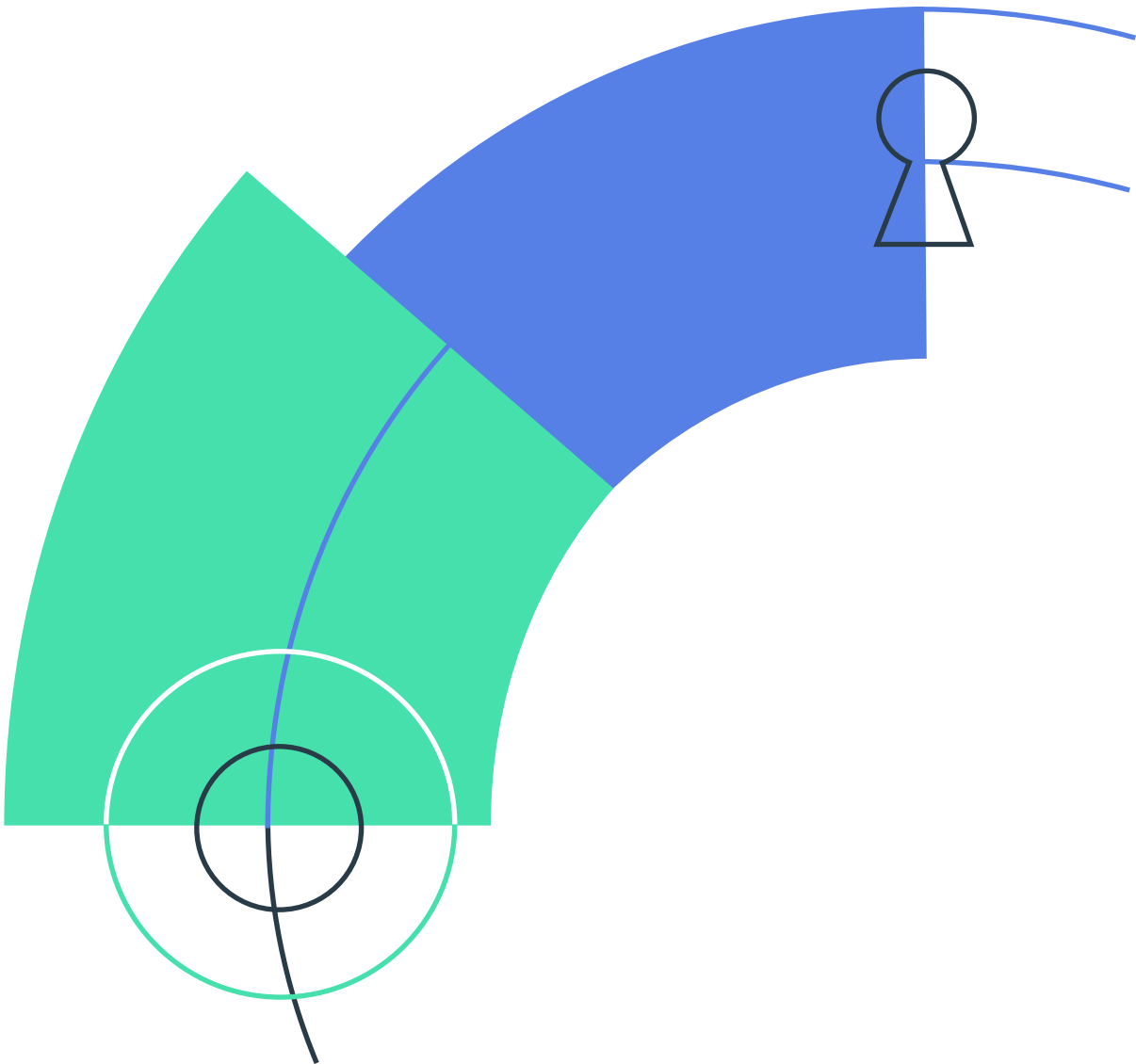


TABLE OF CONTENTS

INTRODUCTION AND METHODOLOGICAL NOTES

The provision of legitimate interest as a lawful ground for processing of personal data first appeared in Directive 95/46/EC of the European Parliament and the Council of the European Union.[6] Its legal definition, which has influenced other definitions in later pieces of legislation around the world[7], focuses on a balancing exercise: on the one hand, stand the legitimate interests of the controller (or third parties); on the other, there are the interests and fundamental rights and freedoms of the data subject. How exactly to achieve this balance, however, is not something that the law specifies in detail.[8] Thus, it is an open provision, subject to interpretations as to its reach and scope.

For this reason, there is ongoing reflection about the application of legitimate interests and its position in relation to other lawful bases. Considering the inexistence of hierarchy between these grounds for processing, such questions, among many others, arise:

- Would it make sense to consider legitimate interest as either a default basis or a last resort?
- Would legitimate interest be an "advantageous" lawful basis, in the sense of carrying fewer legal constraints, or, on the contrary, does it entail a greater ''argumentative burden'' to the controller?
- In which concrete cases is the application of legitimate interest as a lawful basis for processing appropriate?

These are some of the questions that this paper will seek to address. In the first section, the process that culminated in the final version of the legitimate interest provision in the Brazilian General Data Protection Law (Act No. 13.709/2018) is described, with highlights to the different contributions made by civil society[9] throughout the discussion of the original Draft Bill and the progress of Bills 4060/2012, 330/2013 and 5276/2016.

---

6 According to Directive 95/46/EC, item (30): "Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding".

7 As will be seen in this policy paper in relation to legitimate interest in Brazilian law.

8 There are suggestions on how to go about this, for example, that the "proper balance" between the interests would be found by the controller building a robust data protection compliance program. BALBONI, P., Cooper, D., IMPERIALI, R. & MACENAITE, M. **Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection.** International Data Privacy Law, 2013, 3 (4), p. 244-261.

9 Civil society is understood here as entities or individuals from academia, the third sector, and the private sector. This is, for example, the division adopted in the Internet Steering Committee to differentiate the representatives of the governmental sphere from the civil society sphere. Available at: https://cgi.br/members/. In some cases, however, especially when it is referred to by members of NGOs or research center, the term ''civil society'' is to be understood as excluding private companies and/or associations that defend private interests.

After this contextualization, the second section of the paper will be dedicated to an analytical study of the legitimate interest provision, addressing aspects such as (i) the rights and duties triggered by Article 10, both for the data subject and for the controller and third parties; (ii) the argumentative burden created by the provision in relation to some of the data protection principles, such as necessity/minimization and transparency; (iii) and, finally, whether there is a need for specific documentation, and if so, which one.

Finally, the third part of this paper will simulate hypothetical cases where the legitimate interest basis may apply, in order to combine theory and practice. Our goal is to highlight how legitimate interests may be relied upon in different scenarios and thereby examine how this concept comes to life in various ways. In all, 26 fictional cases, pertaining to 10 different areas, are explored. Then, the paper proposes a generalization for each area, indicating the ''temperatures'' of each phase of the legitimate interest assessment. In that sense, the objective of the practical part of this document is not to categorically state whether legitimate interest applies in hypothetical cases, but rather to point out which aspects of the prior assessment may deserve special attention.

SECTION A - THE DISPUTES DURING THE DRAFTING OF THE BRAZILIAN GENERAL DATA PROTECTION LAW

A.1) DRAFT BILL PHASE

The process that culminated in the approval of Act No. 13.709/2018 (Brazilian General Data Protection Law) lasted about 8 years, since the publication of the first Draft Bill[10] submitted for public consultation by the Ministry of Justice, in December 2010. The notion of a legitimate interest provision, however, was not present from the beginning. An analysis of the first version of the Draft Bill, as well as the initial versions of bills 4060/2012[11], authored by then House representative Milton Monti (PR-SP), and 330/2013[12], by then Senator Antônio Carlos Valadares (PSB/SE), shows that there was no lawful basis of legitimate interest as a ground for processing personal data.[13]

Actually, the initial texts, especially the Draft Bill, were centered around consent, until then considered as the prevalent lawful basis, with priority over the others.[14] Article 9 of the Draft Bill provided, as a rule, the need for "free, express, and informed consent of the subject" and listed other grounds[15] as exceptions. In the bills from the House of Representatives, on the other hand, consent was presented as the lawful basis for the processing of sensitive data[16] and personal data of children and adolescents[17].

---

10 MINISTRY OF JUSTICE Draft Bill of the Brazilian Personal Data Protection Law.Brasília, DF, December 2010. Available at: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf

11 NATIONAL CONGRESS Bill 4060/2012. Provides for the processing of personal data, and makes other provisions. Brasília, DF, 2012. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012

12 FEDERAL SENATE Bill 330/013. Provides for the protection, processing, and use of personal data, and makes other provisions. Brasília, DF, August 2013. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927883&ts=1567533189767&disposition=inline

13 As to Bill 330/2013, it had the following provision: "Article 12. The interconnection of personal data must meet the following requirements: I - adequacy to legal or statutory purposes and to the legitimate interests of database owners and managers; [...]". However, the bill makes no further mention of the idea of legitimate interests, in the sense of defining it, nor does it refer to the concept in its justification.

14 BIONI, Bruno Ricardo. ***Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil***. GPoPAI-USP, 2016. Available at: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil

15 Such hypotheses were: contractual or legal obligation, data with unrestricted public access, exercise of specific functions of the Government powers, historical, scientific or statistical research, protection of the life or physical integrity of the data subject or third party when consent is not possible, exercise of the right of defense or cases concerning the subject's breach of obligations under the Consumer Protection Code.

16 In Bill 4060/2012, the provision was as follows: "Article 12. The processing of sensitive personal data, when not requested by the data subject, will only start upon authorization by the data subject, by any means that allows the statement of his or her will, or in the event of legal imposition". On the other hand, in Bill 330/2013: "Article 4 The following principles apply to the processing of personal data: IV - prior and express consent of the data subject as a requirement for collection, when dealing with sensitive data or international data interconnection carried out by private databases (Article 10);"

17 The initial wording of Bill 4060/2012 as to this point was: "Article 17. The processing of personal data of children shall only be possible with the consent of their parents, legal guardians or by legal imposition".

The movements around the insertion of the legitimate interests lawful basis started during the public consultations to which the Draft Bill was submitted. In the first round[18], which lasted about five months, 794 contributions were received, mostly from companies, NGOs and research centers. As a study published by the Brazilian Direct Marketing Association - ABMED indicates, at that time there were few contributions or suggestions related to the notion of legitimate interests.[19] It was not yet at this time that the lawful basis emerged.

This only occurred in July 2015, when the first substitute amendment[20] to Bill 330/2013 was presented by Senator Aloysio Nunes to the Senate Committee on Science and Technology (CCT). It was the first time that the lawful bases for data processing were included in the form of parallel items, with no prevalence of one over the other, and with the addition of the legitimate interest ground.[21] This did not happen by chance. At that same time the second round of public consultations on the Ministry of Justice Draft Bill was taking place, and there was an interest in harmonizing the Senate proposal with the one that would later be introduced to the House of Representatives.[22] An indication in this regard was the participation of then Senator Aloysio Nunes, Rapporteur of Bill 330/2013, in the event that launched the post-public consultation version of the Ministry of Justice Draft Bill, when he stated that the proposal from the Executive should be forwarded, with constitutional urgency, to Congress[23].

At the time of the second public consultation, which had more than 1,800 contributions,[24] both

18 Held in partnership with the Brazilian Observatory for Digital Policies of the Center for Technology and Society of the Getúlio Vargas Foundation in Rio de Janeiro.

19 The only one of them that corresponds to the idea of legitimate interests that was later incorporated is NOKIA's contribution. According to the report: "Finally, Nokia also points out that it is necessary that the hypotheses for waiver also cover cases in which the processing is necessary for purposes of legitimate interests of the data controller or of a third party to whom the data are communicated, with the fundamental rights and freedoms of the data subject always being preserved". Available at: https://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf

20 FEDERAL SENATE Opinion 2015. Brasília - DF (Federal District), Rapporteur Senator Aloysio Nunes Ferreira. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927917&ts=1567533189932&disposition=inline

21 Each item is a discriminative element of the Article or paragraph. Thus, when there is more than one item, they are equidistant from the core arrangement represented by the Article, within the logical structuring of the regulated subject. The normative reading calls for the use of structural interpretation guidelines, considering the system as an organic totality in perennial dynamism. Rules of law contain a reason and a meaning that embody a certain intentionality. Therefore, the legislator's choice to logically distribute the text in a certain way is not trivial. See: MENDES, Gilmar Ferreira. ***Hermenêutica Constitucional e Direitos Fundamentais.*** Brasília: Brasília Jurídica, 2000, p. 82-84; PENNA, Sérgio; MACIEL, Eliane Cruxên. ***Técnica Legislativa: orientação para a padronização de trabalhos.*** Brasília: Consultoria Legislativa do Senado Federal, 2002, p. 124, 125.

22 RIELLI, Mariana. *O processo de construção e aprovação da Lei Geral de Dados Pessoais: bases legais para tratamento de dados em um debate multissetorial.* **Revista do Advogado**, a. XXXIX, n. 144., p. 07-14, 2019.

23 PEDUZZI, Pedro. MJ finalizes a new version of the draft bill on internet data protection. **Agência Brasil,** Brasília, October 19, 2015. "The idea of giving urgency to the matter had already been defended by opposition senator Aloysio Nunes (PSDB-SP), during the opening of the seminar. 'I suggest that the bill be submitted by the president [Dilma Rousseff] with constitutional urgency to the Legislature, to free us from certain hindrances that cause interesting initiatives to be lost in the National Congress,' argued the PSDB senator." Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet>. Accessed on: December 14, 2020.

24 According to the InternetLab study, there were split stances regarding legitimate interests, although there were no entities that rejected the proposal as a whole. On the one side, companies such as Claro, Vivo, Sky, and business associations such as Febraban and Brasscom, among others, brought contributions that included the hypothesis of legitimate interests based on the logics of tacit consent. Part of the argument focused on the idea of "consumer fatigue" in relation to the consent lawful basis. The companies defended legitimate interest as an alternative that facilitates data processing in situations in which there would be no undue impact on the rights of individuals. However, the issue of the subject's interests is not central to these contributions. Other contributions, such as those of Marcel Leonardi, stressed the fact that legitimate interest has been part of the European legislation on the subject since 1995, so that it would create a mismatch and a delay if Brazil elected not to follow this same path. Entities such as ITS Rio and the Research Group on Public Policies for Access to Information (*Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação* - GPoPAI) focused their contributions on the need, in case of a new lawful basis of legitimate interests, for it to be accompanied by a proportionality test, in order to ensure the rights of data

points were discussed in depth - the non-hierarchization of lawful bases, at least in the case of non-sensitive data, and the inclusion of the legitimate interest lawful ground, following international examples. Once the proposal from the Executive was finally consolidated, it was sent to the House of Representatives as Bill 5276/2016 with nine distinct lawful bases, including consent and legitimate interest, all hierarchically equivalent. Thus, as of 2016, all of the different proposals being discussed both in the Senate and in the House included a legitimate interest lawful basis, which has been somewhat refined since then.

FINDING NO. 1

Previously an unknown legal concept, upon its introduction during the public debates that preceded the passing of LGPD, the legitimate interest provision was placed on an equal footing with the other lawful grounds for personal data processing, particularly consent, which had been, up until that point, the main (and, in some cases, only) lawful ground adopted by early drafts of the legislation. Following international examples, the final text doesn't establish any hierarchy whatsoever among the ten (10) lawful grounds described in Article 7.

A.2) CONGRESS PHASE

Senator Aloysio Nunes' substitute amendment was relatively economical in terms of the legitimate interest provision, which was accompanied by the following condition: "provided that they do not override the interests or the fundamental rights and freedoms of the data subject".[25] It is interesting to note that this is somewhat very similar to legitimate interests under the General Data Protection Regulation (GDPR) and Directive 95/46-1995 of the European Parliament. These similarities, as well as some differences in relation to the Brazilian law, will be addressed below.

The text that originated in the Ministry of Justice and was then introduced to the House of Representatives, after the second public consultation took place in 2015, included a more ''robust'' legitimate interest provision, with a series of paragraphs on the following aspects: consideration as to the data subject's legitimate expectations (Article 10, paragraph 1), adoption of transparency measures and opt-out (Article 10, paragraph 2), respect for the principle of minimization and adoption of anonymization measures, when compatible with the purpose of the processing (Article 10, paragraph 3), and, finally, the possibility that the "competent body" (Article 10, paragraph 4) may request a data protection impact assessment for operations based on the legitimate interest lawful ground.[26]

One sees the influence of contributions such as those from the Research Group on Public Policies

subjects in a situation where their consent is relaxed. Thus, suggestions such as the inclusion of mandatory data anonymization as a way to protect the data subject were made. In: INTERNETLAB. **What is at stake in the debate over personal data in Brazil? Final report on the public debate promoted by the Ministry of Justice on the draft bill on personal data protection.** São Paulo, SP, 2016. Available at: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

25 FEDERAL SENATE Opinion 2015. Brasília - DF (Federal District), Rapporteur Senator Aloysio Nunes Ferreira. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927917&ts=1567533189932&disposition=inline

26 BRAZIL. National Congress. Bill 5276/2016. Provides for the processing of personal data to ensure the free development of personality and human dignity. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01jp5ibgm0xjo61lldo1ia7vrk7517713.node0?codteor=1457459&filename=PL+5276/2016

for Access to Information (GPoPAI) and from Instituto Tecnologia e Sociedade (ITS-Rio),[27] both which suggested changes in the Draft Bill to include mentions of legitimate expectations, necessity/minimization, transparency and security measures, including anonymization, among others. Therefore, it is noticeable that the submission of the Ministry of Justice Draft bill to public consultations resulted in a version of legitimate interests that provides certain specific parameters for the balancing assessment between the interests of the controller and the legitimate expectations and rights and freedoms of the personal data subject.[28]

The first substitute amendment from Rapporteur Orlando Silva (PCdoB-SP)[29] to the Special Commission designated to discuss the matter in the House of Representatives was presented after a round of public hearings, among which one specifically addressing the legitimate interest provision.[30] The Rapporteur presented a slightly changed version of the initial text submitted to the House, removing the mention of anonymization and security measures from the Article referring to legitimate interest.

On the other hand, the maintenance of the other paragraphs, which referred to the legitimate expectations of data subjects, as well as the principles of necessity and transparency, was the subject of dispute until the final moments before the presentation of the substitute amendment[31].

The Rapporteur reinforced two aspects in the opinion that accompanied his substitute amendment: (i) first, that the legitimate interest provision corresponded to an European trend existing since the 1990s and that it met legitimate private sector needs; (ii) that, on the other hand, the provision is not to be

27 "The major concern with the advent of the new legitimate interest exception is that this exception undermines, or even weakens, the normative pillar of the draft bill, i.e., consent as the general rule for the processing of personal data [GPoPAI]. Therefore, proponents who controversially debated this new exception end up suggesting that the law should expressly provide for an assessment to weigh the interests involved, which should take a number of factors into account [ITS-Rio]". INTERNETLAB. **What is at stake in the debate over personal data in Brazil? Final report on the public debate promoted by the Ministry of Justice on the draft bill on personal data protection.** São Paulo, SP, 2016. Available at: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

28 BIONI, Bruno Ricardo. ***Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil***. GPoPAI-USP, 2016, p. 50-51. "From the standpoint of normative consistency centered on the general rule of consent and informational self-determination, a more rigid system of checks and balances ultimately does not drain out the promise that citizens should exercise control over their personal data. For instance: I. transparency mechanisms regarding the processing of personal data in case of legitimate interests, together with means in which the data subject may object to processing; II. security standards that minimize privacy risks, such as data anonymization, and further: III. safeguards that include the power to audit such market practices through the requirement of data protection impact assessments. Available at: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil

29 BRAZIL. Special Commission for Issuance of an Opinion on Bill No. 4060, of 2012. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=161610896C391A39888C72EEE6DBA082.proposicoesWebExterno2?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012

30 According to the report from Rapporteur Orlando Silva, the public hearing was composed of representatives of the Brazilian Federation of Banks - FEBRABAN, the Brazilian Institute of Digital Law - IBDDIG, the non-governmental organization ARTIGO 19 and a specialist in privacy and data protection and professor of Digital and International Law at Mackenzie Presbyterian University.

31 DATA PRIVACY BRASIL. ***Observatório da Privacidade****: Memória da LGPD.* Available at: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/. Transcription of the statement by Beatriz Barbosa, Coordinator of Intervozes. "There was an Article that dealt with one of the lawful basis for processing personal data and that, for civil society, was of great concern, which is the hypothesis of legitimate interests of companies and other players to process this data. This has always been a concern for civil society, that this lawful basis would not be a blank check for companies to process data the way they want, so we wanted to include some conditions on this part. We had already gone to the negotiation table and it didn't work, we did not succeed in including this, because the companies hadn't left the negotiation table, but some sectors of civil society were very concerned. I remember that half an hour before Representative Orlando filed his substitute amendment, the final version of the substitute amendment after the round of negotiations, the one that was going to the plenary, he was in a committee discussing another issue, talking to a consultant from the House of Representatives who was going to write the final draft for him and I came up and told him "Orlando, it won't work, this portion cannot pass the way it is, civil society will criticize your report and it will be very bad if it arrives in the plenary session with criticism from civil society.". He said: "Okay, how do you want it?" Then I took a small sheet of paper from the pad I had in my purse, wrote it down, underlined the two parts that needed to be included, and handed the paper, almost like a napkin, to Orlando. Then he took it and handed it to the consultant, who made a not very happy face. He made the inclusion at our request and that was one of the sections of the Law that ended up surviving the rest of the process''.

understood as a blank check[32] and must in all cases be balanced against the interests and rights of the data subjects.

After an opinion on the amendments presented by other members of the Special Commission,[33] the Bill went through the House Plenary[34] and the definitive provision on legitimate interests did not suffer other changes in relation to Silva's substitute amendment. Thus, the version passed by the House (and later endorsed by the Senate) included the following elements that must be present in order for legitimate interests to apply: (i) legitimate purpose: (ii) concrete situation; (iii) balancing in relation to the data subject's legitimate expectations and fundamental rights and freedoms; (iv) respect for the principles of necessity and transparency. It also provides for the possibility that the competent Authority may request a data protection impact assessment for data processing operations based on legitimate interest. Thus, the more robust version of legitimate interests survived as LGPD was passed[35].

FINDING NO. 2

The legitimate interest provision has been the subject of intense dispute. A ''tug-of-war'' has been pulled especially between the third sector (mainly NGOs, research centers and academics) and the private sector to, respectively, restrict and enlarge its scope. In the end, a common denominator was reached, based on a solution brokered mainly by academics, in which this lawful basis would be accompanied by a second provision that set the specific parameters for its application (Article 10). Thus, the Brazilian law innovated by directly providing criteria for the application of an open legal concept and, therefore, potentially bringing greater predictability to its interpretation. From its inception, there was already a concern about the ''side effects'', in terms of legal certainty, of introducing the lawful basis of legitimate interests, something that was partially remedied in the final version of the law.

SECTION B - SETTING LEGITIMATE INTERESTS IN MOTION

B.1) THE RIGHTS AND DUTIES DISENGAGED BY THE LEGITIMATE INTERESTS PROVISION: THE EQUATION OF ARTICLE 7, IX + ARTICLE 10, I + ARTICLE 37

32 A point that was extensively raised by participants of said public hearing, especially Renato Leite Monteiro, then representing Mackenzie Presbyterian University. Available at: https://www.youtube.com/watch?v=F1_NiqerjRs; 1h06min31sec - 1h30min03sec.

33 BRAZIL. Special Commission for Issuance of Opinion on Bill No. 4060/2012. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664206&filename=PPP+1+PL406012+%3D%3E+PL+4060/2012

34 _BRAZIL. Opinion on the Amendments to Bill 4060/12 in the Plenary Session. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664233&filename=PEP+2+PL406012+%3D%3E+PL+4060/2012

35 DATA PRIVACY BRASIL. ***Observatório da Privacidade: Memória da LGPD.*** Available at: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/. Transcription of the statement of Bruno Bioni, Founder and Director of Data Privacy Brasil: "In 2010/2011 there was no legitimate interests provision. In 2015, the version before public consultation had no legitimate interests provision. Then a flood of public contributions arrives, the private sector says 'I want legitimate interests', then comes the third sector and says 'I don't want legitimate interests' because this will make it too flexible. In the center of this pendulum movement you have academia, saying 'look, it is important to have this lawful basis, but it is important to have it with some restrictions, or at least with some guidelines on how this will be interpreted'. This is the typical example where the two poles, the two extremes, did not have the wording they wanted, but they had a common denominator, something they both made concessions on. I think that's very symbolic of what the Brazilian General Data Protection Law is all about".

Legitimate interests, as structured in Brazilian legislation and doctrine, gives rise to a set of rights and duties for controllers, third parties and subjects. In this item, each of these elements will be addressed.

B.1.1) LEGITIMATE INTERESTS AS A ''RIGHT'': LAWFUL BASIS FOR DATA PROCESSING

Comprehensive data protection laws are aimed not only at protecting the rights of data subjects, but also at promoting a free flow of data that gives rise to economic development.[36] This duality is at the origin of the notion of legitimate interests.[37] The very idea of this lawful basis authorizing data processing[38] gives rise to a right for the controller and third parties in the sense that, once the conditions that subject them are met, the right to handle personal data arises.

B.1.1.1) LAWFUL BASIS FOR "CONTROLLERS"

The controller, as prescribed by LGPD, is a natural or legal person, governed by either public or private law, "to whom the competence - decision-making - to process personal data is attributed (Article 5, item VI, LGPD), according to the parameters designed by the new regulation".[39] The controller is the player, within the relationship established between the parties, who decides which direction the processing of personal data will take, including in relation to third parties and processors. Thus, the controller is the first of the players to whom the expressions "necessary for" and "legitimate interests" of Article 7, IX refer. The first aspect that will be addressed in this paper is the meaning and scope of the term ''legitimate interests''.

With regard to that, Article 29 Working Party,[40] in its Opinion on the notion legitimate interests of the data controller,[41] makes some distinctions that deserve attention. The first one is between the concepts of "purpose" and "interest". Purpose is the specific objective of the data processing, while interest relates to the broader value that a data processing operation represents to its controller (or third parties, in that case). An interest, therefore, would be to guarantee the safety and health of a certain group of people, while a purpose would be certain data processing that ensures such interest, for example the installation of access controls in a premise.

A second distinction concerns the term "legitimate" (what does a legitimate interest consist of?). First of all, this interest must be *lawful,* in the sense that it must respect all laws and regulations applicable to that specific situation. Bruno Bioni illustrates this requirement with the example of the prohibition,

---

36 The law itself makes it clear that privacy and data protection must coexist with other fundamental premises, such as economic and technological development and innovation (Article 1, V) and free enterprise, free competition and consumer protection (Article 1, VI).

37 BUCAR, Daniel; VIOLA, Mario. Processing of Personal Data by "legitimate interests of the controller": initial questions and notes. In: TEPEDINO, Gustavo; FRAZÃO, Ana. OLIVA, Milena Donato. (Coord.). ***Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro***. Thomson Reuters, 2019, p. 469.

38 The historical construction of the lawful bases for data processing is related to the idea of lawfulness, a condition for the processing that is mentioned in documents such as Convention 108 of the Council of Europe and the Directive on Privacy Protection and Transborder Flows of Personal Data, of the Organization for Economic Cooperation and Development (OECD).

39 BUCAR, Daniel; VIOLA, Mario. Processing of Personal Data by "legitimate interests of the controller": initial questions and notes. In: TEPEDINO, Gustavo; FRAZÃO, Ana. OLIVA, Milena Donato. (Coord.). ***Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro***. Thomson Reuters, 2019, p. 477.

40 The Article 29 Working Party was, until the coming into force of the General Data Protection Regulation (GDPR), the body responsible for interpreting, in a non-binding manner, the provisions of Directive 95/46/EC and other privacy and data protection matters.

41 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014.

even with consent, to collect pregnancy or HIV-related data in employment situations.[42] Furthermore, the lawfulness of the interest is also related to its *articulated* character, namely that it must be related to a concrete situation and, therefore, not speculative, a condition derived from the very principle of purpose limitation ("legitimate, specific purposes"[43]).

In the case of the Brazilian General Data Protection Law, specifically, both the interest and the purpose (the latter by virtue of the head provision of Article 10[44]), must be legitimate and concrete.

FINDING NO. 3 AND NR 1

The adjective "legitimate" is a recurring qualifier throughout LGPD. It comes, for example, with the definition of the principle of purpose limitation (''processing for legitimate, specific, explicit and informed purposes''). In this case, however, it has a more restricted meaning than in the case of a ''legitimate'' interest: it means that the specific data processing purpose should not be prohibited by law or other regulation. In the case of the lawful basis of legitimate interests, on the other hand, this term triggers an analysis of compliance with the conditions described in Article 10 for an interest to be considered legitimate. It is recommended to take into consideration such a distinction in terms of the scope and range of the term.

B.1.1.2) LAWFUL BASIS FOR "THIRD PARTIES"

Legitimate interests, however, is not only applicable to the controller, but also to the figure of the "third party".[45] This means that the controller may perform data processing that is not in its own interest (or exclusively in its own interest), but in the interest of a third party or of society as a whole. For instance:

(i) A striking example would be the application of the legitimate interest ground to combat fraud. At one time it is in the interest of a company to prevent, for example, the credit card it offers from being defrauded, and it is in the interest of the banking and financial system, as well as of society, that such fraud does not occur. A possible sharing of data among agents of the financial system (other than the financial institution that provides the service to the subject and that would be the controller) would fall under the figure of third parties;

(ii) Another clear example of legitimate interest of third parties is due diligence in merger and acquisition processes, where third parties who have no pre-established relationship with the data subjects have a legitimate interest in processing this data to assess [46] the feasibility of the

42 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd ed.): chapter 5.

43 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014**, p. 25.

44 BRAZIL. Act no. 13.709, of August 14, 2018. Brazilian General Data Protection Law (LGPD). "Article 10. The legitimate interests of the controller may only ground processing of personal data for legitimate purposes, considered as of concrete situations [...]".

45 BRAZIL. Act no. 13.709, of August 14, 2018. Brazilian General Data Protection Law (LGPD). "Article 7 The processing of personal data may only be performed in the following hypotheses: [...] IX – when necessary to meet the legitimate interests of the controller or of a third party, except in cases of prevalence of the rights and fundamental freedoms of the subject which require the protection of the personal data; or [...]". (emphasis added).

46 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de

corporate transaction;

(iii) A hypothesis in which the legitimate interest of a third party also applies is in the processing of personal data by computer emergency response teams and computer security incident response teams. Recital 49 of GDPR expressly states that, for the purposes of network and cyber security assurance, legitimate interest is an applicable lawful basis, and even cites CERTs and CIRTs (English acronyms for said teams) as third parties that could therefore rely on legitimate interests;

(iv) Another example would be the publication of data for transparency and accountability purposes, even in cases where it is not required by the Access to Information Act.[47] In these cases, the prevailing interest is not that of the controller that discloses the data in question, but of other players, such as journalists, employees, and society as a whole;[48]

(v) Another possible case of application of legitimate interests of a third party would be the sharing of data between the controller and third parties interested in its use for academic purposes. A more concrete example is the sharing of data between justice system entities, such as the Public Defender's Offices, the Prosecution Offices, and the Judiciary, and graduate students, based on the legitimate interests of these third parties to conduct academic research on access to justice in the country.[49]

It should be noted that in all cases, the assessments relating to the lawful basis, which will be detailed below, must be performed in order to confirm that it is adequate.

The application of legitimate interests of third parties, however, is not strictly limited to the aforementioned hypotheses. Considering that LGPD does not provide a specific definition of third party, in principle, the interpretation of who this subject may be should not be restricted. The examples mentioned above are cases in which the lawfulness of third parties is more evident, but do not intend to make an exhaustive list.

If, on the one hand, the provision on third parties as one of the subjects that can mobilize the lawful basis of legitimate interests in LGPD comes close to GDPR, on the other hand, it does not define, like the European regulation, who a third party is and when it fits into the figure of recipient. The recipient is defined by the GDPR as the natural or legal person, public authority, agency, or other body to whom the personal data are disclosed, whether a third party or not.[50] To illustrate this figure, the European Data Protection Board[51] uses the example of the payment of salaries of employees of the European Union

Janeiro, 2020 (2nd ed.): chapter 5, p. 240.

47 Take the case, for example, of Public Defender's Offices, which are not listed in the Access to Information Law (LAI), but in view of the legal assistance they provide, are subject to the rules contained in it for the purposes of social control. The same logic can be applied to some trade associations, especially those with the purpose of self-regulation and certification as a basis to legitimize themselves as a normative body.

48 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014, p. 27.

49 It is important to note that LGPD has not fully exempted data processing activities for academic purposes from its scope of application (Article 4, II, "b"), to the extent that such activities must comply with Articles 7 and 11. In other words, such data processing activities must be based on one of the lawful bases contained in these provisions of the law. The Article in question: "Article 4 This Law shall not apply to the processing of personal data: [...] b) of academic nature, in which case Articles 7 and 11 of this Law apply."

50 EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation 2016/679. General Data Protection Regulation. "Article 4 (9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2 However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.".

51 "An illustrative example may be salary payments of officials of the EU institutions and bodies. The salary slip does not only go

(EU) institutions. In this case, the payslip is not sent to the employee only, but also to Eurostat (the EU's statistical organization), which in this case is a recipient. The regulation then goes on to define third party as a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.[52]

FINDING NO. 4 AND NR 2

The provision that the legitimate interest can be of a third party was introduced in the version of the Data Protection Draft Bill submitted to Congress, which then became Bill 5276/2016. Unlike GDPR, the Brazilian law does not provide a definition of third party, nor does it introduce the idea of a ''recipient''. So, it is even more challenging to interpret the scope of the lawful basis of legitimate interests of a third party, something that needs to be urgently addressed by the Brazilian Data Protection Authority (ANPD). Examples of who can be a third party in a data processing operation range from natural persons and legal entities to the wider, more abstract notion of a collectivity. It is advisable to i) treat these categories of third parties differently, as they entail different potential risks for data subjects, and ii) reinforce that, in all cases, the lawful basis must always apply to a concrete situation. In this sense, it is incumbent upon the controller to assess whether the interest of the third party is, in fact, legitimate.

B.1. 2) THE DUTIES ARISING FROM THE LEGITIMATE INTEREST PROVISION

B.1.2.1) THE SCOPE OF ARTICLE 10 OF LGPD

Article 10[53] of the Brazilian General Data Protection Law is the provision that describes the conditions that must be met for the use of the legitimate interests lawful basis. As mentioned earlier, it appeared first in the draft bill that gave rise to LGPD, especially the version from the second round of public consultations promoted by the Ministry of Justice in 2015.

The content of the Article in question shows a concern, expressed by organizations such as GPoPAI and ITS-Rio at the time, with the excessive discretion of the players who would use this lawful basis: the idea of a "blank check" for controllers to handle personal data as they saw fit. In response to this concern, suggestions were made to incorporate elements similar to those present in European regulations, as had already been established by interpretation of the Article 29 Working Party[54] and reinforced in GDPR

to the employee, but also to the institution or body where he or she works, and Eurostat receive the data" (compiled). EUROPEAN DATA PROTECTION SUPERVISOR. **Glossary.** Available at:: https://edps.europa.eu/data-protection/data-protection/glossary/r_en

52 EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation 2016/679. General Data Protection Regulation, "Article 4 (10): 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;".

53 BRAZIL. Act no. 13.709, of August 14, 2018. Brazilian General Data Protection Law (LGPD). "Article 10. The legitimate interests of the controller may only ground personal data processing for legitimate purposes, considered as of concrete situations, including, among others:
I – support and promotion of activities of the controller; and
II - protection, in relation to the subject, of the regular exercise of his rights or rendering of services that benefit him, observing his legitimate expectations and the fundamental rights and freedoms, on the terms of this Law.
Paragraph 1 When the processing is based on the legitimate interest of the controller, only the personal data strictly necessary for the intended purpose shall be processed.
Paragraph 2 The controller shall take measures to ensure the transparency of the data processing, based on his legitimate interest.
Paragraph 3 The national authority may request the controller a data privacy impact assessment, when the processing is grounded on a legitimate interest, with due regard for trade and industrial secrets.

54 Still under Directive 95/46/EC.

Recitals 47 and 48[55].

As important as understanding that the interests of controllers and third parties and data subjects must be weighed as a general guideline, is to understand the function and scope of Article 10 of LGPD. In that sense, at least three interpretive issues deserve to be addressed:

B.1.2.1.1) DO THE CONDITIONS FOR THE APPLICATION OF LEGITIMATE INTERESTS OUTLINED IN ARTICLE 10 REACH ONLY THE CONTROLLER? OR THIRD PARTIES AS WELL?

While Article 7 of LGPD, which lists the 10 lawful bases that can be employed to justify personal data processing, mentions the legitimate interests of ''the controller or third parties'', Article 10, which provides the conditions for the application of the legitimate interests lawful ground, makes no mention of third parties.

A first way to understand Article 10 is through a restrictive interpretation, according to which the conditions it sets concern exclusively the legitimate interests of the controller, not including those arising from third parties. This restrictive interpretation could be extracted from a literal-grammatical interpretive method, which assumes that the words that make up the normative command represent what they strictly describe. This is a valid conclusion which, however, is far from being the only possible interpretation of the provision.

A systematic[56] and teleological interpretation[57] of Article 10, which would also reach the third party, is possible.[58] It avoids a different valuation among those addressed by the rule, and thus achieves a more uniform application of the lawful basis of legitimate interests, regardless of who benefits from it. A preferable hermeneutical result, so as not to affect the very substance of the provision,[59] even more so when the normative arrangement itself does not justify why there should be the imposition of different duties for the controller and third parties.

In this regard, it is important to recall that Article 10 was designed with the intent to govern any and all types of legitimate interest application, regardless of who mobilizes it. This broader interpretation of the scope of Article 10 is in line with the spirit of a comprehensive data protection law, which means to be a ''statute of information''[60] that establishes, as a rule, duties and rights in a *horizontal and symmetrical* way between the different players of this informational ecosystem. At the same time, it stems from a

---

55 Recital 48 of GDPR states: "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.". EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. Regulation 2016/679. General Data Protection Regulation.

56 On the various current hermeneutical techniques and their disregard to the scholastic method of the prevalence of one method over the other, especially the literal-grammatical: GRAU, Eros Roberto. ***Ensaio e Discurso sobre a Interpretação/Aplicação do Direito***. 5th ed. Malheiros Editores, p. 43

57 Teleological interpretation means to consider the global purposes served by the law, which based on coherence, relies on the identification of a rule under the normative scope and its connection with other rules. In:LARENZ, Karl. ***Metodologia da Ciência do Direito***. Translated by José Lamego, Fundação Calouste Gulbenkian, Lisbon, 3rd ed, p. 464.

58 LARENZ, Karl. ***Metodologia da Ciência do Direito***. Translated by José Lamego, Fundação Calouste Gulbenkian, Lisbon, 3rd ed, p. 450.

59 ENGISCH, Karl. ***Introdução ao pensamento Jurídico***. Translated by J. Baptista Machado Fundação Calouste Gulbenkian, Lisbon, 8th ed. 2001, p. 313.

60 LGPD started a new logics, which seeks to regulate an informational order, something that did not exist previously, in such a systematized and harmonic way. See: SCHERTEL, Laura Mendes. Lecture "International Seminar - Brazilian General Data Protection Law: on the way to effectiveness". Superior Court of Justice, 2019. Available at: <https://www.youtube.com/watch?v=0E0USaGQ6h8>

reading of LGPD in its entirety and not just isolated sections.[61]

B.1.2.1.2) ARE THE CONDITIONS DISTRIBUTED THROUGHOUT THE ITEMS AND PARAGRAPHS OF ARTICLE 10 CUMULATIVE OR ALTERNATIVE?

A second interpretive question to be addressed about Article 10 concerns the conditions distributed throughout its items and paragraphs: would they be cumulative or alternative conditions? The room for interpretation arises from the fact that the head provision of the Article in question states that legitimate purposes will be "considered from concrete situations, which include, but are not limited to: [...]".

There are two possible interpretations: (i) that the items listed subsequently, as well as others that are not described, could each give rise to the application of legitimate interests separately, or (ii) that both items must subsequently be complied with as requirements for the application of this lawful basis. In other words, because the elements of ''respect for the legitimate expectations and the fundamental rights and freedoms of the data subject'' are only mentioned in one of the items, there would be room to interpret that the ''promotion of the controller's activities'' would suffice to trigger the application of the lawful basis.

However, if one adheres to the notion that specific provisions of a norm must be consistent with other provisions of the same norm but, mainly, with the norm in its entirety, given the fact that legal rules are intended to fulfill certain purposes by completing other provisions in a finalist manner, this understanding would be inadequate.[62] In this case, the central objective of Article 10 is to create parameters that guide the application of the legitimate interests provision by promoting a balance of interests, as well as expectations and rights.

For the purpose of argument, even if one relies on a literal method of interpretation, in this specific case the connective device between the two items of Article 10 is ''and'', rather than ''or'', which also suggests that they must be read and interpreted together in order to avoid stripping the provision of its very essence.

FINDING NO. 5 AND NR 3

Employing different techniques of legal hermeneutics in order to interpret Article 10, an adequate conclusion is that this provision (i) refers to both the legitimate interests of the controller and of third parties and that (ii) the list of items and paragraphs of the Article imposes cumulative, and not alternative, conditions. This ensures an uniform application of the lawful basis, regardless of who relies on it. It also does not undermine the function of Article 10 as a whole, which is to promote the balancing of the interests of the controller or third parties with those of the data subject. A systematic and teleological interpretation of Article 10 is in line with the very spirit of a general data protection law, which is to establish, as a rule, duties and rights in a horizontal and mostly symmetrical manner.

B.1.2.1.3) DO THE OBLIGATIONS DERIVED FROM THE LAWFUL BASIS OF LEGITIMATE INTERESTS ALSO APPLY TO MICRO AND SMALL BUSINESSES?

61 GRAU, Eros Roberto. ***Ensaio e Discurso sobre a Interpretação/Aplicação do Direito***. 5th ed. Malheiros Editores, p. 44.

62 ENGISCH, Karl. ***Introdução ao pensamento Jurídico***. Translated by J. Baptista Machado Fundação Calouste Gulbenkian, Lisbon, 8th ed. 2001, p. 141.

As the purpose of this paper is to propose interpretations that can guide data processing activities of companies and other entities of different sizes, it is important to start from an assumption presented by LGPD itself: the potentially differentiated regime for micro, small, and innovative or disruptive businesses, such as startups. This gives room for asymmetric regulation when the size and economic capacity of an enterprise justify a more lenient regulatory regime, so as not to harm free competition (Article 2, VI, of the LGPD), without leaving aside the element of risk of the data processing activity.

As provided for in Article 55-J, XVIII, the Brazilian Data Protection Authority has authority to enact simplified and differentiated rules, guidelines, and procedures, including as to deadlines, so that these business models can adapt to the law. This provision is in line with one of the core objectives of the LGPD, which is to harmonize the protection of data subjects' personal data with economic development and innovation.

In this sense, it will be up to the Authority to delimit a specific normative regime for this group of enterprises, which may include more flexible procedures also with regard to legitimate interest. An example of what could happen in practice is a less strict interpretation of the requirement to document processing activities based on legitimate interests. However, it is important to stress that the differentiated regime is contingent on further regulation by the Authority and, until that eventually happens, all rules apply to all business models, i.e., they are horizontal.

FINDING NO. 6 AND NR 4

LGPD was built on the basis of the need to balance the protection of personal data and the data subject's fundamental rights with economic development and innovation, a dichotomy that is also at the core of the legitimate interest provision. In this sense, the law established the possibility for a differentiated regime for small businesses, including alternative procedural matters such as deadlines, to be defined by the Brazilian Data Protection Authority. This differentiated procedure can be applied to legitimate interests, such as for example, by not requiring specific documentation, or by relaxing the components of the Legitimate Interest Assessment. However, it is important to point out that this is an open-ended possibility, so that, in principle, the provisions of the law apply horizontally to all data processing agents.

B.2) REINFORCED ARGUMENTATIVE BURDEN WITH RESPECT TO SOME OF THE PRINCIPLES

When one looks at the conditions that must be met to apply the legitimate interests lawful basis, it is clear that what they create for the controller and third parties is a strengthened argumentative burden in relation to some of the principles of the legislation, such as purpose limitation, necessity, and transparency.[63] The LGPD principles, described in Article 6, have horizontal application and spread out to all provisions regardless of lawful basis, but in the case of legitimate interests, the legislator opted to highlight some of them.[64]

Article 10 serves as a ''modulation barrier'' to the vote of confidence given to the data processing agent, who will have discretion in assessing whether its own interest is legitimate. To balance this

63 DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. United Kingdom, 2017. Available at: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

64 BUCAR, Daniel; VIOLA, Mario. **Processing of Personal Data by "legitimate interests of the controller": initial questions and notes.** *In Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro.* Thomson Reuters, 2019, p. 476.

discretion, LGPD articulated parameters of accountability (Article 6, X) that can be traced back to the following principles.

B.2.1) PURPOSE LIMITATION AND ADEQUACY

The first two principles from which the conditions for the applicability of legitimate interests can be derived are purpose limitation (Article 6, I) and adequacy (Article 6, II). There must be a specific, well delineated purpose to each processing activity, which in turn must be fully compatible with said purpose, according to each context.

B.2.1.1) CONCRETE SITUATION

As mentioned before, the legitimate interest (as well as the purpose, in the Brazilian case) must be concrete, a provision that was was the result of cooperation at the time the Draft Bill was under discussion.[65] The existence of a concrete situation represents a further requirement that the legitimate interest lawful basis should not be conceived as a "blank check". For this reason, situations that may or may not exist in the future, or that are abstract and generic, are not considered an acceptable purpose that would justify the use of the lawful basis of legitimate interests.

This requirement is directly related to the principle of purpose limitation, since while it is true that the legitimate interests lawful basis is not linked to an *a priori* purpose,[66] as is the case with other grounds for processing[67], this does not mean that it does not require a specific purpose for *each situation* of personal data processing, observed concretely. At the same time, data processing carried out on the basis of legitimate interests must be appropriate to the specific purpose intended.

FINDING NO. 7 AND NR 5

Relying on legitimate interests as a lawful basis for processing creates a greater argumentative burden regarding the principle of purpose limitation since, in order to avoid its use in a speculative manner, the lawmaker chose to stress that its application results only from a concrete situation. This reinforcement serves the data processing agent itself, as the more clearly their interest is outlined, the easier it will be to assess it, especially in order to analyze whether the amount of processed data is really necessary, as well as what the measures to mitigate the impact on the rights and freedoms of the data subject are. Conversely, the more generic the interest, the more difficult it will be to demonstrate that the data processing agent is not somehow abusing its position.

65 "[...] When processing is based on legitimate interests, a specific balancing test is required, where the legitimate interests will be weighed, and the legitimate interests of those resorting to this lawful basis must be real, cannot be speculative, and cannot be based on an assumption that in the future I will process this personal data for this hypothetical purpose that could be useful to society, they must be based on concrete cases. This concrete and specific situation has to be weighed against fundamental rights [...]". Speech by Renato Leite Monteiro at the Deliberative Meeting to discuss bill 4060/12 on the processing and protection of personal data, held on 04/05/2017. He recalls that this was one of the points of tension at the time of the second public consultation in 2015 of the draft bill. Available at: https://www.youtube.com/watch?v=F1_NiqerjRs; 1h20min05sec - 1h20min40sec.

66 LEONARDI, Marcel. ***Legítimo interesse***. Revista do Advogado AASP. No. 144, 2019, page 69.

67 In the Brazilian case, one can mention credit protection, which was inserted in the final stage of discussion of the bill 4060/2012 in the House of Representatives.

B.2.2) GOOD FAITH

Article 10, item II brings new elements to the mix, which must be observed when the purpose is "protection, in relation to the subject, of the regular exercise of his/her rights or provision of services that benefit him/her". To this end, a new factor is added: respect for his [the subject's] "legitimate expectations and fundamental rights and freedoms".

The provision generates an immediate question: would respect for the subject's legitimate expectations be required, on the part of the controller, only in the case of this specific purpose? It doesn't seem so. To justify such a stance it is important to understand what the notion of legitimate expectations represents and how it relates to a principle that is very dear to Brazilian law: the principle of good faith.[68]

Regarding the idea of the data subject's legitimate expectations, Working Party 29's Opinion on legitimate interests affirms that a *compatibility* analysis is required, that is, a check on the *contextual proximity* between the use made of the subject's personal data and what he/she expects. Does the subject expect or should expect that specific use? In more colloquial terms, won't he/she feel ''betrayed'' by such use of his/her personal data? If the expectation already exists, the impact of processing has probably already been somewhat scaled. But if this expectation does not exist, the impact (positive or negative) will be unexpected for the subject, something that must be taken into consideration in the balancing process.[69] Herein lies the ''legitimate expectation''.

It is also important to highlight that the idea of compatibility is related to the principle of purpose limitation, since its very definition is the "performance of processing for explicit, legitimate, specific purposes that are informed to the data subject, without the possibility of further processing in a manner *incompatible* with those purposes". Thus, it should be analyzed whether further processing is contextually close to the original use of the personal data and whether the data subject has an expectation that the secondary use will be carried out.

This legal arrangement is related to the principle of good faith, a landmark of Brazilian private law and the head provision of Article 6 of the Brazilian General Data Protection Law.[70] By including good faith as the principle from which the others unfold, the Brazilian lawmaker tied the indeterminate concepts of legitimate expectation and legitimate interest to a very traditional element of Brazilian legal culture.[71]

The principle of good faith implies the existence of a duty of conduct on the part of the data processing agent, with emphasis on: (i) *loyalty* to the data subject, so as not to frustrate the trust placed in him, which can only be assessed on a case-by-case basis; this makes room for new (secondary) uses ofthe data that do not contradict the context of the information flow;[72]and (ii) *care*, which is linked to the notion of ''abuse of rights'', that is, that the right to process personal data does not "clearly exceed the limits imposed by its economic or social purpose [...]".[73] In this sense, the notion of abuse of rights would be

---

68 To see more about the correlation between "legitimate expectation" and the principle good faith in Brazilian law: MARQUES, Cláudia Lima; ***Contratos dos Código de Defesa do Consumidor: o novo regime das relações contratuais***. São Paulo: Revista dos Tribunais, 2011, p. 282; MENEZES CORDEIRO, António. ***Da boa-fé no direito civil***. Coimbra: Almedina, 2011, p. 1238; and LISBOA, Roberto Senise. ***Confiança Contratual***. São Paulo: Atlas, 2012, p.143.

69 DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. United Kingdom, 2017, p. 17. Available at: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

70 Good faith would be a "principle of principles": "Article 6 The activities of personal data processing shall comply with good faith and the following principles: [...]".

71 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd ed.): chapter 5, p. 225.

72 Ibidem, p. 228.

73 BRAZIL. Civil Code. "Article 187. The subject entitled to a right that, in exercising it, clearly exceeds the limits imposed by its

the gateway to the "ethical and social limits imposed on an activity", precisely at a turning point in ethics amidst the regulatory debates about new technologies.

In this way, the Brazilian lawmaker tried to avoid an inadequate "legal transplant"[74] of a number of concepts, including the legitimate interests lawful basis without the proper correspondence and fitting into the Brazilian legal system. Good faith fulfills this ''modulating'' function around the introduction of an undetermined legal concept that was, until then, alien in Brazil. Based on these considerations, we will proceed to a systematic analysis of the provisions of LGPD regarding legitimate interests, with a special focus on the provision of ''respect for legitimate expectations'', and good faith.

The inclusion of good faith in Article 6's ''head'', which is the core of the provision and expresses its general rule,[75] is indicative of its centrality, including in relation to the other principles. As a principle, good faith is inserted in the section of preliminary provisions of the law, which also provides its premises (Article 2), scope of application (Article 3, and Article 4) and definitions (Article 5). It represents, in this sense, part of the core provisions that guide the norm and are applicable to all Articles thereof.

The provision on legitimate interests, in turn, is broken down into two Articles, both belonging to the first section of the Chapter on "Processing of Personal Data", entitled "Requirements for Processing Personal Data". Article 10, which is discussed at length in this document, completes the provision of Article 7, which lists the possible lawful bases for processing personal data. Hence, Article 10 aims to regulate, in a more detailed way, legitimate interests as a specific ground for processing.

Article 10 has the traditional structure of an Article of law, as it has a head provision, items which further develop it and paragraphs which explain or modify it.[76] The requirement to respect the data subject's legitimate expectations, in its turn, is a direct development of the main provision, where the legislator chose to exemplify purposes for data processing based on legitimate interests. As mentioned before, the additive particle ''and'' suggests that whether the purpose in question is the support and/or promotion of the activities of the controller or the regular exercise of rights by the data subject, the legitimate expectations and the rights and freedoms of the data subject should be considered in the assessment.

This reading corresponds with the purpose of a legitimate interests provision and with the greater objective of LGPD itself, but it is also consistent with the idea, reasserted herein, that the interpretation of the lawful bases, and of the other rules contained in LGPD, should be guided by the principle of good faith. The guarantee that a balancing exercise will be conducted and that it will take into account the expectations of the data subject in a given situation instills the elements of trust and protection against abuse into the relationship between the parties involved.

At this point, it should be noted that this understanding does not ensure that the data subject's legitimate expectations will *prevail* in all cases, but that they be considered on an equal footing with the elements that support the interests of the controller or third party so that, based on the balance between both, a final decision on whether to proceed with the use of this lawful basis will be reached.

---

economic or business purpose, by good faith or morality, also commits an unlawful act".

74 The idea of a "legal transplant" was coined by Alan Watson in the 1970s to indicate the transposition of a rule or even a legal system from one country to another. In: A. Watson, **Legal Transplants: An Approach to Comparative Law**, Edinburgh, 1974.

75 ALVARENGA, Marcos de Castro; LESSA, Beatriz Helena Mendes Ribeiro. ***Técnica Legislativa.*** Belo Horizonte, 2013. Available at: http://camaramuriae.mg.gov.br/portal/wp-content/uploads/2018/08/apostila-tec-legislativa-unificada.pdf

76 MARINHO, Arthur de Sousa. ***Sentença de 29 de setembro de 1944***. Revista de Direito Administrativo, vol I, p. 227. Also according to PINHEIRO, Hesio Fernandes. ***Técnica Legislativa.*** 1962, p. 100.

FINDING NO. 8 AND NR 6

The idea of ''legitimate expectations'' is directly related to the principle of good faith, to the extent that it is based on a duty of loyalty and non-frustration of the data subject's trust. In addition, another element of the concept of good faith is the prohibition to the ''abuse of rights'', which in this case would correspond to a limitation on the processing of personal data that does not pass the legitimate interest test. In that sense, the interpretation of legitimate interests, particularly in regard to the data subject's expectations, must also take into account the strong influence of the principle of good faith in Brazilian private law, in order to avoid an inadequate legal transplant of the concept. It is important to emphasize that good faith is the "principle of principles" as it stands in the head provision of Article 6, unfolding into the other principles listed throughout the corresponding items. As a result, the best interpretation of the provision is the one that considers that the legitimate expectation of the subject must be *considered* in every case where legitimate interest is applied, even if it does not prevail in the final result of the balancing of interests at stake, since it is not an absolute value.

B.2.3) NECESSITY

Along with purpose limitation and adequacy, the principle of necessity is also one of the conditions for the applicability of legitimate interests. While the principles laid out by Article 6 must apply to all processing situations, there is explicit reference to the principle of necessity when the lawful basis in question is legitimate interests.

B.2.3.1) NECESSITY IN THE STRICT SENSE

Article 10, paragraph 1 of LGPD states that: "When the processing is based on the legitimate interest of the controller, only the personal data strictly necessary for the intended purpose may be processed." This is a goes back to the historical[77] principle of necessity, or data minimization, according to which the smallest possible amount of personal data that is sufficient to meet the intended purpose should be used, and no more than that.[78]

In addition to the assessment to determine the minimum amount of data, it should also be considered whether a lawful basis other than legitimate interests could be applied in the concrete case.[79] This does not mean that there is a hierarchy established among different lawful bases, but it is rather an exercise that serves the data processing agent himself, insofar as the other lawful bases do not, as a rule, demand an enhanced argumentative burden such as that required by legitimate interests.

In that sense, assessing whether there is another applicable lawful basis does not make legitimate interests hierarchically ''inferior''. The need to verify other lawful bases applicable to the processing in all

77 It is present, for example, in the Convention 108 of the Council of Europe, the first binding document on personal data protection.

78 Further above, Article 6, which defines the guiding principles of the law, states: "Article 6 The activities of personal data processing shall observe good faith and the following principles: [...] III - necessity: limit processing to the minimum required for the attainment of its purposes, with coverage of data that is pertinent, proportional and non-excessive in relation to the purposes of data processing;".

79 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd ed.): chapter 5, p. 236.

cases is precisely a consequence of the lack of hierarchy among them, as they are all potentially applicable. The criterion for determining the applicable basis is the ''fit'' between the normative provision and the concrete case.

It is important to note that the adjective "necessary" is not to be understood as "indispensable", but neither is it synonymous with "useful" or "desirable". The most straightforward way to identify the element of necessity is to ask whether there is another, less intrusive, way to achieve the identified purpose.[80] Such assessment can lead to some answers: if there is no other way to achieve the purpose or if the other way would require disproportionate effort, then the processing can be considered necessary. If there are different ways to achieve the same purpose, however, it is possible (although not mandatory) to conduct further evaluation, such as a Data Protection Impact Assessment[81] to help identify the least intrusive hypothesis.

B.2.3.2) NECESSITY IN A BROAD SENSE

If there is necessity in the strict sense, i.e., designed to mitigate the intrusive nature of data processing, another type of necessity assessment does not concern the *quantity* of data collected and processed, but rather the *impact* that the processing has on the fundamental rights and freedoms of the data subject.

Thus, it does not matter whether little or much data is being handled in a particular processing for a particular purpose; but it is assumed that virtually any processing has the potential to harm the data subject, so that regardless of the quantity of data, the controller must incorporate measures to mitigate risk. Measures to promote and protect the rights and freedoms of data subjects that fall into this category are, for example, anonymization or pseudonymization, as they are able to mitigate the potential negative impacts of personal data processing. This also explains why the LGPD multifactorial assessment is divided into four steps, which will be discussed later.

FINDING NO. 9 AND RN 7

Unlike other lawful bases, in the case of legitimate interests there is explicit reference to the principle of necessity as a condition for applicability. Necessity, or minimization, is hereby divided into strict sense, which refers to processing the least amount of personal data necessary for a given purpose, and broad sense, which refers to the articulation of safeguards to mitigate the risks to the fundamental rights and freedoms of data subjects. This double duty of care triggers two distinct judgments, one about the least intrusiveness of the data processing, the other about the least harmfulness.

B.2.4 TRANSPARENCY[82]

80 DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. United Kingdom, 2017, p. 17. Available at: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

81 LGPD itself establishes the prerogative of the Brazilian Data Protection Authority to require the controller's data protection impact assessments in the event of processing based on legitimate interests.

82 It should be stressed that this principle, in particular, is related to other regulations that make up the micro-system of personal data protection, especially the Consumer Protection Code, which states, in Article 43, as follows: "The consumer, without prejudice to the provision in Article 86, will have access to existing information in registries, files, records and personal and consumer data filed about him/her, as well as their respective sources. Paragraph 1 The registries and consumer data must be objective, clear, true and in easy-to-understand language, and may not contain negative information referring to a period of more than five years".

The fourth principle used as a parameter for the application of legitimate interests is the principle of transparency, which in LGPD is provided for in Article 6, VI. Besides being a general principle of law, in the case of legitimate interests it is reinforced by Article 10, paragraph 2, according to which "the controller shall take measures to guarantee the transparency of the data processing based on his legitimate interest''.

Transparency measures are part of the legitimate interest assessment, which includes, after weighing the interests of the controller or third party and those of the data subject, the adoption of safeguards that can mitigate remaining imbalances in this relationship. The greater the impact of the processing on the data subject, the more attention should be paid to safeguards, including active transparency practices, i.e., spontaneous sharing of information, without the need for a request by the data subject.[83]

In the specific case of this safeguard, the data processing agent is expected to inform the data subject, in a clear and transparent (easily understandable) manner, about the various aspects of the processing in question, from how it is carried out to what lawful basis is employed and for what purposes. Such information should be ''clear, adequate and ostensible'' (Article 9). In addition, part of the duty of transparency concerns clear communication, to the data subject, of his rights, as provided for in Article 9, paragraph 3, according to which:

> Paragraph 3 When the processing of personal data is a condition for the supply of a product or for the rendering of a service, or for the exercise of a right, the subject shall be informed especially of such fact, and of the means through which he may exercise the rights listed in Article 18 of this Law.

However, it is not only the data subject who has an interest in broad transparency measures about processing based on legitimate interests. This is also important to enable *public scrutiny* by relevant stakeholders,[84] including the National Data Protection Authority. In other words, it is not because the lawful basis is not consent that it is devoid of any perspective of control and, above all, of the possibility to curb abuse. In this case, there is a kind of deferred self-determination, as both data subject and collectivity should be involved to a certain degree. One of the possible consequences of this logic is that the legitimate interest assessment should be subject to publicity.

It is in this sense that active transparency practices have fundamental importance, as they serve as a manner of social, and not just individual, control. Under the perspective that data protection protects both individual and collective legal interests, such as non-discrimination and human dignity, transparency concerning processing practices is of utmost importance. There are cases in which the abusive processing of personal data leads to violations of rights affecting entire segments of the population, there being situations of discrimination by race, gender, and socioeconomic profile. Active transparency by companies and other entities also plays a role of social responsibility, subjecting their own practices to public scrutiny, on the one hand; and creating a ''market culture'', on the other.

83 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014, p. 42.

84 MATTIUZZO, Marcela; PONCE, Paula. ***O Legítimo Interesse e o teste da proporcionalidade: uma proposta interpretativa***. *Internet e Sociedade*, V. 2, n. December 2, 2020. p. 70 "Accountability measures associated with legitimate interests, in this sense, represent ways to ensure the possibility of subsequent scrutiny of the use of this lawful basis by the data subjects and other stakeholders, such as the regulator itself."

FINDING NO. 10 AND NR 8

The principle of transparency is one of the norms which best express how informational self-determination is not limited to consent. Its reinforcement as one of the obligatory safeguards for the use of the legitimate interest lawful basis grants not only individual, but also social control over data processing activities throughout their course. This is because while notions such as reasonable efforts may possibly rule out the requirement of full disclosure at the individual level, active transparency measures should be encouraged in order to ensure accountability. It is therefore recommended that the scope of such transparency duties be made explicit by ANPD and, on the part of data processing agents, that it be seen as a measure of their own accountability.

B.2.4.1) RIGHT TO OPT-OUT

Article 29 Working Party highlights, at several points[85] of its Opinion on legitimate interests, "an unconditional right to opt-out" as an example of the safeguards that the controller must provide to the data subject when applying the legitimate interests lawful basis. In fact, this is one of the items that the opinion addresses in more depth, along with the relationship between transparency and accountability and the empowerment of data subjects through the right to data portability.

But what about LGPD? The Brazilian General Data Protection Law provides, in Article 18, paragraph 2, that "the data subject may object to data processing based on one of the lawful bases, except consent, in case of non-compliance with the provisions of this Law." This is a "way for the data subject to obstruct the processing of his or her data"[86] and, thereby, have more control over it, regardless of the lawful basis adopted. This is so because the possibility of opting out applies to all lawful bases, except for consent, since consent has its own ''outlet'' (the possibility to withdraw consent at any time).

It is necessary, therefore, to take a closer look at the condition that the law imposes for the exercise of the right to opt-out: "in case of non-compliance with the law." A possible interpretation, suggested by Bioni[87], is to consider that, as soon as transparency measures are applied, the data subject is given the opportunity to express his or her opinion on the processing. If the subject expresses his or her disagreement because he or she considers it contrary to his or her legitimate expectations, and if the controller does not abide by this decision, then there would be a disregard of the law.[88]

It is worth pointing out that this does not mean that the right to opt-out is absolute or that it must be met under all circumstances. First, the very condition of "non-compliance with the law" already indicates that the prerogative does not apply unjustifiably. Moreover, the data subject's disagreement does not automatically trigger the requirement to terminate the processing. This is so because, although the data subject may decide to oppose the processing, that would still require a contextual analysis of whether the controller or third party has compelling legitimate grounds for processing which override the subject's own interests.

---

85 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 3.

86 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 247.

87 Ibidem. p. 248.

88 This is, according to the author, a systematic interpretation of Article 18, paragraph 2, referring to the right the opt-out, and Article 10, paragraph 2, on mandatory transparency measures.

While an explicit opposition by the data subject is a strong indication that the processing in question may be contrary to his or her expectations and/or rights and freedoms, the possibility that the controller or third party may demonstrate that their interests outweigh the data subject's in a given context claim cannot be ruled out.

Finally, it should be noted that the chance to opt-out of processing can be seen as one of the possible safeguards to be applied on the initiative of the controller, regardless of there being a legal obligation in that sense. A way to mitigate the possible negative impacts on the data subject and "change'' the balancing in favor of the ultimate lawfulness of the processing in question.[89]

FINDING NO. 11 AND NR 9

LGPD makes the right to object to data processing conditional on the existence of a "failure to comply with the law". Since the legitimate expectations of the data subject are one of the parameters that must be observed in order to ensure the lawful application of legitimate interests, a possible interpretation is that the right to opt-out could be triggered under the argument that the data subject's trust has been frustrated, which will be contextually balanced with the other interests at stake. Otherwise, such parameters would be too limited in scope. This is an interpretation that avoids an asymmetrical regime between the lawful bases, more specifically in relation to consent, since, in this case, the data subject holds the one-sided right to revoke it at any time. An interpretation that places consent and legitimate interests on an equal footing, as they were articulated in Article 7, is also a matter of internal consistency of the law. Nevertheless, it is reiterated that the right to opt-out is not absolute and may be overruled if the analysis of the specific case reveals that the interests of the controller or of third parties outweigh the legitimate expectations and the rights and freedoms of the data subject. It is also important to point out that, regardless of it being a legal obligation, providing the possibility of opting out of data processing operations should also be seen as a good practice, a safeguard to minimize impacts.

B.2.5) ACCOUNTABILITY

A fifth principle that can be observed in the legitimate interests provision is that of accountability, provided in Article 6, X of LGPD. Accountability is a central element of the very notion of legitimate interests since this lawful basis relies mostly on an assessment and a decision made and justified by the data processing agent.[90]

The principle of accountability is also reflected in the provisions where the law requires controllers and processors to keep records of their processing activities. Article 37, specifically, provides that this record-keeping is particularly relevant when the processing is grounded on legitimate interests. Keeping records of processing activities serves a number of different purposes related to the general notion of accountability: while it allows processing agents to have a better understanding of the flow of personal data they deal with and build a dynamic governance plan, it also facilitates (and, in some cases, enables) the fulfilment of data subject's rights. Besides, record-keeping is essential in the face of external scrutiny: in order to be able to demonstrate compliance with LGPD requirements, one must have proper documentation.

89 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 45.

90 Ibidem. p. 43.

In the case of the lawful basis of legitimate interests, as demonstrated by the legislator's choice to highlight it in Article 37, record-keeping is all the more important for accountability, considering there is a previous assessment involved in the decision to apply it as a ground for processing. In the next section, it will be argued that, besides keeping and updating descriptive records of processing activities, the legitimate interest provision also triggers a duty to document the legitimate interest assessment.

B.2.5.1) THE LEGITIMATE INTEREST ASSESSMENT AS A SPECIAL RECORD OF THE DATA PROCESSING ACTIVITY

Since it appeared on the legislators' radar, the lawful basis of legitimate interests was always understood to attribute a higher margin of discretion to data processing agents – which should be properly modulated. The Brazilian solution was to explicitly provide for parameters that would guide the application of this lawful basis, while reinforcing some of the core principles of LGPD, as discussed before.

This, coupled with the emphasis that the data processing agent must keep records of its activities "especially when based on legitimate interests," leads to the normative implication that, besides being mandatory, the legitimate interest assessment should be somehow recorded. There is no indication as to the form of this assessment, and it is interesting to have room for flexibility (depending, for example, on size and economic capacity of the agent), but there must always be a prior assessment that is documented.[91]

The idea of a legitimate interest assessment, as applied in the context of GDPR, varies in its structure, so that there are versions such as the one proposed by the Information Commissioner's Office (ICO), which subdivides the test into three phases, and versions such as the one of the former Article 29 Working Party, which determines that there are four phases.[92] While there is no guidance or interpretation provided by the Brazilian DPA on the matter yet, The Brazilian law was structured in such a way that the subdivision of a test in *four phases* is the most appropriate one. Namely: (i) legitimacy; (ii) necessity; (iii) balancing; and (iv) safeguards.

91 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 247.

92 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014.** p. 33. Available at: https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

COMPARATIVE TABLE OF LEGITIMATE INTEREST ASSESSMENTS IN EUROPE AND BRAZIL

PHASE/TEST	EUROPE (ICO)	EUROPE (WP 29)	BRAZIL
Phase 1 - Legitimacy Value judgment by the controller	**Article 6(4), b, of GDPR; Recitals 47 and 50, of Directive 95** • Specific situation • Lawful purpose	**Article 6(4), b, of GDPR; Recitals 47 and 50, of Directive 95** • Specific situation • Lawful purpose	**Article 10, head provision, LGPD** • Specific situation • Lawful purpose
Phase 2 - Necessity Requirements that inform the legitimate interests of the controller or third party.	**Article 6(4), a, of GDPR; Recitals 47, 49, 50, of Directive 95** • Adequacy • Minimization • Other lawful bases	**Article 6(4), e, of GDPR; Recitals 47 and 50, of Directive 95** • Assessment of impact • Nature of the data • Type of processing • Legitimate expectations	**Article 10, paragraph 1, of the LGPD** • Adequacy • Minimization • Other lawful bases
Phase 3 - Balancing Requirements that inform the legitimate interests of the controller or third party.	**Article 6, (4), c, d, e; 6(1), f, of GDPR** • Legitimate expectation • Fundamental rights and freedoms • Safeguards: transparency measures, right to object, pseudonymization[93]	**Article 6(4), c, d; 6(1), f, of GDPR; Recital 47, of Directive 95** • Fundamental rights and freedoms • Transparency • Proportionality	**Article 6, I, 7, IX, and Article 10, II, of LGPD** • Legitimate expectation • Fundamental rights and freedoms
Phase 4 - Safeguards Necessary guarantees when applying the lawful basis		**Safeguards: Article 6(4), e, of GDPR; Recital 50, of Directive 95** • Transparency measures • Right to object • Pseudonymization • Portability	**Safeguards: Article 10, paragraphs 2 and 3, of LGPD** • Transparency measures Additional measures: • Right to object • Pseudonymization

Thus, Brazil opted for a four-phase legitimate interest assessment, which reflects the structure of Article 10 of LGPD. The last phase, which is mainly extracted from the reinforced principle of transparency,

93 In the interpretation of the former Article 29 Working Party, the safeguards granted, as requirements to be considered in the balancing phase, constitute a phase of their own - and not part of the balancing phase. Article 29 DATA PROTECTION WORKING PARTY. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46**/EC. 2014**. Available at: https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

at the same time functions as a way to ''tip the balance'' in favor of the processing and an opportunity for external scrutiny, either from the data subject or competent authorities.

B.2.5.2) DATA PROTECTION IMPACT ASSESSMENT

The last paragraph of Article 10 of LGPD addresses data protection impact assessments: "The national authority may request a data protection impact assessment from the controller when the processing is based on legitimate interests, subject to commercial and industrial secrets."

Based on this, the following question has been the subject of debate: would a data protection impact assessment be *required* in every situation in which legitimate interest may apply? It doesn't seem to be the case precisely because it is not the lawful basis in question that triggers this specific assessment, but rather the high risk of the processing activity, as defined by LGPD in its Article 5, item XVII.[94] It is expected that the Brazilian National Data Protection Authority will further define situations where a data protection impact assessment would be mandatory[95].

The decision to ground a given processing activity on the legitimate interests of the controller or of a third party doesn't alter the risk posed by the activity itself. At the same time, it seems that the obligations derived from the principle of accountability are already met by the legitimate interest assessment, which can, in its turn, help identify risks that could use further evaluation.

FINDING NO. 12 AND NR 10

In terms of assessments carried out prior to adopting the lawful basis of legitimate interests, the requirements of Article 10 point out to the obligation to conduct a legitimate interest assessment (without establishing a specific form). A data protection impact assessment, at this point, is not considered mandatory by LGPD, even though ''the Authority *may* require the controller to present a data protection impact assessment when the processing is based on a legitimate interest'' (Article 10, §3º). This interpretation seeks to avoid a "trivialization" of DPIAs, considering it is the data processing activity itself, and not the lawful basis, that defines the level of risk in a given situation.

SECTION C – PUTTING THE LEGITIMATE INTEREST ASSESSMENT (LIA) INTO PRACTICE

As noted throughout the previous analysis, legitimate interest is a lawful basis that demands an eminently contextual analysis. Such an abstract and indeterminate legal concept comes to life only when it is analyzed together with a specific factual situation. Consequently, the 4 phases of the legitimate interest assessment, which are the ''qualifying steps'' for an interest to be legitimate, achieve a great degree of variation.

In this scenario, this section first aims to analyze concrete situations - emulating fictitious cases divided into different areas or sectors – to emphasize the theory of legitimate interest in practice. From

94 This Article should be combined with Article 55-J, XIII, which is the provision that qualifies the risk as being high.

95 This is one of the topics covered by the first phase of the Regulatory Agenda published by ANPD, which means that it is a priority which will be dealt with in the near future by the Authority. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-da-protecao-de-dados-anpd-publica-agenda-regulatoria-bianual-da-autoridade-para-2021-2022

these cases, sectoral generalizations will be made, focusing on which of the 4 phases of the legitimate interest assessment present a higher level of criticality considering one given area or sector. For this purpose, we used colors that measure the ''temperature'' of each phase, a kind of **thermometer of legitimate interests**, whose aim is not to state whether a specific case ''passes the test'' or not, but rather to point out sensitive points that deserve special attention from processing agents, data subjects, and authorities.

C.1) LABOR RELATIONS

C.1.1) CASE STUDIES

C.1.1.1) GENERAL MONITORING OF EMPLOYEES

The division of social welfare programs of the Ministry of Economy has a total of 100 employees. Only 15 of them have access to the database with the personal data of citizens who have some type of social benefit and, consequently, to the information requested (registration data, socio economic profile) for verification of eligibility and maintenance of the benefit. The others only have access to working documents saved in internal network folders, related to internal orders, studies, opinions, and analyses, which do not contain data from the beneficiaries of social programs.

To avoid security incidents related to the beneficiaries' personal data, the Ministry's information security committee suggested the implementation of monitoring measures involving all its employees based on legitimate interests. Nevertheless, its final decision was to reject the proposal to subject all employees to the same kind of workplace monitoring. The grounds for that decision were that:

a) only the 15 employees were to have their workstations monitored and, more specifically, with the activation of a *software* that prints their screens only when they access the beneficiaries' databases (**phase 1 and 2 of LIA**);

b) otherwise, the wide and indiscriminate adoption of such monitoring would have a disproportionate impact on the rights and freedoms of all employees. In this regard, it should be noted that the restriction to activate the print screen *software* only when there is access to the beneficiaries' database also has the purpose of modulating the impact on that portion of the employees subjected to more intrusive monitoring (**phase 2**).

C.1.1.2) USE OF KEYLOGGERS

An employee who worked as a web developer for a company that, at the time of his hiring, had a staff of about 20 employees was dismissed due to an analysis, by the employers, of the results presented by a keylogger, that is, a software that runs on a computer to monitor and store all keyboard entries (as well as the time of entry and the interval between two entries). Upon joining the company, the employee had committed in writing to use the company systems and hardware only to perform the agreed-upon tasks, considering information security purposes, but the monitoring revealed that this agreement has been breached. On the other hand, the company did not inform employees that it would make use of a *keylogger* to monitor this traffic.

When analyzing the case, a Court held that the legitimate interest basis could not be properly applied by the company in this case for the following reasons:

a) Data obtained in this way makes it possible to create a comprehensive and complete profile of the data subject's private navigation. In addition, special categories of personal data and other highly

sensitive data such as passwords for protected areas, credit card information, PIN numbers, etc. are recorded, without this being necessary for the purposes of monitoring and supervision (**phase 2**);

b) Adequate safeguards, especially transparency measures, have not been implemented since the use of keyloggers and its purpose have not been informed to employees (**phase 4**).

C.1.1.3) TEMPERATURE CONTROL IN TIMES OF COVID-19

In the context of the COVID-19 pandemic, a technology company decides to resume its face-to-face (on-site) activities, with the establishment of a series of health and safety measures: rotation of employees, special distances between workstations, obligatory use of masks, reinforced cleaning, etc. Besides these measures, the company has also established a routine for checking body temperature using a specific measuring device. Every day, at the entrance of the building, a designated professional "tests" all employees, measuring their temperature and informing the result to each one. The temperature is recorded by the employee on a simple spreadsheet, associated with the employee's name, date, and time of entry.

Occasionally, it is pointed out that an employee has a high body temperature and, for this reason, he or she may be prevented from entering the building to work. By objecting the decision, an employee points out that he was never asked for express permission to perform the testing, nor was he given the option to object to the practice. Furthermore, he points out that the measurement is not accurate and that his leave from work is unjustified. The employer, in turn, claims that the processing of the personal data in question takes place on the basis of its legitimate interests.

Analyzing the case, a Committee reaches the following conclusions:

a) First of all, the personal data involved in the case in question is health data and, therefore, sensitive data. In this sense, the legitimate interest is not an applicable lawful basis under Article 11 of LGPD;
b) Even if it were possible to apply legitimate interests, the case raises questions concerning at least two aspects: first, regarding the necessity (**phase 2**) to store the collected temperatures by associating them with other personal data, since the alleged usefulness of this data is quickly lost. In addition, concerning safeguards (i) the company has not established transparency measures in order to demonstrate that it would perform data collection and processing and, especially, what the specific purpose is; (ii) there was no possibility to object (opt-out), that is, the employee opting not to inform his temperature; (iii) there is no indication of security measures established to protect the personal data, which was stored in a simple spreadsheet accessible by anyone in the company's cloud.

C.1.2) ANALYSIS OF LEGITIMATE INTERESTS IN LABOR RELATIONS

The lawful basis of legitimate interests can be potentially applied in a series of situations that take place in the work environment, from the moment of prospecting and hiring, through day-to-day work, up to the possible dismissal of employees.

Legitimacy:

The monitoring of employees by their employers is part of the subordination element that is a hallmark of labor law, being "one of the ways in which the employer exercises his management power over his employees."[96] This way, there is no *a priori* illegitimacy from a legal point of view. The other

96 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de

element that makes up the legitimacy test, the concreteness of the situation, depends on the type of monitoring that will be employed – in any case, it must be specified (in other words, the purpose cannot be just generic "monitoring"). One point of attention that can be raised is the processing of sensitive personal data, as it cannot happen on the basis of legitimate interest.

Necessity:

When assessing the need for monitoring,[97] especially in terms of minimization in the strict sense, that is, of the amount of data that is actually necessary to achieve the respective purpose, it is important to keep in mind that the labor relation is characterized by a deep asymmetry[98] . Monitoring corporate network traffic (i.e., tracking all websites accessed by employees) and employing keyloggers and screenshot softwares (i.e., software that records everything typed by employees on a machine and takes pictures of the computer screen with a certain frequency), for example, are possible and relatively common practices. The question is whether measures such as these are overly intrusive, or, in other words, whether it would be possible to achieve the same purpose – productivity control or data security,[99] for example – with less collection and processing of personal data. In the case of screenshots, as an illustration, it is possible to suggest that the data be collected every 30 or 15 minutes rather than every minute. Another question is who, among the employees who have different positions, responsibilities and levels of access, should be subject to monitoring and what types.

Balancing:

In this case, the legitimate expectations of the data subject as to the processing in its entirety must be observed. In the formal work environment, it can be said that some level of monitoring of attendance and performance by the employer is expected. Thus, the previously mentioned necessity requirement, which deals with levels of intrusiveness, must be fulfilled in order for the specific monitoring to be consistent with what an employee may expect. On the other hand, one should note the possible *chilling effect* that continuous monitoring by the employer can have on other employee fundamental rights and freedoms that go beyond privacy, such as their freedom of speech.[100]

Safeguards:

The main safeguard, required by LGPD itself, is transparency, translated here into providing information to employees about the monitoring to which they are subject.[101] Other measures, such as applying *privacy by design* in the development of softwares and systems, conducting impact assessments,

Janeiro, 2020 (2nd edition): chapter 5, p. 239.

97 According to the Article 29 Working Party, at the time of Directive 95/46/EC, some of the Member States considered that the most appropriate lawful basis in this case was performance of a contract. In this sense, if there were another lawful basis, legitimate interest could not be applied.

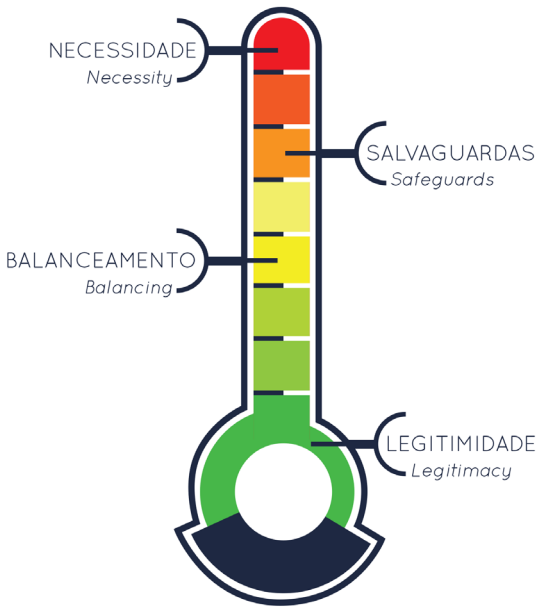
98 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 239.

99 In this case, it should be considered that a more intrusive monitoring may be necessary depending on the level of hierarchy/access of a certain employee to raw/more sensitive databases in comparison to other employees who have access to more segmented folders.

100 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 37.

101 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 241.

in addition to the data minimization already mentioned, are possible.[102]



C.2) BACKGROUND CHECK

C.2.1) CASE STUDIES

C.2.1.1) CRIMINAL RECORD MONITORING AND ''ONLINE VETTING''

A company is in the process of hiring several employees and, for this purpose, it is outsourcing a background check service on potential employees. The service offered by the outsourced company was a "package", consisting of ''simpler'' measures, such as identity and address verification and "character check" through contact with former colleagues/employers, and more complex measures, such as social media vetting and the aforementioned criminal record check. All measures were applied to all applicants, regardless of their individual characteristics and the jobs they applied for.

One individual, who made it to the final phase of the selection process, but was not hired, questioned the practice of background checks, especially the criminal record check and social media analysis. As to the latter, it was pointed out that some elements verified by the company, such as likes, could generate abusive discrimination.

A Committee made up of high-ranking company employees reviewed the case and the lawful basis of legitimate interests that justified it. The Committee concluded that, in principle, the legitimate interest basis might be appropriate, given that LGPD allows it for the "support and promotion of the controller's activities", but only if the activity was carried out with regard to the specificities of the position for which the individuals in question were applying, since there is binding case law[103] that limits criminal background

102 Article 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 56.

103 BRAZIL. Superior Labor Court. "The requirement of Criminal Record Certificate from job applicants is legitimate and does not characterize pain and suffering when supported by an express legal provision or justified by the nature of the job or the special degree of trustworthiness required, such as from housekeepers, caregivers of minors, the elderly, or the disabled (in daycare centers, nursing homes, or similar institutions), cargo truck drivers, employees who work in the agribusiness sector handling perforating tools, bank employees and the like, workers who handle toxic substances, narcotics, and weapons, workers who work with confidential information." Appellate Decision concerning the Defense of Repeated Appeals: 43000-58.2013.5.13.0023, Electronic Court Register of 09/22/2017, Judge-Rapporteur João Batista de Pereira.

check.

However, the requirements of the legitimate interest assessment would not have been met with respect to **phases 2 and 3**. The Committee felt that there was a violation of the principle of necessity, as the outsourced company collected a very large amount and variety of personal data, much of which would not relate to the intended purpose. In addition, there was no differentiation of the data collected in relation to the intended position, which, in the Committee's view, would be inappropriate since some positions would warrant greater scrutiny as they deal with sensitive information, but many others would not.

Finally, in addition to the violation of the principle of necessity, an imbalance in relation to the rights of the data subjects was also verified, since the checking of criminal record without express legal provision and the checking of information regarding personal interests and opinions on social media were considered discriminatory.

C.2.1.2) POLITICALLY EXPOSED PERSONS

The Financial Activities Control Council (Coaf) defines a particular category of individuals as politically exposed persons. They are those people who, due to their position as government agents performing relevant functions or people close to government agents, generate a special interest of the authorities (who start monitoring their financial activities) and also of companies that intend to do business with them.

A company receives a financially beneficial proposal from a company which has as one of its partners an individual who fits the definition of a Politically Exposed Person (PEP). The company's compliance team is called in to present its opinion on the transaction and informs that, before any progress is made in the negotiations, it needs to analyze the following information: full employment background, corporate interests, involvement in fraud and corruption, forced labor and/or terrorist financing investigations.

Another team analyzed the lawful grounds for the processing and concluded that legitimate interests was an appropriate lawful basis, to the extent that the PEP background analysis is aligned with the greater scrutiny to which this category of individuals is subjected (**phase 1 and phase 3**). In addition, only categories of data that were considered reasonable and sufficient given the purpose of avoiding business with legally or ethically compromised individuals were collected in the case (**phase 2**). The person in question, moreover, was aware of their position and the consequences for the business, there being transparency in the relationship with the company (**phase 4**).

C.2.1.3) ''BACKGROUND SANTA EFIGÊNIA'' COMPANY

The ''Background Santa Efigênia'' company, which specializes in research and background analysis of several natures, including criminal records, is going through a reinvention process. Originally, the company sold ''packages'', from the most complete to those focused on a single type of information, such as social network information. The contracting companies sent the basic information of the individuals, and the check was carried out without any kind of discrimination in relation to the characteristics of the position intended or the individual analyzed (**phase 2**). The lawful basis employed to justify the processing of personal data is that of legitimate interests. The team responsible for the transition holds meetings to discuss what changes need to be made for compliance with the requirements of this lawful basis.

The change the company is going through precisely focuses on creating a plan with different levels of investigation depending on (i) the level of sensitivity of the information to which a potential employee would have access; (ii) the seniority level of applicants - whether trainees, junior or senior assistants; (iii) whether it is a position of trust or not; (iv) whether there is a legal provision that requires a specific type of investigation depending on the case (**phase 2**).

The change is considered positive from the point of view of applying the lawful basis of legitimate interests since the greater segmentation of the processed data is in compliance with the principle of necessity/minimization.

C.2.2) ANALYSIS OF LEGITIMATE INTERESTS IN BACKGROUND CHECKS

Legitimacy:

There is no presumed illegality in conducting an investigation during a selection process for hiring employees (there may be if the investigation exceeds certain limits, as has already been established in Brazilian case law). Investigation represents, pursuant to the LGPD, a "support and promotion of the controller's activities[104]." Moreover, it must be about a specific interest and purpose.

Necessity:

Herein lies the greatest difficulty in the analysis of background checks. How much and what variety of personal data is actually *required*? This will depend, among other elements, on the specific purpose within the overall purpose of conducting background checks. For example, if the purpose is to get references about the prospective employee from their previous employers/colleagues, there is no need to search the individual's social media.

Balancing:

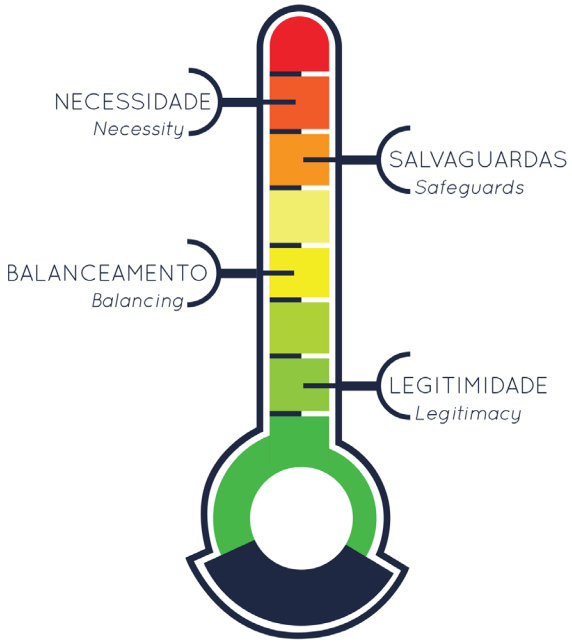
With regard to the legitimate expectation concerning processing, one can say that it exists, at least to a certain extent, since it is expected that, in a selection process, potential employers will seek to confirm information or seek more information about the applicants. The same can be said about the case of politically exposed people, who have an expectation of certain processing due to their position. On the other hand, in relation to the interests, rights and freedoms of individuals, it is important to note that the right to work is a social right and a fundamental principle of the Brazilian Constitution,[105] so that the controller must be careful not to include in its checking elements that have little to do with the quality of the application and that may prove to be discriminatory and limiting of access to this right.

Safeguards:

The background check process can, depending on how it is carried out and the criteria taken into consideration, prove to be discriminatory, which is especially worrying considering that it has practical effects on people's lives, such as a rejection in a job. Thus, it is important to establish safeguards, with an emphasis on transparency throughout the selection process, so that applicants know (i) that they are being checked, (ii) what kind of information is being checked, and (iii) which sources are being checked.

104 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 243.

105 Ibidem. p. 243.



C.3) INTERNAL INVESTIGATIONS

C.3.1) CASE STUDIES

C.3.1.1) VIDEO SURVEILLANCE

A hotel chain has developed a system for occasions, which have become somewhat recurrent, when it receives complaints about objects disappearing from guest rooms and common areas. The company provides standardized training for all employees, plus specific guidance depending on the trust level of the position. In addition, all employees use magnetic cards to access all hotel rooms. In the corridors, there are cameras situated at strategic locations, which allow a view of the entrances to each room. The hotel chain stores the data from the cards (which include the precise times of access to each of the spaces) indefinitely and the images from the cameras for a period of three months (for storage space reasons) and uses this data to conduct internal investigations when necessary and convenient (**phase 2**). The company justifies its data processing on the basis of legitimate interest.

An analysis, after objection, of this lawful basis reached different conclusions for the different types of data collection and processing. It was understood that, a priori, there would be no illegality in the practice. As to the collection of data by electronic card, a usual market practice, it was considered appropriate, necessary, and that it did not harm the rights and interests of the personal data subjects. However, it was considered that the collection of images, although legal and possibly necessary, hurt the rights and interests of data subjects, as well as their reasonable expectations of privacy in certain spaces(**phase 03**). The processing proved to be overly intrusive (**phase 2**), as it reached the bedroom doors and, occasionally, the interior space (when they were open). It was recommended that the cameras be changed to capture only the corridors and elevators (**phase 4**).

C.3.2) ANALYSIS OF LEGITIMATE INTERESTS FOR INTERNAL INVESTIGATION PURPOSES

Legitimacy:

In addition to background investigations on their employees, controllers can also conduct internal investigations on other aspects of the life of a company and the people who work there. There is no legal limitation presupposed in this sense, as long as it is a well-cut and specified purpose.

Necessity:

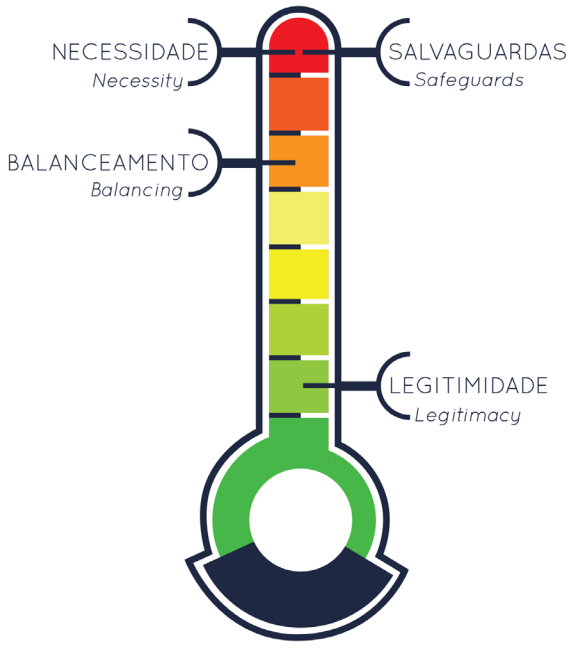
In the case of internal investigations, the aspect of necessity is central, as there are different levels of intrusiveness and impacts depending on the investigation carried out. For example, in the case of an ongoing investigation into recurring hotel guest claims, controlling access to rooms using electronic cards that reveal who entered (and when) can be considered a less intrusive means than using a camera, while satisfactorily fulfilling the purpose pursued. Directing investigations to specific people, based on concrete evidence, is also an adequate alternative to procedures carried out indiscriminately.

Balancing:

Employees can be considered to have a legitimate expectation that, given an occurrence, their employer will carry out an investigation that may involve the processing of their personal data. This expectation may not exist, or be lower, in the absence of a concrete fact, something that must be observed in all employee monitoring situations. Special attention to the aspect of necessity can also result in a reduction of potential impacts on the rights and freedoms of individuals, through the adoption of less intrusive measures. In spite of this, the analysis of impacts, even if residual, should always be carried out, in order to allow a better dimensioning of the applicable safeguards.

Safeguards:

As in other cases, transparency, with clear and easy-to-understand information about the several aspects of legitimate interest-based processing, is essential.



C.4) HUMAN RESOURCES AND GRANTING OF BENEFITS

C.4.1) CASE STUDIES

C.4.1.1) GRANTING OF BENEFITS

An NGO specialized in consumer rights collects data from its employees for several purposes, which include granting benefits, some provided for in law (such as transportation vouchers) and others that make up a special package provided by the association on its own initiative. Knowing that consent is not the most appropriate figure for the processing of employees data and that the basis of legal or regulatory obligation does not cover all the processing performed, the NGO adopts the legitimate interest lawful basis to justify this practice, justifying this choice as follows.

The NGO reports that, besides having assessed whether other lawful bases would be appropriate in the concrete case, it also only collects information that is strictly necessary (**phase 2**) for the granting of each benefit and that it informs employees about the collection and the purpose for which it is carried out (**phase 4**). Thinking about the storage time of this information, the NGO stipulated that it would be restricted to the statute of limitations for labor lawsuits, which is of two years as of the end of the contractual relationship with the employees. After this period, the data is deleted from the NGO's database. **(phase 2 and phase 4)**

Concerning the system used to store such data, the document explains that, due to fear of putting the data in a cloud service, the executive board decided that employee information, including that related to the granting of benefits, would be stored on its own servers. **(phase 4)**

C.4.2) ANALYSIS OF LEGITIMATE INTERESTS IN HUMAN RESOURCES

Legitimacy:

There is no legal restriction on the processing of personal data for human resources purposes and for granting benefits, some of which are even provided for in law.[106] In addition, the purpose of each processing must be concrete and well specified.

Necessity:

In the example mentioned above, regarding the transportation benefit for employees, there is a specific purpose for which only some data (home address general itinerary to get to the workplace) are strictly necessary. In this sense, any further personal data that the employer may require would be considered excessive for that purpose.

Balancing:

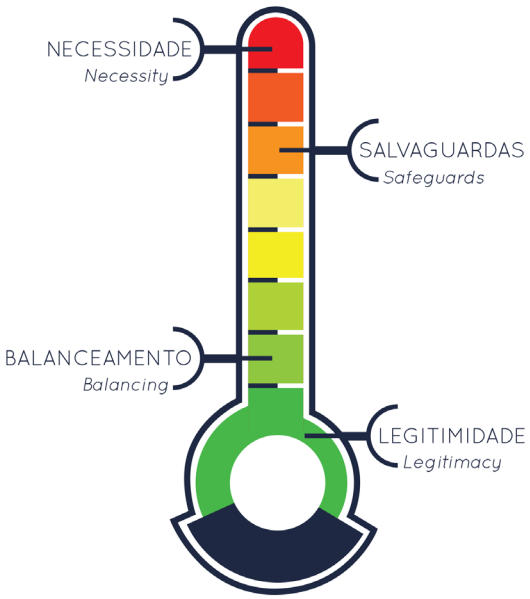
The practices of requiring personal data to enable the granting and controlling of employees benefits are common in companies daily activities, so that it can be affirmed that they are within the legitimate expectations of employees. In addition, in the case of benefits, this is in the employee's

106 According to Law No. 7.418/85, it is the employer's duty to provide the employee having the job registered in his social-security card with a transportation voucher. For this purpose, it is common to require the employee to provide his home address and the list of public transportation he uses to go to work.

interest, and in some cases it is the employee's right. Thus, as long as the processing is proportional and does not incur in any discriminatory aspect, it can be considered fair at this stage.

Safeguards:

As well as with the last items, transparency about the processing is essential to mitigate any remaining imbalances in the relationship between controller and the data subject. In this case the right to object (opt-out) to processing can make the very granting of benefits impossible, something that must also be informed beforehand. Security measures are of utmost importance, both for digital record-keeping and businesses which still keep physical forms and folders containing personal data of employees.



C.5) MERGERS, ACQUISITIONS AND CORPORATE LAW

C.5.1) CASE STUDIES

C.5.1.1) INCORPORATION OF A LINE OF BUSINESS

A communications company focused on the television segment decided to expand its product portfolio, considering that a good option would be to acquire the business line of another communications company specializing in periodicals. In this case, the television network aimed to incorporate one of the magazines produced and marketed by the other company.

In the process of closing the deal, the first company realizes that it will be necessary to share the personal data of the magazine's subscribers, in order to be able to continue its distribution. In consultation with its lawyers, the company concluded that in order to carry out this specific processing it would be appropriate to rely on the lawful basis of legitimate interests.

In its assessment, the company considered that, in the first place, there was indeed a legitimate interest and purpose in the case, which is the distribution of the product to subscribers **(phase 1).** Secondly, it considered that no information would be shared other than that strictly necessary for the continuity of the distribution of the magazines. Any data considered excessive, contained in the merged

company's databank, would therefore be eliminated **(phase 2)**. In addition, the company understood that, in the specific case, it was reasonable to assume that the data subjects would not have their expectations frustrated in relation to the processing, since the purpose had remained the exact same in relation to that performed by the former controller **(phase 3)**.

Still, seeking to identify possible safeguards in relation to the procedure, the company concluded that there were no security problems in storing data, which would remain on high-standard servers already in use. Other than that, it also decided to inform, in a separate communication, all subscribers about the operation **(phase 4).**

C.5.1.2) DUE DILIGENCE AND CORPORATE CONTROL

A bookstore chain realizes that more than 80% of its book sales come from the same publisher. Thus, interested in reducing its transaction costs, the bookstore chain begins to negotiate a merger process with the publisher and hires a law firm to proceed with the negotiation. In a meeting with the firm, the lawyers emphasize the importance of establishing a due diligence process on the publisher, explaining that due diligence is the study, auditing, investigation, and evaluation of risks and opportunities on the company with which a corporate transaction is intended to be carried out (**phase 1**). The bookstore realizes that this, in fact, seems a necessary procedure for doing business with the publisher. However, one of its officers, concerned with what he had just heard about the Brazilian General Data Protection Law, asks whether it would be necessary to ask for the consent of all data subjects involved in this procedure.

The lawyers assured that it would not be necessary to require the consent of the data subjects who will be part of the due diligence since, in this case, the processing of the data is in the company's legitimate interest. The firm also emphasizes that its due diligence is performed based on well-defined criteria and requires only samples of personal information (unless there is a specific point that is more critical and requires a more in-depth analysis). In addition, as long as it does not interfere with the evaluation of the company, the office always requires that the information be aggregated and anonymized (**phase 2 and 4**).

Finally, they reinforced that everything will be shared by VPN and will be stored on their own server and only for the period referring to the civil statute of limitations, so that, after the period, all information will be deleted from the office's database (**phase 4**).

C.5.2) ANALYSIS OF LEGITIMATE INTERESTS IN MERGERS AND ACQUISITIONS

Legitimacy:

The auditing process is indispensable for certain corporate transactions and is a way to prevent risk situations for a company, including those provided for in laws such as the Anticorruption Act (Act 12.846/2013). This is also a specific situation where certain specific data is used to support the activities of the controller or a third party.[107] Similarly, data processing is, in itself, essential for any merger or consolidation of companies transaction, involving, for example, customer and employees data, the processing for this purpose being, a priori, legitimate.

Necessity:

It is not possible to distinguish in advance which data, including personal data, are strictly necessary in an audit procedure or for the implementation of a corporate transaction, which may vary

107 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 240.

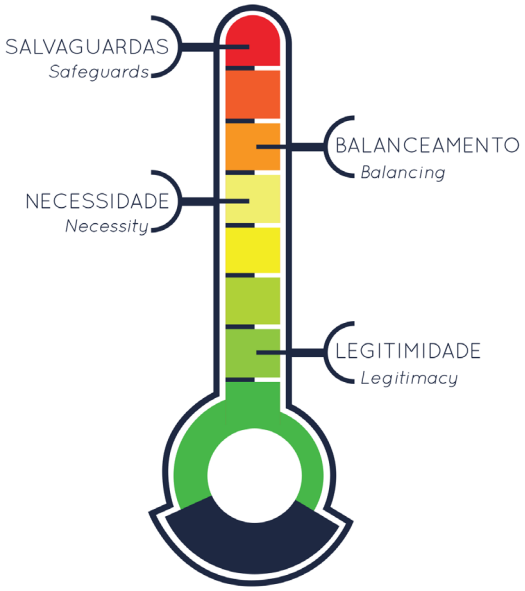
from case to case. Thus, it is up to the corporate department professionals to find an optimal point[108] between the effectiveness of the procedure and the minimization of the collection and processing of personal data, always applying the applicable safeguards. This balance can be achieved, for example, by collecting samples of data, rather than all of it.

Balancing:

In principle, the personal data used in a due diligence process are merely analyzed with the purpose of assessing the convenience of a given transaction, without major repercussions for the data subjects that may be involved. A difference may arise, for the subject, after the transaction in question is finalized, insofar as it may involve aggregation of information and changes in the purposes of the processing of personal data, but this is not a question of the due diligence process per se. In corporate transactions that involve the transfer or sharing of personal data, the assessment of the data subject's legitimate expectations will mostly depend on whether the purposes of processing are altered or not, something that must be carefully assessed on a case to case basis.

Safeguards:

Security measures such as performing the entire operation and occasional auditing process in controlled environments (precisely to avoid the leakage of strategic information to other companies) are common safeguards, also related to the use of aggregated data in the reports, since there is no need, most of the time, to open individual data for auditing purposes.[109] When the transfer or sharing of data is necessary for the continuity of the services provided by a company, it is important to ensure the information security of the procedure and, in addition, to ensure that the data subjects are aware of the information concerning the processing in question.



108 Ibidem.

109 BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento***. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2nd edition): chapter 5, p. 241.

C.6) TRANSPARENCY

C.6.1) CASE STUDIES

C.6.1.1) ''LOVE SERENADE''

A group of activists has developed a robot designed to monitor the spending reimbursements of Brazilian legislators. The purpose of the tool was to investigate suspicions that some representatives used the prerogatives of the position for private expenses.

One of the expenses identified as suspicious by the robot was an expenditure of more than ten thousand reais in alcoholic beverages by a member of parliament during a trip to the city of Las Vegas. As soon as this information was made public, the representative invoked the violation of his privacy and also the protection of personal data regarding his financial transactions and private expenses. The processing was based on legitimate interests (in this case, of third parties).

The answer to the questioning was as follows:

- The purpose of monitoring and exposing suspicious reimbursements of legislators is a practice that interests society at large, allows public scrutiny, and promotes transparency of state expenditures. (**phase 1**)
- Furthermore, the information monitored and collected was restricted to what was strictly necessary, i.e., only expenditures in which public, and not the data subject private, funds were spent. The identification of the name of the individual and the description of the object of the expenditure are essential in order to achieve the purpose of transparency and subjecting the expenditure to the opinion of society. (**phase 2**)
- In this case, the right to access of information, and the principles of transparency and accountability of public expenditures, provided for in several pieces of legislation, overcomes the representative's own individual interests. This is especially so if we consider that he is a public figure who is making use of public funds, a different circumstance from non-public figures spending private funds. (**phase 3**)

C.6.2) ANALYSIS OF LEGITIMATE INTERESTS FOR TRANSPARENCY PURPOSES

Legitimacy:

The processing/disclosure of personal data for transparency purposes is one of the recognized uses of legitimate interests, which may also be supported by transparency legislation, such as the Access to Information Act.

Necessity:

When it comes to transparency, especially with regard to government agents, the personal data processed should be restricted to those that actually serve a public interest, such as data relating to the exercise of public duty, and not personal data relating to the private life of agents, as this would be considered excessive.

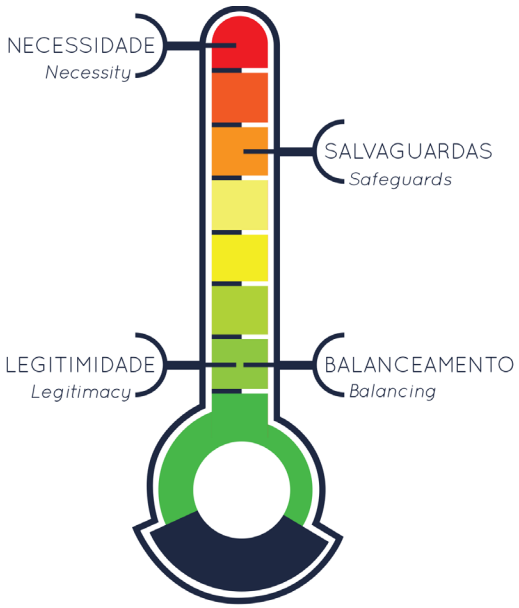
Balancing:

Along the same line of necessity, once it is guaranteed that the personal data collected and

disclosed are of public interest, the collectivity's interest prevails over individual interest, provided, of course, that there is no excessiveness or processing of unnecessary data, which would possibly tip the balance in favor of the data subject. Furthermore, it must be considered that in cases of public interest, the data subject himself has an expectation that his privacy will be relativized.

Safeguards:

Appropriate safeguards, in this case, are transparency about forms of processing, purpose, and other aspects of data processing for publicity purposes, as well as information security.



C.7) ADVERTISING, MARKETING AND CUSTOMIZATION

C.7.1) CASE STUDIES

C.7.1.1) DIRECT EMAIL MARKETING

A company is scanning its entire database, which was originally built for the purposes of registering purchases at its physical stores, with the following information: name, cell phone and email, as well as the products that the customer purchased at the store. The information collected does not allow the company to perform a sophisticated segmentation of customers, but the association of the data with the products purchased makes it possible to target personalized email marketing based on past purchases. So, the company hires a small digital marketing team, and its first action is to create some email categories and target them to the customers registered in the database, according to their preferences, which are revealed by the purchases they have made in the previous year. In the message itself, there is a banner with a button that allows the customer to unsubscribe from the mailing. The company justifies this secondary use of personal data with the lawful basis of legitimate interests.

A later analysis of the use of the lawful basis revealed that there were significant efforts on the part of the company to comply with the steps of the legitimate interest assessment and to document them. It was also considered that the data subjects already had a pre-established relationship with the company, so

they would not be surprised by such an advertising approach (**phase 03**). On the other hand, the following measures were recommended to strengthen the processing: question whether it is necessary to keep the full name of the individuals in order to effect marketing campaigns (**phase 2**); strengthen transparency, informing, together with the opt-out banner, exactly which data the company holds and the purpose of the processing (**phase 4**).

C.7.1.2) NETWORK PROFILES

Interested in expanding its customer network and getting to know its audience better, a bar decided to create a Facebook page and an Instagram profile. Besides using the social media profiles to publicize events, menus, and promotions, the bar owner has also developed a software that automatically takes contact information from the profiles that interact positively with posts and includes it in a spreadsheet. The purpose of the collection is to send targeted messages with promotions to potential customers (**phase 1**).

The first question the owner considered was which data would be transferred to the spreadsheet. She concluded that, considering the purposes she intended to achieve, only the first name (to direct messages with a personal tone), the contact data (email, phone number **or** link from the platform's own chat), and the user's age range, when available, would be collected (**phase 2**). Thinking about which profiles would have the information collected, the owner decided that the software would only insert data from profiles that interacted positively at least once in their networks (**phase 3**).

Ultimately, her biggest concern was to ensure that the software would be able to identify when a user asked to cease to receive advertising from the bar. The owner had in mind that this could alienate her audience and tarnish the reputation of her establishment. So, in every promotional mailing, there was the option to no longer receive the ad, in which case the user's data was automatically deleted from the spreadsheet (**phase 4**).

C.7.1.3) REGISTRATION FOR ACCESS TO CONTENTS

A fintech company that offers financial market assets would like to expand its customer base, so it hires a marketing consultancy, which suggests that a good way to reach its target audience is by producing content related to the service it provides. The consultant reinforces how the practice, besides giving credibility to the fintech, still has the advantage of, from a simple registration for access to content, resulting in a database that can potentially be used for a different purpose (**phase 1**).

The company then questions whether, in this case, it would not be necessary to require users' consent at the time of registration and, thus, link access to the contents to the agreement to share the information.

The consultant advises that this is not the most appropriate approach since the mere fact of making access to content conditional to the granting of data would already mischaracterize a freely given consent, so that an adequate alternative would be to collect and process the data based on the legitimate interests of the company. The fintech then asks to what extent access to their content would indicate that there is a potential customer relation and that it would be appropriate to use this data.

The consultant's answer was that, while the express interest in accessing the content, such as papers, newsletters, market tips and others produced by the company may be an indicative that an individual has a reasonable expectation of receiving further information on the company's products or services, that may not necessarily be the case since these purposes are, in fact, different (**phase 3**).

The consultant points out that, in this case, the fintech must pay special attention to the safeguards, which implies that it must inform the data subjects that the data are also being collected for advertising targeting and apply a clear opt-out mechanism so that the data subject, if he wishes so, no longer receives advertising (**phase 4**).

C.7.1.4) MARKETING FOR ELECTORAL PURPOSES

A candidate for governor decides to invest in digital technologies in his next campaign and, to learn about the possibilities presented by the market, consults three different agencies specialized in marketing for electoral purposes.

The first agency proposes that the campaign starts to analyze the number of hits and most accessed content on the candidate's website. In addition, it suggests using the website to collect users' contact data and send them advertisements and invitations to collaborate with the campaign.

The second agency proposes the monitoring of interactions on the candidate's social media profiles in order to design more efficient strategies, in addition to using specific ads tools to impact audiences similar to those who interacted positively with the candidate's social media content.

The third agency reports that its knowledge of the electorate's profile is the most advanced on the market and that it is based on a rating app, in which users are rewarded with points whenever they rate the services of a company, restaurant, store, etc., something that enables inferences on their interests and preferences and can be used for a number of different purposes.

Fearing possible implications of the approaches in relation to LGPD rules, the candidate decided to consult his lawyer. The expert explained that, in all the models presented, the data processing could be based on the legitimate interests of both the candidate to promote his campaign and the agencies to promote their businesses (**phase 1**). However, to ground a processing on this lawful basis, it would be necessary to observe a few points.

One of them concerns the care with the legitimate expectations of the data subjects In this case, the processing of information concerning individuals who were actually interested in the content of the campaigns represents a lower risk as to the possible abuse of data compared to those obtained by platforms with different original purposes, such as through applications **(phase 3).**

Still regarding the profiling of individuals or groups for electoral purposes, proposed by the third company, this is a point of greatest attention since it involves the use of personal data to identify personality traits, interests and even predict behavior, with a potential direct impact on both individuals and society at large. While LGPD does not limit lawful bases in cases of processing for the purpose of profiling, the phase of balancing the legitimate interest in the face of the rights and freedoms of the data subject gains special relevance in this case and it is possible that further regulation and/or guidance, either by ANPD or the electoral justice, will deal with this hypothesis, including in the electoral context.

Finally, the lawyer points out that, regardless of the approach chosen, it is important that the data subjects be offered a clear means to object to the processing if they wish so, as well as transparency measures at all times (**phase 4**).

C.7.1.5) CROSS-REFERENCING OF PERSONAL DATA

A large technology company decides to "optimize" its personal data processing operations by combining all its databases – more specifically, those coming from (i) search engines; (ii) email; (iii) web browser; and (iv) maps. This is data that is collected when individuals use the company's services, and that generates market intelligence in return. The purposes of each collection, however, are distinct. They are, respectively: (i) customization of the services requested; (ii) development of new products and services; (iii) displaying personalized advertisement; and (iv) analytics.

The aggregation of data was questioned, and an assessment of the data processing in question and the application of legitimate interests to ground it revealed that it was inadequate. This occurred for two main reasons: first, the combination of a number of different data, which were originally segmented according to purpose, to then serve all purposes simultaneously, is contrary to the principles of purpose limitation and adequacy, while also making it difficult to justify the *necessity* for the data (**phase 2**). Furthermore, it was found that there had been no extra transparency measures applied after the change and that in none of the services was there any effective possibility of objecting to processing (**phase 4**).

The nature of the data, the diversity of the services, and the lack of specific information and opt-out options tipped the balance of the legitimate interest assessment in this case (**phase 3**).

C.7.1.6) AD TECHS

Two siblings have taken over the family's advertising agency. The company has always been focused on television advertisement, but the siblings would like to broaden their scope and also work with online media channels. To effect this change, the brother would study the ad techs business and the sister would be responsible for doing a legal analysis on the project. They decided that, by implementing cookies on websites, they would collect several browsing information from users in order to trace behavioral profiles and, based on this, target ads on webpages.

The legal department warned that any personal data processing, while possible, requires a lawful basis (in addition to the other requirements of the law). It explained that most companies misuse consent in these cases, inserting tabs where the user is induced to "accept" the processing. The legal department indicates that an appropriate alternative could be to use the data based on the legitimate interests of the company, which needs to do so in order to promote its ad-targeting business (**phase 1**).

The sister points out that one of the issues to be observed in applying legitimate interests is the relation between the purpose of the activity and the processing of the information, and that the amount of data collected be the minimum necessary (**phase 2**). However, since this is an activity whose purpose is to target content, there are no clear limits as to what this minimum would be since both quantity and quality of data leads to a more precise targeting.

Remembering to assess the legitimate expectations of the data subjects, the group decided that it would seek to mitigate the lack of a pre-established relation by means of a notification, which would indicate that browsing data was being collected. (**phase 3**) The agency also decided that the notification tab would feature an opt-out alternative and that, in addition, the company would strengthen its transparency system. This way, all its ads would feature access to a portal for the user to understand "why" that message was directed to them. (**phase 4**)

C.7.2) ANALYSIS OF LEGITIMATE INTERESTS IN ADVERTISING, MARKETING AND CUSTOMIZATION

Legitimacy:

Marketing is a purpose, in principle, legitimate[110]. It can unfold into several different specific purposes, which must be concrete.

Necessity:

In the current context of marketing and advertising practices, it may be complex to address necessity and minimization, as these practices are increasingly based in the collection of a series of information, that work quantitatively and qualitatively to form profiles that allow for targeted content. Even so, it is possible to restrict the amount of data processed - from a perspective of necessity alone, there is no need, for example, to know the identity of a specific person, but only a certain group to which they belong, to form a profile and direct a personalized message. In this sense, it is even possible to

110 There are cases, as in GDPR, where there is express mention of direct marketing as a hypothesis for the application of legitimate interests. In short, there are regulations to the practice, but not prohibitions. In the case of Brazil, it is noteworthy that email marketing for electoral political purposes must respect consent, according to Article 28, III, of Resolution No. 23.610/2019. In this case, the use of the legal basis for that specific purpose would not be legitimate.

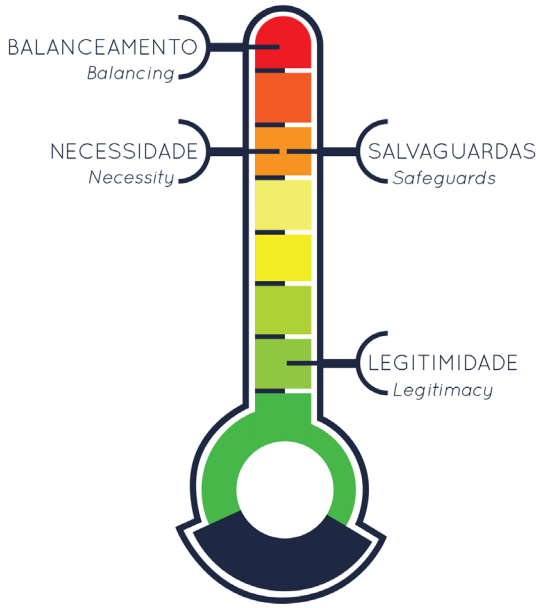
speak of pseudo-anonymization as a good practice adopted by companies.

Balancing:

It should be noted whether there is a legitimate expectation on the part of the data subject to receive the advertising in question, which can be measured, in some cases, by the existence, or not, of a prior commercial relationship between the parties. If there is no such relationship, there are still other ways to measure legitimate expectations, such as interactions on social networks. The specific case must be observed, in order to assess the level of ''contextual proximity'' of the potential client / employee / voter with the agent and check if there is a legitimate expectation that is sustained in practice. In addition, the practice of creating behavioral profiles sparks the need for an in-depth analysis of the rights and freedoms at stake, including in order to establish appropriate and sufficient safeguards.

Safeguards:

The main safeguard, in this case, must be the transparency, including to make the data subject aware of his or her right to object to the processing ("opt-out"). In the case of email marketing, for example, along with each message, there should be the possibility for the individual to easily select the option to no longer receive content from that sender or of that nature.



C.8) ANALYTICS

C.8.1) CASE STUDIES

C.8.1.1) PRODUCT PERFORMANCE ASSESSMENT

Noticing a decline in the number of subscriptions to their digital magazine, the managers of a newspaper decided to contract a startup specialized in measuring content performance. The magazine's

intent in this case is to verify how the general public has been receiving its work, which articles have generated more engagement, so that it can design contents that are more compatible with its audience and that interact in a more satisfactory manner with the subscribers. (**phase 1**)

The technology company provides a program capable of capturing page access metrics, time spent reading content, how far the articles were read, and which parts of the texts the user paid most attention to, all by capturing data from cursor movement and clicks. The magazine's managers were impressed by the idea but also concerned about their customers' data, processed on the basis of legitimate interests.

The startup then clarified that, since the purpose of the collection is solely for performance measurement, there is no need to identify users, which is why their IP addresses are automatically deleted before the data is shared with the company (**phase 2**). It also added that, as its goal is to produce statistical indicators, all information goes through a process of anonymization and aggregation. (**phase 4**)

Everything that will be collected from the magazine's website will be shared by VPNs and stored in the servers of the startup, which has a strict data security policy and guarantees the disposal of all information transferred once the agreement with the magazine is terminated. (**phase 4**)

C.8.1.2) COMMERCIAL STRATEGY

A network of university preparatory courses with units all over the country realized that the performance of some units was much more prominent than others, without there being substantial differences in the levels of training of the teachers or the materials used. The network then decided to act strategically concerning the teaching methods employed in its classes.

The idea of the project was to statistically analyze the correlation between (i) teaching methodologies adopted by the teachers, (ii) characteristics of classes, such as age range, class schedule, and region of the units, and (iii) students' exam results and grades obtained from simulated activities. Based on this, the university preparatory course's goal was to better understand which teaching methods were related to better results for certain class profiles (**phase 1**). The lawful basis employed for the processing of the personal data involved in this analysis was that of legitimate interests.

Managers were concerned to ensure that these analyses were not intrusive and did not undermine their relationship of trust with the network and its students. For this reason, it was decided that only the information strictly necessary for the analysis would be used and not all the information in the institution's database, which included a much wider range of personal data on students (**phase 2**).

One of the points raised by the creators of the project was that university preparatory courses are expected to monitor students' performance, so that seeking to extract strategies to improve teaching methodologies (and results, as a consequence) would be compatible with the pre-established relationship between the parties (**phase 3**). Undoubtedly, regardless of such expectations, the university preparatory course decided that it would be transparent with the students about the main aspects of the analyses performed and the personal data involved, to ensure that anyone who wished so could object to the processing (**phase 4**).

C.8.1.3) INTELLIGENCE GENERATION

The State Public Defender's Office is engaged in a project to systematize and generate intelligence concerning the legal proceedings of all its agencies distributed throughout the state. The purpose is to create an informational base from their individual litigations, which will serve as input to generate intelligence for the filing of public-interest civil actions. The idea is that the Defender's Office will be able to measure the most recurrent demands, identify the biggest issues by region, and, thus, start public-interest civil actions (**phase 1**).

The program has a double function, that of serving as an indicator of the problems faced by the users of this public service and that of being a strong persuasive argument, both to reach agreements

between parties and to increase the chances of success of the Public Defender's Office in the Judiciary.

Since the data were entrusted for a reason other than to be used for this type of analysis – even though the purpose of the latter is to improve the work of the Public Defender's Office (**phase 3**) – the public servants soon questioned to what extent the data would be shared with the base of the program. After a series of discussions, they concluded that, for example, data referring to the moment of screening users to determine if they qualify for a public defender would not need to be shared with the program (**phase 2**). At the same time, it would not be ideal to aggregate and anonymize the information contained in the case records, since it would be important to locate the parties and the case record number of granting or agreement in a lawsuit, as this would be essential information for the occasional execution phase.

C.8.2) ANALYSIS OF LEGITIMATE INTERESTS IN ANALYTICS

Legitimacy:

The use of the analytics by companies, or even associations and other entities represents a legitimate interest, there being no legal prohibition for this practice. It must have a clear and specific purpose.

Necessity:

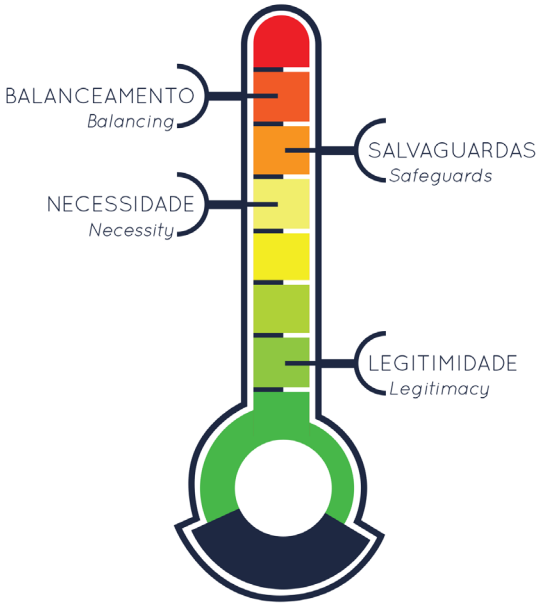
The very nature of analytics, an applied use of data for strategic purposes, often does not require direct identification of the user (but may still require identifiable data), so controllers must be aware, in each case, of the actual amount of data that will be strictly necessary to obtain the intended results.

Balancing:

The aspect of legitimate expectations of the data subject can be delicate in the case of analytics since most of the time, individuals are unaware of the mechanisms that are used to collect data and process it in order to extract intelligence. In addition, the data used has been often collected for a different purpose, which reduces the possibility of there being a legitimate expectation. It is important, therefore, to refer to the ideas of ''compatibility'' and ''contextual proximity'' addressed in the theoretical sections of this document.

Safeguards:

When possible, measures such as pseudo anonymization and data aggregation should be applied, but, in some cases, keeping the data in an at least identifiable manner may be essential to establish a strategy. In any case, transparency vis-à-vis the data subject is an indispensable measure that can help sustain the legitimate interest.



C.9) ARTIFICIAL INTELLIGENCE

C.9.1) CASE STUDIES

C.9.1.1) STUDENT EVALUATION

Due to a global pandemic, all schools were closed for an entire school year. In this context, countries all over the world had to rethink, among many other things, how the entrance of students into universities would work.

In Brazil, the solution found was to replace scores of ENEM, the largest exam for students to enter federal universities, with a score assigned by an artificial intelligence system, based on the school performance of students during high school. The purpose of using the tool was, therefore, to support social isolation measures while also operationalizing an objective criterion to determine who should have access to public higher education. (**phase 1**) The lawful basis used to justify the data processing was that of legitimate interests.

Knowing that the solution was likely to raise controversy, the government decided to be as transparent as possible about the use of the AI system (**phase 4**). The first point emphasized was that only data regarding the student's academic performance would be used, so that other sensitive and potentially discriminating data would not be analyzed by the algorithm (**phases 1 and 2**). Secondly, it argued that the academic records data refer to the measurement of academic performance, and, thus, would be compatible with the purpose of replacing the national Exam (**phase 3**). Finally, it reiterated that all information would be processed transparently and in a high-security, fraud-proof and information leak-proof system (**phase 4**).

Despite the governmental statements, protests were not avoided and mainly criticized the difficulty of understanding the tool, given the lack of clarity about the operation of the system and the importance of the criteria employed (**phase 2 and 3**). In addition, the breach of students' expectations was considered, since they did not take the tests during their school years with the perspective that they would be used in the future for their University admissions (**phase 3**).

C.9.1.2) BONUS SYSTEM AUTOMATION

The managers of a computer company decide to automate the bonus system for their employees. Their idea is that, from then on, the bonus will be measured by integrating several pieces of information regarding productivity and by sizing the profits that each employee brings to the company. To start running the software, managers reported that it would be necessary to share employee productivity and profitability data so that the AI could identify organizational patterns and the progression of the work performed by the workforce over time.

Those responsible for the project took the proposal to the executive board of the company, which was concerned about possible results that distorted the merits of its employees, also questioning the possible risks of AI making discriminatory inferences. Despite this, they decided to go ahead with the project. Both directors and managers understood that the company had a legitimate interest in seeking to improve its bonus system (**phase 1**).

Still, they agreed that a number of issues had to be addressed if the processing of data for these purposes was to take place properly. One of the points discussed was that, so that the amount of data treated would not be excessive and in order to paint an accurate picture of the company's reality, only information referring to the activities of the last 5 years would be used. (**phase 2**).

Both agreed that there would be no problems regarding the employees' expectations regarding the processing of their data, since this same information had served the purpose of granting bonuses previously, with a different system (**phase 3**). In addition, other measures should be taken. One of them would be the creation of a space where employees could safely question the results of the system and also the data that has been entered into it. Another one, considered as a good practice by the company, was to promote as much transparency as possible about the tool's calculation methodology, thus allowing questions and corrections to be made about its operation and results (**phase 4**).

C.9.2) ANALYSIS OF LEGITIMATE INTERESTS IN ARTIFICIAL INTELLIGENCE

Legitimacy:

In principle, the use of artificial intelligence for several purposes, by companies and other entities, is legitimate and supported by law.

Necessity:

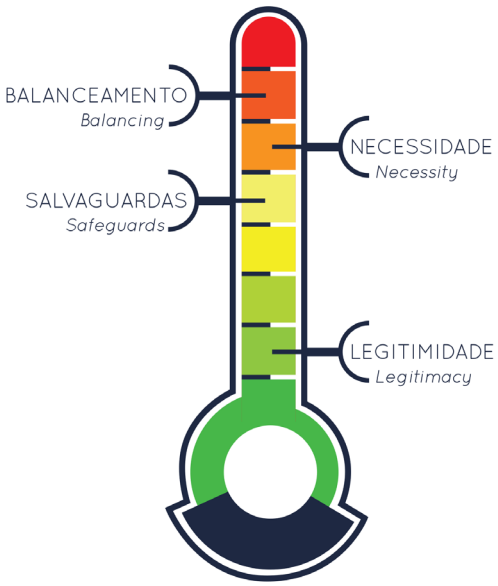
It is common that artificial intelligence systems need a substantial amount of data to "feed" them and allow them to encode or learn. Despite this, it is still important that the relationship between the data collected and its necessity for achieving the specific purpose of that AI work cycle is made very clear.

Balancing:

This is when applications of artificial intelligence supported by legitimate interests can become critical. This is because, depending on the type of AI and also on whether these systems produce partial or fully automated decisions, it is possible that the use of personal data will result in highly impacting decisions, without it being clear how such decisions have been reached. Thus, in addition to analyzing whether there is any level of legitimate expectation present, it is also important to assess the possible imbalance between the interest of the controller or third party and the rights and interests of the data subjects and how this impacts the balancing stage.

Safeguards:

Precisely because of the criticality, existing in certain cases, of the use of artificial intelligence vis-à-vis the data subjects, the implementation of safeguards that can mitigate the negative effects of the processing, such as strong information security, pseudo anonymization, transparency measures and the possibility to object to processing, must be applied.



C.10) LOGISTICS

C.10.1) CASE STUDIES

C.10.1.1) INVENTORY MANAGEMENT

A small chain of pharmacies wants to optimize the management of orders and product inventories, understanding that the most efficient way to carry out logistical control of this type would be based on the purchases of its customers. In addition to measuring inventories, this strategy would help the pharmacy understand which products have the greatest demand and which are no longer worth selling. The chain then intends to install a system that collects and systematizes all its sales in both physical and virtual stores, generating stock replacement notices **(phase 1).**

It so happens that, in certain situations, the sales data were automatically linked to the buyers' information, such as when using the pharmacy's loyalty system or when making online purchases. Considering that in these cases the collection of personal data took place for specific purposes which were different from stock control, the pharmacy realized that it would need a lawful basis to justify the logistics system, identifying legitimate interests as the most appropriate.

The pharmacy concluded that the most important thing was to minimize the amount of data shared with the system **(phase 2)**, thus, the integration with the purchase would be restricted to the product of the sale, price and time, automatically removing all information directly related to the buyer, in order to generate a pseudo-anonymization **(phase 4)**. It is also important to note that, in this case, the use of data for logistic purposes does not escape the expectation that the user has about the business in its entirety **(phase 3)**. In addition, transparency measures regarding the use of the data and its purpose would be put into practice, informing the data subjects about the new processing operation **(phase 4).**

C.10.1.2) TRANSPORTATION AND DELIVERIES

A retail chain, interested in optimizing its goods delivery system, enters into a partnership with a startup specialized in collecting and processing geolocation information. The service offered by the startup is the correlation of delivery information from the retail store with strategically designed routes, so that the product arrives as quickly as possible at the customers' address. The geolocation data serve as a guide, which, based on information about travel time, congested routes, and the best traffic times by region, automatically determine the most efficient route to be taken by the delivery person (**phase 1**). To make the partnership possible, it will be necessary to integrate the delivery orders database with the startup's system. The lawful basis applied by the controller to such operation is legitimate interest.

To comply with the requirements of the legitimate interests provision, the company was careful to think about an integration that restricted the sharing of information to what was strictly necessary. In this sense, although the retailer's sales register contains a lot of information about the buyer, for each delivery a customer code would be generated and, thus, only the delivery address, the purchase date and the customer code (which the customer also has in order to confirm his or her identity during delivery) would be shared with the startup's system. Based on this information, the software would indicate to the delivery person the routes referring to the codes assigned to the customers, so that only this employee would have access to the customer's purchase and identification information (**phases 2 and 3**). Despite this measure, a later analysis found that the company had failed to inform the practice to customers through transparent warnings and to give them the opportunity to object to the processing. This was subsequently remedied in a later version of the strategy (**phase 4**).

C.10.2) ANALYSIS OF LEGITIMATE INTERESTS IN LOGISTICS

Legitimacy:

This is a legitimate purpose, without legal restriction, which must also be concrete in each case.

Necessity:

In the case of logistics, it is possible to considerably reduce the amount of data considered necessary for the activity in question - a point that should be noted by controllers when planning data processing, especially since it is common for companies to hold registration data, collected for other purposes, which should not be automatically "transferred" for the purpose of logistics.

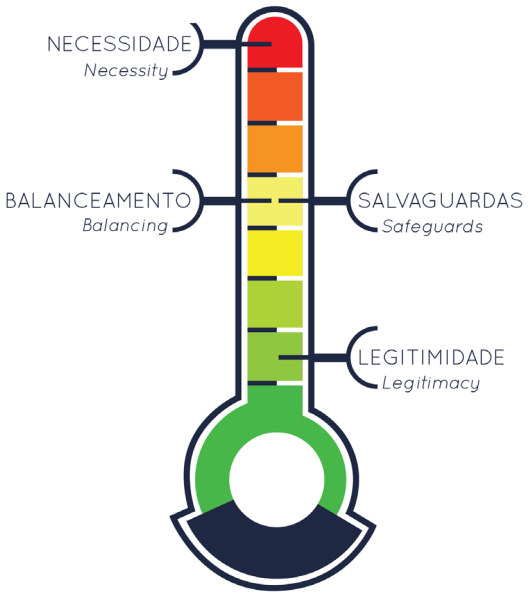
Balancing:

Data subjects have an expectation that some data collected in a purchase will be used to facilitate delivery logistics, which is even a measure favorable to them. Nevertheless, it is necessary to verify if the processing, in the specific case, does not present any kind of unintended harm or discriminatory effect to the interests and rights of the data subjects.

Safeguards:

The use of data for logistic purposes can be considered so commonplace in a company that safeguards concerning personal data can be occasionally forgotten. Measures such as strong information

security policies, transparency and pseudo anonymization should be considered.



C.11) EXAMPLE OF A LEGITIMATE INTEREST ASSESSMENT

"Trabalho para Todos" is an association whose mission is to promote activities and projects that reduce unemployment in the country. One of its projects was the creation of an online platform, "Emprega Mais", whose specific purpose was to bring together companies that were hiring and potential employees.

"Emprega Mais" operates as follows: interested people register on the platform (giving their name, email address, and phone number), also entering some professional information (previous experience and other relevant information). There is also a place for companies to register their job openings, indicating the functions to be performed and, if any, the requirements needed for each position. "Emprega Mais", identifying candidates compatible with the criteria of a certain position, contacts the company to inform it that it has applicants that may be of its interest. If the company informs that the vacancies are still open, "Emprega Mais" then informs the candidates of the existence of the opportunity and suggests that they contact the company in question.

The association, however, considered that this intermediation model made the process slow, delaying the contact between the company and the candidates. Having that in mind, "Trabalho para Todos" realized that it would be more efficient if the information of candidates compatible with the vacancies were directly shared with the companies that were hiring. In the new model, the employer, if interested in the candidate, could contact him directly, which would facilitate the approach.

"Trabalho para Todos" soon realized that sharing data with companies would mean carrying out a new kind of data processing of those registered on its platform. Considering that, in principle, the collection of information would serve only (i) to verify the compatibility between candidates and vacancies and (ii) for "Trabalho para Todos" to contact the data subjects, it was understood that the sharing of data with companies was something different that required its own lawful basis for processing.

That being said, "Trabalho para Todos" concluded that the most appropriate lawful basis in the case, according to the provisions of the Brazilian General Data Protection Law, would be that of legitimate interests. For this purpose, it verified and documented the legality of the processing by means of a legitimate interest assessment:

PURPOSE *Description of the necessary purpose for which the personal data will be processed*
The purpose of sharing is to bring together job seekers and potential employers.

Personal data processed *List of all kinds of data involved in a processing operation and needed for its purpose*
• Full name • Phone number • Email • Education • Previous work experience

LAWFUL BASIS	DETAILS	NOTES
Legitimacy of the interest (Article 10, head provision, and Item I of LGPD)	*Legitimate purpose* Description and verification of the controller's or third party's interest in processing the data to verify whether it is legitimate, i.e., lawful and appropriate.	The purpose of sharing is to make an informed suggestion concerning possible employees to the companies, an interest that is legitimate, in the sense that it is lawful and, as will be seen, concrete. Also, while the processing is of interest to Emprega Mais, there is also a potential benefit to the data subjects themselves. Finally, the end goal of the activities conducted by Emprega Mais, and by this specific processing, is to help unemployed people get jobs, a process that will be optmized by the new flow of communication.
	Specific situation Description of the actual context in which the data processing will take place, provided that abstract or generic situations that may exist in the future will not be accepted.	The association will share contact details of those who have signed up for its job search program only when there are objective indications that there is a match between vacancies and candidates.

Necessity (10, paragraph 1, of the LGPD)	*Minimization* Verification that only the personal data strictly necessary to achieve the intended purpose are being processed, thus avoiding the use of excessive, non-compliant, and inappropriate data. Checking whether there are other less intrusive kinds of data available to the controller that could possibly be used to achieve the same purposes.	The sharing data is restricted to what is necessary to identify the candidate (name), for the company to contact him or her (email/phone number – both were required considering the possibility of loss or that one of the means would be outdated), and for the company to verify whether the minimum requirements expected to fill the vacancy would be met (education and experience).
	Other lawful bases Verification of whether a different lawful basis, such as consent, performance of a contract, legal obligation, or another provided for in the list of Article 7, would be more appropriate in the context of processing in the specific case.	The association believes that while it might be possible to process the data based on consent, this basis did not prove to be the most suitable, mostly due to the large number of applicants and the difficulties posed by securing and managing valid consent. Performance of a contract (or steps prior to entering into a contract) doesn't apply either, for a number of reasons that include the parties involved in the relationship and the fact that, even hypothetically, the link between applicants and companies is too abstract to be considered a preliminary step prior to entering into a contract of employment. All things considered, legitimate interests was understood to be the most adequate lawful ground for processing.
Balancing (Article 6, I, 7, IX, and Article 10, II, of LGPD)	*Legitimate expectations* Verification: (i) whether there is some kind of pre-established relationship with the data subject from which his or her possible expectation may be inferred; or (ii) whether the average person, in the context of the data processing, could envisage that his data could be processed for the purposes described here.	There is a pre-established relationship that is consistent with the processing. The data is provided by the data subject and the reason why it is collected in principle – which is to check the compatibility between candidates and vacancies – is closely related to the second stance of processing, i.e., the sharing of data from those seeking employment with those who are hiring.

	Fundamental rights and freedoms Checking whether fundamental rights and freedoms (such as privacy, freedom of speech, freedom of movement, freedom of assembly and association, and others provided for in the law) will be disproportionately impacted to the point of harming the individual in an unauthorized manner.	The analysis carried out by "Emprega Mais" revealed that the risk posed by the processing activity was low. This assessment took into account the fact that the processing does not involve, as a rule, sensitive data (Art. 11, LGPD). Also, while the system applied to determine potential candidates is partially automated, the actual process of connecting applicants and companies is not and it doesn't itself involve predictive analysis or inferences. The potential impacts of the sharing are measured against the potential benefits and it is understood that remaining risks can be remedied by adequate safeguards, such as enhanced transparency and an opt-out mechanism.
Safeguards (10, paragraph 2 and paragraph 3, of the LGPD) Measures and tools employed to guarantee the rights of data subjects and prevent their data from being misused.	*Transparency* Explanation, in a clear and easy to understand manner, of which data is collected, how it is used, for what purposes, for how long, as well as specific information regarding data sharing, responsibilities of data processing agents and the rights of the data subject.	The association has an easy to understand privacy policy displayed in an accessible way on its website. There is a clear description of the data collected, the type of processing, its purpose, specific information concerning the sharing, the duration of the processing and the exercise of data subject's rights. Another measure taken to proactively ensure transparency was to publish a summarized version of the legitimate interest assessment. In addition, the mechanisms to request acess to the data (and other data subject rights) are also available in an accessible way on their website.
	Opt-out mechanism How the data subject can object to the processing of his or her data if he or she does not agree with it or if the processing is unlawful.	Among the safeguards "Emprega Brasil" makes available, on its site , an option for the data subject to indicate that he or she doesn't want their data to be directly shared by Emprega Mais with potential employers. There is also a clear explanation of the consequences of this choice and the website provides an alternative where the data subject may contact potential companies through an institutional contact.
	Other risk mitigation measures Examples of possible measures: anonymization; pseudonymization; segmentation of the databases; data access control.	"Emprega Mais" realized that mitigation measures such as anonymization would not make sense in relation to the purpose of the processing. Possible mitigation measures would be the storage of data in a secure location (its own servers) and the segmentation of the databases according to the purpose of processing.

GLOSSARY

Analytics: Applied use of data in analysis and systematic reasoning for the purposes of executing efficient decision making process. It uses mathematical, statistical, and predictive modeling techniques for the purpose of finding meaningful patterns and knowledge through data.

Anonymization: Use of reasonable and available technical means at the time of processing, whereby a data loses the possibility of association, directly or indirectly, with an individual, as defined in the Brazilian General Data Protection Law, Article 5, XI.

Machine learning: The Subfield of Artificial Intelligence that explores the ability of computers to detect patterns and create connections to develop by themselves to perform a function without direct programming by a human.

Database: Structured set of personal data, established in one or several places, in electronic or physical support, as defined in the Brazilian General Data Protection Law, Article 5, IV.

Controller: individual or legal entity, governed by public or private law, who is responsible for decisions regarding the processing of personal data, as defined in the Brazilian General Data Protection Law, Article 5, VI.

Consent: free, informed, and unequivocal statement by which the data subject agrees with the processing of his personal data for a specific purpose, as defined in the Brazilian General Data Protection Law, Article 5, XII.

Cookies: Internet files that store a user's browsing data, which are used to identify the visitor, identify network usage patterns, and facilitate the sending of data between pages on the same site.

Aggregate Data: Summarized or statistically treated data, numbers presented in the form of a single, whether a total, an average, percentages, proportions, etc.

Personal Data: Information related to an identified or identifiable individual, as defined in the Brazilian General Data Protection Law, Article 5, I.

Sensitive Personal Data: Personal data on racial or ethnic origin, religious conviction, political opinion, association with a union or religious, philosophical, or political organization, data concerning health or sex life, genetic or biometric data, when related to an individual, as defined in the Brazilian General Data Protection Law, Article 5, II.

IP Address: A numerical representation for the “Internet Protocol”, used to identify where a device is connected to the Internet, also containing parts of the nature of the connected device.

Artificial Intelligence: Human-like intelligence executed by software systems, technology that simulates the human capacity to reason, perceive, make decisions, and solve problems.

Processor: individual or legal entity, governed by public or private law, who performs the processing of personal data on behalf of the controller, as defined in the Brazilian General Data Protection Law, Article 5, VII.

Pseudonymization: A procedure that renders data pseudonymized, that is, that removes the immediate identification of the data subject, but does not completely break the link between data and subject, being subject to reversal techniques.

Privacy by Design: The idea that personal data protection should guide the design of a product or service that facilitate the control and protection of personal information.

VPN: Acronym for “Virtual Private Network”, which is a virtual private network, corresponding to an intermediate network between the user and the Internet and offering additional tools for secret browsing.