/data protection in the financial sector

white-paper

BAPTISTA LUZ
ADVOGADOS

Last update: 12.04.2017

Renato Leite
Pedro Ramos
Ana Paula Collet Camargo
Laura Felicíssimo

/ INTRODUCTION

Although data protection regulations have been rising in the world in the last few years, Brazil does not have a General Data Protection Law.

Regarding data protection in the Brazilian Financial Sector, since the second semester of 2016 some associations and regulatory agencies have started some specific initiatives. In August 2016, ANBIMA, a Brazilian association for the financial and capital markets published a cyber security guideline[1], which shows the need for proper data protection procedures in the financial sector, since financial interests motivate the majority (80%) cyber security incidents in Brazil. Recently, in July 2017, the Brazilian Securities Authority (Comissão de Valores Mobiliários - CVM), published a study about the "perception of cyber risks in the activities of fiduciary administrators and intermediaries"[2]. The Brazilian Central Bank (BACEN) has opened a consultation[3] about a mandatory resolution to the entire financial sector regarding information security procedures and standards. The consultation, that was open until November 21st, deals aspects such as the need to appoint a cyber security officer and data localization rules determining that financial data must be stored in Brazil, measure that, if enacted, will probably impose extra costs that currently are not supported due to data been stored over the cloud in places with lower costs.

However, the Brazilian Financial Sector is subject to several sectorial regulations that affect how data must be processed. See below the list of relevant regulations, which will be discussed through this text:

[1] Disponível em: goo.gl/CFHsBT
[2] Disponível em: goo.gl/xNvBEn
[3] Disponível em: goo.gl/s7YvUU

- The Federal Constitution
- Criminal Code (Law no. 2,848/1940)
- Limited Company (Law no. 6,404/1974)
- Securities Market (Law no. 6,385/1976)
- Definition of crimes against the National Financial System (Law no. 7.492/1986)
- Consumer Code (Law no. 8,078/1990)
- Money laundering (Law no. 9,613/1998 as updated in 2003 and 2012)
- Bank Secrecy (Complementary Law no. 105/2001)
- Civil Code (Law no. 10,406/2002)
- Credit Report and Credit Scoring (Law no. 12,414/2011)
- Access to Information (Law no. 12,527/2011)
- Information Technology Crimes (Law no. 12,737/2012)
- Internet Bill of Rights ("*Marco Civil da Internet*") (Law no. 12,965/2014)
- Marco Civil da Internet Regulation (Federal Decree 8.771/2016, which regulates protection of personal data over the Internet)

/ MANAGING PERSONAL AND FINANCIAL DATA

The Right to Privacy is protected by the Brazilian Constitution (Article 5, X), as well the Right not to have Communication Intercepted, except in case ongoing criminal investigations (Article 5, XII). The Civil Code gives emphasis to the individual right to privacy and, for such a reason, courts, with the requirement of a person, may adopt all necessary remedies to stop activities that may affect an individual privacy.

The Consumer Code, Section VI, on its turn, regulates consumers' registers and database, especially regarding credit default history. Its article 43 regulates that the consumer shall have right to access to the information related to them available at registers and databases. Detailed provisions are:

(i) these registers must be user-friendly and negative information cannot be available after five years;

(ii) consumer must be aware of any register or database using their data;

(iii) consumer can demand the immediate alteration of incorrect data;

(iv) once the prescription of a consumer's debt applies, the Credit Protection Systems will not give any information that could prevent access to new credit.

The Consumer Code has been interpreted by the Ministry of Justice to clarify that clauses that allow for data transfer to third party without proper consent can be deemed invalid. Also, consent is needed to collect and use the data for purposes other than open registering the consumer to a database of clients or credit default.

In accordance with the regulation above, the Credit Report and Credit Scoring Law sets forth the database creation and consultancy regarding client's due performance for credit history. This type of database can only maintain the data necessary to evaluate someone's economic situation; it cannot retain excessive (not related/unnecessary) or sensitive data. Moreover, the data subject must give its consent so that the register can be opened. However, the person who owns the data can ask for its cancellation, in order to have access to it or correct its uses at any time.

Additionally, "Marco Civil da Internet" (Law no. 12,965, Article 7) defines that any organization collecting, using and treating data subjects' personal data for services rendered over the Internet must obtain his/her consent after providing clear and detailed information about data processing procedures. The purpose for the data collection must be legitimate and not prohibited by law. Also, the Federal Decree that complements "Marco Civil" defined what should be considered as: i) 'personal data' (the data related to the identified or identifiable individual, including identification numbers, locational data or electronic identifiers, considering that they are referred to a person); and ii) 'treatment of personal data' (all operation related to personal data, including collection, production, receipt, qualification, use, access, reproduction, issue, distribution, processing, filing, storage, exclusion, assessment or control of the information, modification, communication, transfer, spread or extraction) as stated on article 14, I and II; and iii) registration data, that encompasses parent's name, address and personal qualification (including full name, marital status and profession).

Also, the Decree sets some information security rules that must be followed by companies that treat personal data, including: i) the setting of a strict control on data access, including the duties of people who may access it; ii) the use of two-factor authentication systems, or other mechanism to ensure the individuality of the responsible for processing the log; iii) the need of a detailed inventory on the accesses to connection logs and logs of access to applications (including time, duration, identity of the responsible for the access and the accessed file); and iv) the use of cryptography technologies or similar protection measures to ensure data integrity.

Some observations are necessary regarding the Brazilian Criminal Code, which has a section dedicated to secrecy violation crimes. The invasion to a third party's electronic device, via unauthorized access and in breach of security systems to obtain or alter data can result in a detention penalty of three months up to one year, including payment of a fine. This penalty can increase if the invasion causes economic losses.

Databases of public records are subject to Law no. 12,527/2011, which allows public data secrecy only when a disclosure has the potential to jeopardize the financial or economic stability, amongst other situations concerning sovereignty.

/ MONEY LAUNDERING

The Money Laundering Law specifies that the financial sector must:

(i) identify its clients and maintain updated registers about them;

(ii) keep a record of all financial transactions that go beyond the permitted limit;

(iii) answer properly to all requests made by COAF (The Brazilian Board for Financial Activities Control) or another proper regulator, so this board will be responsible to keep secrecy about the answers sent;

(iv) render special attention to any transaction that shows serious evidence of constituting a crime, communicating the fact, in secrecy, to COAF within 24 hours;

(v) Institutions or people that do not cooperate with the requirements above may be subject to the following sanctions: warnings; fines; temporary inability to exercise management positions of financial institutions; disempowerment to the exercise of the activity, operation or function.

/ BANKING SECRECY AND CONFIDENTIALITY

There is a specific law in Brazil demanding confidentiality from financial institutions. The regulatory framework is complemented by several regulations provided by regulators such as the Brazilian Central Bank and the Securities Authority. Complementary Law no. 105, from 2001, according to which only the following situations do not violate the confidentiality obligations:

- information exchange between financial institutions for database purposes;
- information of credit defaulters required by credit protection entities;
- communication of illicit activity to proper regulators (e.g. CVM, COAF);
- information disclosure with the express consent of all the people involved and data subjects;
- the breach of confidentiality can also be required as part of a legal investigation, especially if for the following crimes: terrorism; drug or arms trafficking; extortion by kidnapping; against the national financial system; against the public administration; against tax law and social security; money laundering; practiced by criminal organizations.

It is possible to see similarities between Money Laundering Law and the Bank Secrecy Complementary Law when concerning data protection. The bank secrecy compliance and the data protection compliance permit exchange of private data if requested by specific public bodies associated with the financial sector or for legal investigation support.

The Law no. 7.492/1986 defines the crimes against the national financial system. In this regulation, violation of secrecy at an operation or service offered by a financial institution can result in a

detention penalty of one to four years and the payment of a fine, except if the information is required by authorities.

/ DATA BREACH NOTIFICATION

Brazil does not have a regulation to instruct data breach notifications in any sector. However, there are two general data protection bills related to protection of personal data. Both proposals shall enact instructions regarding data breach notifications for every sector of the Brazilian society, regardless of its nature.

Article 47 of Bill no. 5,276/2016, proposed by the Chamber of Deputies, establishes some procedures in case of any security incident. The proposed measures are very similar to the ones in Article 24 of the Bill no. 330/2013, of the Federal Senate. In summary, the data processor shall:

(i) communicate the incident within reasonable time to the Data Protection Authority (which shall be created);

(ii) offer detailed information about the nature of the damaged data, the personal information involved, the procedures used to protect the data, the risks related with the incident, the measures adopted to deal with it and, if the case, the reasons for the data processor to take too long to communicate the fact.

Depending on the damage caused to the data, the Data Protection Authority may ask for other measures as reporting the incident to the data subject, promoting the incident on the media or taking more actions to revert the incident (Article 48 of Bill no. 5,276/2016).

/ MARKETING, NEW MEDIA AND COMMUNICATIONS

Marco Civil stipulates that media's relationship with its users is a "consumer relation", therefore subject to the Consumers Code, which was already analysed in topic two. However, there is no specific relation regarding the use of data for marketing purposes.

Both general data protection bills mentioned are oriented to regulate the use of data for commercial practices, hence they will also apply for marketing purposes as well. Both proposals require the consent of the data subject, who should understand very clearly the purposes for the consent to be valid. In addition, companies should be responsible for data protection, keeping the use strictly to what was authorized.

/ INSURANCE

First, it is important to bear in mind that the data protection rules from the Consumer Code apply to insurance companies. On top of that, insurance companies are also considered financial institutions by the Law no. 7.492/1986, mentioned before, that defines the crimes against the national financial system. In this regulation, violation of secrecy at an operation or service offered by a financial institution can result in a detention penalty of one to four years and the payment of a fine, except if the information is required by authorities.

The National Council of Private Insurance (Conselho Nacional de Seguros Privados) issued the Resolution CNSP nº 297/2013 that regulates insurance companies' operations. This resolution determines that the insurance companies are responsible for the integrity, security and secrecy of their operations. On the other hand, they must provide to customers clear, precise and suitable information about the rights and obligations related to the insurance products offered.

Regarding, medical insurance, it is important to mention medical records regulation. Electronic medical records are regulated by the Federal Medicine Council's Resolution No. 1.821/07 ('the Resolution') (only available in Portuguese here). However, the Resolution focuses on the digitalisation of physical medical records and does not provide appropriate safeguards for sensitive personal data such as health data. There is no law making it mandatory for medical record service providers to request patients' consent to process their data, based on the fact that consent was already given to the medical doctor. However, market practices indicate that consent shall be obtained. There are internal policies dealing with this matter, which can be challenged in a court of law, such as in

cases where consent cannot be obtained, for example in the event of an emergency or when the patient is disabled. However, the medical records of an individual cannot be transferred to third parties, because they are considered part of a doctor/patient confidential document. This requirement is regulated by the Criminal Code, the rules of professional confidentiality and by medical profession regulations.

/ OTHER AREAS OF INTEREST

The relationship amongst professionals of the financial sector and data security is regulated by Brazilian Criminal Code and by specific rules presented by sectorial legislation.

The Criminal Code, in the section dedicated to secrecy violation crimes, enforces that the violation of professional secrecy can result in a detention penalty of one month to one year or the payment of a fine.

On the same direction, Limited Companies Law imposes the duty of loyalty to managers of this type of company. Managers cannot use for their own benefit, even without prejudice to the company, commercial opportunities discovered as a result of their role. They cannot omit from the company good business opportunities either; if these could bring benefits to them or someone else.

It is also necessary to keep secrecy of information that was not yet promoted outside the company, especially if it can influence the stock exchange. The managers must also make efforts so that the employers under their responsibility or people of their trust do not act against this rule.

If any person is damaged because of a fault in this duty, they have the right to be indemnified by the wrongdoer.

The Securities Market Law considers a crime against this market the use of relevant information yet not provided to the market. The penalty, in this case, is bigger than the one provided for in the Criminal Code, combining one to five years of reclusion with fines of up to three times the amount of the benefit obtained.

To reinforce the importance of this subject, the Securities Commission (CVM), authority responsible for regulating the securities market and its stokeholds in Brazil, issued Instruction 31, of 1984. This Instruction underlines the need to inform the market about relevant information that can affect all the investors of a company with shares on the stock market. In case the company opts to maintain some information in secrecy, such a decision must be submitted to CVM and all managers and shareholders must respect such secrecy.

/ CONCLUSION

Even though Brazil is still developing specific legal requirements to protect data regarding, the financial sector is already very concerned about data protection and already has specific regulations and directives to protect important information. The general rule is that financial data must be kept confidential. Also (i) information that might affect the market shall be disclosed; (ii) but, in some cases a company can keep a fact confidential if such a fact does not affect the market operation, however all the people involved must keep secrecy and should not take benefit out of it.