ITS
Instituto
de Tecnologia
& Sociedade
do Rio

Report

Algorithm Transparency and Governance: a case study of the Credit Bureau Sector

Introduction

The present study assesses the way credit bureaus[1] ('CB') make use of personal data – through collection, process and access –, thereby focusing on the possible impacts that such use exerts on vulnerable groups, aiming to identify the best practices that can render more transparent and informed the relationship between CB and personal data subjects.

The study has three parts. In the first section, we discuss how CB handle concepts such as risk assessment and how the use of personal data may lead to discriminatory conducts in credit granting. Secondly, we display the Brazilian legislative panorama regarding the protection of personal data. In the last part, we finally draw our conclusions on the data access mechanisms that CB provide, based on the analysis of the terms of use of the services that Serasa-Experian (in relation to the Mosaic service) and Boa Vista offer. Moreover, we make considerations about the best practices that CB shall adopt for services relative to the collection, process and access of third-party data.

The methodology of this work consisted of a legal analysis of the service contracts of these CB available both on their own websites and on the pages of public entities with which the CB have contract. It equally included an assessment of the products and the information that these CB make available on their websites.

[1] The term Credit bureaus traditionally refers to a for-profit or non-profit private institution that manages databases of the financial system on the situation of credit borrowers (see Simeon Djankova, Caralee McLiesha, Andrei Shleifer. Private credit in 129 countries. Journal of Financial Economics 84 [2007]. P. 305) Today, however, these entities have expanded their scope, acting not only in the financial sector, but also in several other sectors, including providing information to the public sector, thus becoming information bureaux, as we will further explain in the next topic.

Chapter I – Credit and discrimination[2]

1.1 – Risk Assessment, credit bureaus (‘CB’) and positive/negative discrimination

The CB base their activities on a risk assessment mechanism[3], which verifies the probability of a person being a debtor[4] and then allocates it to a particular risk category in order to justify decisions relative to the granting of credit[5], interest rate[6] and possible conclusion of contract[7].

In order to carry out this analysis, CB seek to obtain as much information as possible about the person that seeks credit[8], such as data concerning habits and economic condition[9], and others that may not directly relate to credit capacity, for instance health information, including those relative to genetic data[10].

The commercial sector, through associations such as the Shopkeepers' Chambers (Câmaras de Dirigentes Lojistas - ‘CDLs’), and financial institutions were the first segments in the country to develop the research on consumer information for credit granting. These Chambers, together with other trade associations, created the first unified databases on information on default, which their associates could feed and consult. Since the first CDL, created in Porto Alegre in 1951, congeners have emerged in Rio de Janeiro, São Paulo and other units of the federation, thereby providing several cities with so-called ‘credit protection services’, aimed at assuring greater security to the granting of

[2] The authors of this report carried out the translations contained in the text.

[3] LIEDTKE, Patrick M. What’s Insurance to a Modern Economy. The Geneva Papers, 2007, 32; p. 214.

[4] JENTZSCH, Nicola. Financial Privacy: An International Comparison of Credit Reporting Systems. Springer: 2007; p. 274.

[5] BAKER, Tom. Containing the Promise of Insurance: Adverse Selection and Risk Classification. University of Connecticut School of Law Articles Working Paper Series. 2001.

[6] International Finance Corporation (IFC) - World Bank Group. Credit bureau knowledge guide. Available at http://www.ifc.org/wps/wcm/connect/2867f3804958602ba222b719583b6d16/FI-CB-KnowledgeGuide-E.pdf?MOD=AJPERES&CACHEID=2867f3804958602ba222b719583b6d16. Access on November 13, 2016.

[7] VIOLA DE AZEVEDO CUNHA, Mario. Privacidade e Seguro: a coleta e utilização de dados pessoais nos ramos de pessoas e de saúde. Cadernos de Seguro – Teses n. 33. Funenseg: Rio de Janeiro, 2009; p. 22.

[8] MEYER, Roberta B. MEYER, Roberta B. The insurer perspective. In Genetics and life insurance - Medical underwriting and social policy. Mark. A. Rothstein. MIT Press: 2004; p. 29.

[9] International Finance Corporation (IFC) - World Bank Group. Op. cit.; p. 12.

[10] International Finance Corporation (IFC) - World Bank Group. Op. cit.; p. 7.

credit for trade.

These services are nonetheless of a conspicuously local nature. In order to obtain a greater degree of coverage and efficiency, other services of national scope and with unified databases gradually replaced those local ones, as is the case of the services that Serasa, Boa Vista and SPC Brazil currently provide. Such businesses rely on information both from public sources (eg, notarius publicus or courts of justice for data on lawsuits) and private sources (from their own databases) to integrate the services they offer to their clients.

Today, the activity of these CB does not limit to mere credit analysis. Some CB have, over time, offered other types of service aimed at further purposes: marketing, market prospection and others. They have become real bureaux of information, reaching up to the current figure of data brokers – entities that seek to extract to their clients content and the usefulness of the range of information to which they have access, which often comprises the transaction of their own information.

The clients of these bureaux are their consulters. In the case of credit analysis, these consulters may be traders or financial institutions that need to make a decision relative to the granting of credit or possibly some other financial service to a person. Once they carry out the credit operation, the credit assignor (who was the consulter of the bureau) becomes the creditor of the data subject (who becomes the respective debtor). The bureaux take into account data concerning natural or legal people. The present study refers to these people as data subjects. Even so, with exception to some specific reference, this study deems subjects only natural persons, insofar as the considerations and conclusions that we adopt relate to those that affect these people. In addition to ‘data subject’, we will also use ‘potential customer’, ‘customer’ and ‘consumer’ in order to refer to the person that the collected and processed information concern. These nomenclatures differentiate the contractual timing of such persons – either prior to taking credit or during that relationship. By the same token, they can refer to the specific nomenclature that certain legislations apply, such as the Consumer Protection and Defense Code

(Código de Proteção e Defesa do Consumidor – ‘CDC’), which uses ‘consumer’, or the draft of a general bill on personal data protection currently being processed at the Chamber of Deputies, which uses ‘data subject’.

1.2. Generalization and discrimination

The CB base most of their decisions on generalizations. Generalizations occur when a whole group of people receives the same treatment because of the behavior of some members of the group[11]. Thus, when CB analyze a group of clients to create a risk profile, or when they assess individual risks, they do so based on previous behaviors of others who have similar characteristics, considering data such as age, gender, ethnicity, or even domicile, as in the use of the residence ZIP code[12].

On the one hand, this generalization is necessary due to the asymmetry of information between clients and credit providers. On the other hand, this kind of generalization may engender distortions about individuals or groups of individuals, particularly those in vulnerable situations, or among those who behave in a deviant manner. The value of a car insurance for newly qualified drivers clearly illustrates this, as it is considerably higher than that for other adults[13]. By generalizing the behavior of young drivers, one can define in an abstract way that young people are more associated with vehicle damage than more experienced drivers, even if these young drivers never end up causing a traffic accident.

The major problem of generalization is the discrimination that it can arouse, since deviant individuals in the target group do not have the opportunity to prove that the generalizations made about the group do not apply to them and that this may be detrimental to them in certain circumstances[14]. Conversely, generalization often brings about benefits: in the above example of the young driver, if the price for insurance were the same for those who cause and those who do not cause accidents, the consequence would be an overall increase in the insurance value. This same reasoning

[11] SCHAUER, Frederick. Profiles, Probabilities and Stereotypes. Cambridge, Massachusetts: Belknap Press of Harvard University Press, 2003. P. 3.

[12] Ibid; p. 4.

[13] Ibid. p. 4.

[14] Op. cit.; p. 50.

applies to the credit granting.

1.3. Adverse selection

The collection and processing of personal information[15] aims to reduce information asymmetry in the relationship between suppliers and customers, thereby attenuating the adverse selection[16]. In certain situations, the asymmetry of information between the data subject and the credit provider is unavoidable, either because the potential customer does not voluntarily provide the information or, even when its provision is voluntary, its use is legally prohibited, as in the case of the Credit History Law[17]. In these situations, the CB play a key role insofar as they can gather information from sources other than only those that the data subjects provide.

Hence, in the case of credit granting, adverse selection is an undesirable fallout of the lack of available information on the future client's performance in relation to their ability to pay off debts. Under such circumstances, the CB yields an important service to the credit assignor since it reduces the possibility of the adverse selection phenomenon taking place, which would mean the entry of a larger number of clients with a high potential for delinquency.

The discussion on adverse selection is not a simple one, as it entails not only economic issues, but also other relevant matters, such as the potential risk of discrimination in credit granting. An example of adverse selection occurred in the US when insurers decided to base themselves on information about victims of domestic violence. In this case, the quest for avoiding adverse selection brought about a negative discrimination, when suggesting that women victims of domestic violence could not contract life, health and disability insurance[18].

We therefore perceive that the collection and use of personal information is of fundamental importance in order to avoid adverse selection and ensure the health of the financial markets. Even so, there are

[15] Section V of Art. 4 of Law 12,527/11 defines information processing as the 'set of actions relative to the production, reception, classification, use, access, reproduction, transport. transmission, distribution, archiving, storage, disposal, evaluation, destination or control of the information'.

[16] BAKER, Tom. Op. cit.; p. 2.

[17] Law no. 12,414, of June 9, 2011.

[18] BAKER, Tom. Op. cit.; p. 12

limits to such collection and use, in order to avoid that this procedure gives rise to negative discrimination hypotheses, as we have seen from cases in the USA. In the next chapters of this study, we seek to identify the limits that both the national legislation and the jurisprudence, notably the Superior Court of Justice, bear for the collection and processing of data that the CB perform.

1.4. Vulnerable groups

Before analyzing the limits that the national legislation and jurisprudence outline with respect to the collection and processing of data by the CB, it is important to scrutinize the groups considered vulnerable and the impact that the segmentation for credit granting purposes may exert on people in these groups.

For this purpose, we will deem vulnerable groups the conjunction of people who, for different reasons, do not have the same access to goods and services or to the full exercise of civil rights as other sectors of society do. Examples of vulnerable groups are the elderly, women, the disabled and the low-income population[19].

As discussed in the previous topic, generalizations can induce to distortions that sometimes affect disproportionately some groups, particularly those in situations of vulnerability.

In Brazil, the Superior Court of Justice[20] recognized the possibility of using techniques of generalization and discrimination aimed at granting credit. However, at no time did the aforementioned decision address the segmentation of society or the framing of specific people and niches of the population,

[19] Brazilian Center of Analysis and Planning – (Centro Brasileiro de Análise e Planejamento – Cebrap), of the Social Service of Commerce – (Serviço Social do Comércio – SESC) and the Municipal Secretariat of Social Assistance of São Paulo, SAS-PMSP. Mapa da Vulnerabilidade Social da População da Cidade de São Paulo (Social Vulnerability Map of the Population of the City of São Paulo). 2004. Available at http://www.fflch.usp.br/centrodametropole/upload/arquivos/Mapa_da_Vulnerabilidade_social_da_pop_da_cidade_de_Sao_Paulo_2004.pdf. Access on November 13, 2016. See Fundo Monetário Internacional. O papel do FMI para ajudar a proteger os mais vulneráveis na crise mundial. Available at https://www.imf.org/external/lang/portuguese/np/exr/facts/protectp.pdf. Access on November 13, 2016.

[20] Special Appeal n.1,419,697 - RS. Reporting Justice Min. Paulo de Tarso Sanseverino. 2nd Section. Judged on November 12, 2014.

such as those we present in our case study. For this reason, verifying the discrimination of groups considered vulnerable requires an evaluation not merely of the sampling of the data used in a decision-making system, but equally of their criteria.

In this context, it is also important to highlight that certain outputs considered, for instance, negatively discriminatory, stem from the analysis of data that do not directly identify the specific nature that characterizes the vulnerability of a group, but function as a link for this feature. Take the case of the postal zip code. Although the zip code does not contain information that, in itself, entails value judgment, when combined with the assessment of socio-demographic data on the set of inhabitants in certain localities, identifiable by the zip code, several inferences may emerge, which can engender the discrimination of a vulnerable community.

2. Limits on data processing for credit grant

2.1. Guidelines applicable to the processing of personal data

Differently from around 110 other countries, Brazil does not have a general law on the protection of personal data. Only general constitutional provisions and some sectoral rules discipline the issue in our legal system. In its Article 5, Section X, the Brazilian Federal Constitution recognizes privacy, intimacy, honor and image as fundamental rights. This same Article 5 guarantees the protection of other aspects of private life (Articles 5, XI, XII, and XIV). Furthermore, Section LXXII created a new constitutional action, the habeas data.

The Brazilian Civil Code, in turn, adopted a discipline like that of the Federal Constitution by including, in its Article 21, privacy as a personality right. It also extends, where applicable, to the protection of personal rights to legal entities[21].

In addition to the constitutional remedy of the habeas data, the only norms that specifically address the processing of personal data, which thus deserve special attention in this study, are the Consumer Protection Code[22], the Credit History Law[23], the Law on Access to Information (LAI)[24] and the Internet Bill of Rights, being the latter related to online data.

2.2 Sources of Information and their use aimed at credit granting

2.2.1. Information that the Government retains - Access to Information vs. Data Protection

Article 31 of Law 12,527/ 11 (LAI) provides that personal information relating to intimacy, the private life, honor and image 'shall have its access conceded only to legally authorized public agents and to the person to whom

[21] Article 52 of the Civil Code conveys this meaning.

[22] Complementary Law 105/2001 regulates the exchange of negative information between financial institutions and the Central Bank of Brazil.

[23] Law 12,414, from 2011.

[24] Law 12,527, from 2011.

they refer, regardless of classification of secrecy and for a maximum term of 100 (one hundred) years from its date of production' (our emphasis).

In turn, Article 4, Section IV of LAI establishes that personal information 'are those related to the natural person identified or identifiable'. One can therefore infer that data relating to legal persons are not subject to the access restriction that Article 31 conveys. It is yet noteworthy that third parties may even disclose or access personal information by means of a legal provision or express consent of the person to whom they refer, as Section II of the same Paragraph 1 of Art. 31 acknowledges.

The restriction on the provision of personal information only for those relating to intimacy, the private life, honor and image seems to be the position that the Brazilian Office of the Comptroller General adopts in its Handbook for States and Municipalities on the Access to Information Act. This organ defines personal information as 'that relating to intimacy, the private life, honor and the image of people'[25], thereby reinforcing the wording of Art. 3, V, of Decree 7.724/ 12, which regulated LAI[26].

The major issue that rises with the automated processing of personal data, however, is the uncertainty as to the real effects of the processing of personal data – which ultimately hinders an unequivocal association between personal data processing and a particular effect – such as damage to the image or honor.

This association of personal data to some effects is increasingly difficult to assess with certainty due to the enormous ease of collection and the possibilities that emerge alongside the processing of personal data with techniques capable of extracting meanings and uses that could influence different spheres of a person's life. It is against this background that the mere reference to the effects of the processing of personal data for personality rights becomes anachronistic, and it is practically impossible to determine, by the mere sectional analysis of their characteristics, what effects the

[25] Controladoria Geral da União. Manual da LAI para Estados e Municípios. 1st edition Brasilia, 2013; p. 29.

[26] Art. 3, V - personal information - information related to the natural person identified or identifiable, relating to itimacy, the private life, honor and image.

access to certain personal data may entail to their subject. In this context, it is necessary for the data subject to have concrete rights over their use, and an objective view on the processing of personal data that recognizes as a principle its protection by itself becomes relevant.

We must therefore take into consideration the set of means available today for the treatment of personal data[27] that render it impossible to evaluate in advance the effects of its treatment on the person, as well as the general clause of personality protection present in our legal system. While pondering these, we must highlight the need for an interpretation that comprises, to the maximum extent, the protection of personal data together with an employment of access to information that meets the public interest of transparency and control.

It is noteworthy, however, the fact that the access restriction set forth in Art. 31 of LAI does not comprise pure and simple personal information is not in any way equivalent to considering a standard option of the law to allow access to personal data when not deemed relative to the intimacy, private life, honor and image of the person concerned. The aforementioned difficulty in recognizing the effects derived from the use of a particular category of personal data makes it the case to consider that any personal information is currently capable of causing undesirable consequences to personality aspects, which induces to the non-provision of personal data as a standard operation. Moreover, the public administration may restrict access to it because it understands that it is essential to the security of society or of the State, as Art. 23 of LAI[28] predisposes.

Furthermore, even if the information does

[27] The aforementioned Decree n. 8.771/ 16 equally conveys a definition of data processing:

Art. 14. For the purposes of the provisions of this Decree, it considers:

(...)

II - processing of personal data - any operation carried out with personal data, such as the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, disposal, evaluation or control of the information, modification, communication, transfer, diffusion or extraction.

[28] Art. 23. We deem indispensable to the security of society or of the State and thus subject to classification the information whose disclosure or unrestricted access may: I - endanger the national defense and sovereignty or the integrity of the national territory; II - prejudice or jeopardize the conduct of negotiations or the international relations of the country, or those that other States and international organizations provide; III - endanger the life, safety or health of the population; IV - pose high risk to the country's financial, economic or monetary stability; V - prejudice or jeopardize strategic plans or operations of the Armed Forces; VI - prejudice or jeopardize scientific and technological research and development projects, as well as systems, assets, facilities or areas of national strategic interest; VII – pose risk to the security of institutions or high national or foreign authorities and their families; or VIII - compromise intelligence activities, as well as ongoing investigation or inspection related to the prevention or repression of infractions.

not have restricted access, it does not mean that its collection requires no procedure. Articles 10 to 14 of LAI and 11 to 14 of Decree 7,724/12 establish the guidelines for access to information held by the Federal Government, the states of the Federation, the Federal District and Municipalities and communes, public foundations, public companies, mixed capital corporations and other entities that these federative entities control directly or indirectly.

Finally, another limit to the access to personal information, whether restricted or unrestricted, is the principle of purpose. The secondary use of personal information, i.e. its use for purposes other than those that drove the collection of the information, is a matter of absolute relevance in several regulations related to the protection of personal data.

In accordance with the purpose principle, the reason for the collection or provision of personal information must be consistent with the ultimate purpose that drives the submission of this information to processing. Accordingly, when collecting information directly from the subject or consulting a data repository, its use will always coincide with the reason for this collection. This creates a link between the information and its origin, thereby channeling it to the target of its collection, so that any further processing takes this bond into account.

Thus, the principle of purpose is a corollary of the assumption that personal data, as a direct expression of personality, never loses the linkage with the data subject. Before being merely abstract and subject to free disposition, this piece of information, as it identifies some characteristic of a person, will always be bound to the subject. A deviation from the purpose of its collection may render harmless any attempt to protect and control this information by its subject.

Although there is no generic normative in the Brazilian legal system dealing with the principle of purpose, the Credit History Law and the Internet Bill of Rights contain provisions that, in light of the general clause of personality protection and the consideration that personal information is an integral element of the personality, materialize this principle in a transversal way.

2.3. The collection of information directly

from the data subject

The Consumer Protection Code does not require the consent of the data subject to open a registration on their behalf – a situation quite different from the one the Internet Bill of Rights and the Credit History Law provide for. Moreover, there are understandings in the sense that in situations where the treatment is different from that for which the data intended, there should be the consent of the data subject. However, it is worth noting that, after the issuance of the judgment on the case of credit scoring and the issuance of the Summons 550, the Superior Court of Justice dismissed the requirement of consumer consent in these cases.

2.4. Information from third party – private

The Consumer Protection Code does not prohibit the collection of data nor does it require the consent of its respective subject, as verified from the reading of the caput and Paragraph 2 of Article 43. Also within the scope of the Consumer Protection Code, one must send to the consumer a written notification of every act regarding the collection of personal and consumption data when the consumer does not request them. This certainly does not authorize the CB to grant data submitted to secrecy or any other type of legal protection nor does it allow their processing aimed at assessing the credit profile of their subjects. Additionally, one must make, upon the data subject request, any correction to the recorded data immediately and must communicate it to the subject within five working days.

However, the most recent trend in the Brazilian legal system is to require the consent of the data subject so as to allow their treatment in different situations. Such is the case of the Credit History Law, which, unlike the Consumer Protection Code, requires the consent of the subject for the collection and processing of their data

.

All things considered, in any situation related to the assessment of credit risk, it is essential to observe the rules that both the Consumer Protection Code and the Credit History Law introduce. This is equivalent to say that the collection and processing of personal data of consumers for this purpose can only take place when they are not excessive, i.e. when they relate to the credit risk analysis of the consumer, and where they are not sensitive. As a result, we already have two clear limits for the collection and processing of personal data for purposes of credit risk assessment.

In turn, the Internet Bill of Rights reinforces the logic of consent to legitimize certain data processing, as well as for its supply to third parties. Another limit that the Internet Bill of Rights establishes is the right of the user to the definite exclusion of personal data provided to a particular internet application at the end of the contractual relationship between the parties. The Internet Bill of Rights also relies on the principles of purpose and transparency as guiding precepts for the processing of personal data in the virtual environment, which is fully applicable to the credit risk evaluations that the CB perform, since these entities often rely on information collected on the Internet. Besides, it is important to note that the information bureaux must comply with indicating the information sources they use to the data subjects whose credit risk they are assessing.

3. Case Studies

In Brazil, several companies have offered, in their portfolio, personal information analysis services for various evaluation purposes. Some of them limit to or, at least, center on credit analysis, whereas others have a broader scope and aim at a range of objectives that, in fact, vary according to the demand of each customer of the service.

As an approach and case study, we identified services of two bureaus that perform activities in Brazil (Serasa Experian and Boa Vista) and thereby compared the transparency and nature of the personal information that feed them, which based the formulation of good practices recommendations that the sector should implement.

3.1. Analysis of data access mechanisms that information bureaux provide

Since mechanisms of evaluation and social stratification have unprecedentedly increased the use of personal information, this activity boasts a remarkable complexity. This complexity reflects not solely on the high volume of data amenable to processing by these mechanisms in an automated way but also on the opacity inherent to them.

Such mechanisms usually configure algorithms. Algorithms constitute a set of steps or activities required to accomplish a task – be it a ballistic calculation, an e-commerce platform and even tasks like voice recognition. Given that computers have been able to automate and execute algorithms, these have greatly increased their capacity and, consequently, their field of application.

The fact that algorithms execute ever more tasks makes them ubiquitous in our daily lives. Under these new circumstances, along with the greater efficiency one witness when considering several parameters of new business modalities that algorithms transform or render possible, we must take into account fundamental changes in what one can expect from the activities entrusted to them in terms of transparency, trust, predictability and other factors that directly concern the individual and society.

Many of these changes are tributary to features intrinsic to algorithms. Perhaps the most obvious one relates to the transparency of its operation. Thus, the data subject often lacks any evidence of what actually occurs between the input of his/her personal information and the final result, precisely because of the complexity of the operations performed, which makes it difficult to apply conventional transparency mechanisms.

At least two factors affect transparency regarding the operation of the algorithms: the first is that algorithm users traditionally claim that they are subject to intellectual property rules and that these consist in a commercial secrecy. In addition to this factor, some algorithms present such complex mechanisms that further hinder any objective gain with respect to transparency. At this point, we must highlight the algorithms that "learn" from the data that feed them and consequently modify themselves in such a way that, given their dynamic nature, their idealizers or programmers cannot strictly anticipate the output.

These considerations, coupled with the enormous relevance that algorithms have been exerting in our daily lives, make it ever more necessary to establish parameters in order to monitor algorithms and correct their results whenever needed. Classical cases in which this may be necessary occur when algorithms end up favoring discrimination or favoring certain individuals in situations that should praise equality[29].

Several lines of action are under evaluation to counter this problem. An axis underpinning many of them is the realization that transparency relative to algorithms, although fundamental, is not enough to put citizens in a condition of knowing the effects of these on their lives and making informed and legitimate choices in certain situations that require some form of facilitation or intermediation[30].

3.2. Use of personal data by credit bureaus: recommendation of best practices

[29] For a detailed discussion on the theme, see: Solon Barrocas & Andrew Selbst. Big Data's Disparate Impact. In 104 California Law Review (2016).

[30] In this respect, the creation of a regulatory agency to tackle algorithms has already been glimpsed. Andrew Tutt. A new agency. An FDA for algorithms. In: ssrn.com/abstract=2747994

In Brazil, several companies have been providing in their portfolio services of analysis on personal information for various evaluation purposes. Based on the case study of services offered by two bureaux that carry out this type of activities in Brazil, namely Serasa-Experian – in relation to the Mosaic service – and Boa Vista, we have elaborated recommendations of best practices, in order to investigate the level of transparency and the nature of the personal information that feed them.

4. Recommendation of best practices

Based on the particularities of the personal data and big data processing activity raised and on the elements of our current legislation, as well as on bills on data protection currently under discussion at the National Congress, we have elaborated recommendations related to transparency, good faith and protection of personality.

With respect to transparency, the focus is on the possibility of the bureau to provide data subjects with a clear attribution of their source aiming to elucidate any questions relative to the legitimacy of their use. Such measure renders it easier to trace and recognize the origin of problems with inaccurate information or with quality inadequacies, as well as the need to create a whistleblowing structure – similar to the one of an Ombudsman - that enables data subjects to exercise the rights pertaining to them.

As for good faith, the procedures related to personal data as well as the inferences and conclusions that may ensue shall respect the legitimate expectations of their subjects, deemed as such in terms of the purposes the subjects expect from the use of their data.

Lastly, as far as personality protection is concerned, the services offered to clients of the bureaux may not provide or facilitate discriminatory practices to their clients. In no case may they rely on sensitive or excessive information, or even those incompatible with the purposes that the data subject could reasonably envisage at the time of collection. They must particularly refrain themselves from deploying any type of processing that, despite stemming from legitimately collected personal data, results in inferences or conclusions that reveal sensitive data or lead to discriminatory practices.

5. Conclusion

The activities that the Credit bureaus develop are of great importance to the national economy. For this very reason, and considering the expansion of this activity in recent years, CB should be aware of the potential risks of negative discrimination that their actions may usher. Albeit the inexistence of a specific norm in Brazil that regulates the processing of personal data, both the legislation and the jurisprudence of the higher courts bring about parameters that establish clear checks for the processing of personal data aimed at risk analysis for the purposes of obtaining credit.

The legal compliance assessment of the data collection and processing that the CB carry out – the object of our analysis – found that the item of greatest concern relates to transparency regarding the performance of these entities, especially with respect to the information sources and the data used. We have equally identified that there are no channels of communication for the data subjects to exercise, in a facilitated and informed manner, their rights concerning the processing of their personal data.