Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2018

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in January 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2015
Fourth edition
ISBN 978-1-912377-38-1

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Preface

Cybersecurity 2018

Fourth edition

Getting the Deal Through is delighted to publish the fourth edition of *Cybersecurity*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Australia, Italy, Philippines, Spain, Turkey and Ukraine.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2018

Brazil

Rafael Mendes Loureiro Hogan Lovells
Leonardo A F Palhares Almeida Advogados

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

It is important to clarify that Brazil lacks specific regulation on cybersecurity; although there are efforts to adopt a binding and integrated regulatory framework, Brazilian legislation on the matter is still evolving. The current legal framework is a patchwork of laws and regulations, as several 'soft laws' have been adopted.

In this regard, there are several official guidelines or laws that promote cybersecurity, such as the National Strategy for Defence, the Green Paper on Cybersecurity, the Cyber Defence Policy, the White Paper on National Defence, the Brazilian Civil Rights Framework for the Internet, the Carolina Dieckmann Law and the National Institute of Information Technology (ITI) rules.

In 2008, Brazil enacted Decree No. 6,703/2008, which created the National Strategy for Defence, under which three strategic sectors (outer space, cybernetics and nuclear energy) were identified as essential for national security. The Decree granted powers to the Brazilian armed forces on matters involving cybersecurity, given that, at the time, the military was being restructured and was seeking a new role as a key player in the political scenario of the twenty-first century.

The Green Paper on Cybersecurity, drafted in 2010 by a working group under the Office of Institutional Security of the Presidency of the Republic (GSI/PR), sets forth the key aspects of cybersecurity in the country and constitutes a first attempt to set out the principles for a future cybersecurity policy. This Green Paper views cybersecurity as an international challenge and makes reference to several strategies adopted by international entities, such as the Organization of American States (OAS), the Organization for Economic Cooperation and Development (OECD) and the International Telecommunications Union (ITU).

Prepared in 2012 by the Ministry of Defence to guide activities and proceedings related to cyber defence and cyberwarfare at the strategic and operational levels, the Brazilian Cyber Defence Policy establishes principles, objectives and guidelines for the consolidation of cybersecurity, which may serve as the basis for a specific legislation on the matter in the future.

The White Paper on National Defence, also prepared in 2012, following consultations with the government and the civil society, outlines the objectives of the National Defence Policy for the following two decades and establishes a budget.

The Brazilian Civil Rights Framework for the Internet, Law No. 12,965/14, regulates the use of the internet in Brazil through a series of principles, guarantees, rights and duties for internet users. The idea of the project emerged in 2007 and was collaboratively discussed in an open consultation with significant involvement of the civil society. The bill was ultimately sanctioned and approved in 2014.

The Brazilian Civil Rights Framework for the Internet addresses several issues, such as:

- net neutrality;
- privacy;
- data retention;
- the social function of the internet;
- freedom of expression and transmission of knowledge; and
- obligations related to the civil liability of both users and providers.

Known as the Carolina Dieckmann Law, the Cyber Crimes Act (Law No. 12,737/2012) defines certain cybercrimes, such as hacking into computers, violating user data or taking down websites. The project was drawn up when intimate photographs of actress Carolina Dieckmann were taken from her computer and made available on the internet.

The Law also provides for increased penalties if the invasion causes economic loss or if there is any disclosure, commercialisation or transmission of data or information to third parties. The penalties may also be increased if the crime is committed against the President of Brazil, the presidents of the Supreme Court, Chamber of Deputies, Senate, Legislative Assemblies and Municipal Chambers, among other authorities of the direct and indirect administration. In the absence of specific legislation, those who commit a cybercrime will be tried within the Brazilian Criminal Code itself.

In addition to the above, the ITI published a booklet entitled 'The ITI Industry's Cybersecurity Principles for Industry and Government', which establishes principles governing the joint effort of the industry and the government for the development of a policy framework to increase cybersecurity.

It is important to bear in mind that Brazil is not yet at the same level as several other jurisdictions in which there is a duty to notify authorities and users of data security breaches.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In Brazil, the patchwork of cybersecurity laws mainly addresses issues in connection with the banking industry. Other economic sectors are still neglected with regard to specific cybersecurity legislation. Nevertheless, policymakers are beginning to respond to concerns from other areas and industries, albeit in a fragmented and non-integrated manner. In order to combat cybercrime more effectively and address cybersecurity concerns, Brazil needs to involve the civil society and broaden public discussions on the issue. Lawmakers, law enforcement agencies, businesses, civil society organisations and citizens need to take a more active role in the construction of effective cybersecurity laws.

In addition, the existing cybercrime legislation has been the subject of significant criticism over the years for being too lenient. As an example, critics point to the Carolina Dieckmann Law, which defines the invasion of computer devices (hacking) as a criminal offence; however, the Law only establishes soft penalties (three months to one year in prison in addition to a fine). In comparison, the United States Personal Data Safety and Privacy Act establishes sentences of up to five years or a fine for similar offences.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Brazil has adopted international information security management policies. The Brazilian Association of Technical Standards (ABNT) developed NBR ISO/IEC 27001: 2006, which is an identical translation of ISO/IEC 27001: 2005, prepared by the Joint Information Technology Committee (ISO/IEC/JTC 1), Subcommittee on IT Security Techniques (SC 27).

The issues related to information security and communications, cybersecurity, and security of critical infrastructures are addressed

by the National Defence Council (CDN) and the Council of Foreign Relations and National Defence (CREDEN), linked to the GSI/PR.

The GSI/PR addresses issues related to Information Security and Communications (SIC) and Cybersecurity (SegCiber); the Information Security and Communications Department (DSIC), with activities in the APF. In addition, the GSI/PR manages SIC, and oversees the Incident Treatment Centre of Federal Public Administration Networks (CTIR Gov) as well as security accreditation.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

As mentioned, Brazil does not yet have specific laws regarding data protection and cybersecurity; however, according to the Brazilian Civil Code, responsible personnel and directors may be held accountable for actions taken on behalf of the organisation that involve negligence, malpractice or recklessness. Although the Brazilian Civil Code does not specifically address cybersecurity issues, it is possible to apply its provisions by analogy, depending on the facts of the case.

In addition to the provisions of the Brazilian Civil Code, there are two bills currently under discussion that specifically relate to data protection. Bill No. 5.276/2016 intends to create a civil data framework, with definitions of personal data, anonymous data, what data can be sold and what can be collected, among other points. The other bill (No. 330/12) is being discussed and, in addition to providing important definitions related to cybersecurity, also suggests the creation of a central authority for the protection of personal data.

Given that Brazil does not have a dedicated data protection law, the country still relies on a patchwork of provisions set forth in its Federal Constitution, the Brazilian Criminal Code and the Brazilian Civil Rights Framework for the Internet, which in its articles 10 and 11 states:

> *Art. 10. The custody of and access to Internet application connection and access logs, to which this Law refers to, as well as personal data and the contents of private communications, must respect the intimacy, private life, honor and image of the parties directly or indirectly involved.*
>
> *Art. 11. Any process involving the collection, storage, custody and processing of records, personal data or communication data by connection providers or Internet application providers in which at least one of these activities takes place in the national territory, shall respect Brazilian law, the rights to privacy, and the confidentiality of personal data, private communications, and records.*

In addition, the Brazilian Civil Rights Framework for the Internet establishes the following in its article 12:

> *Art. 12. Without prejudice to other civil, criminal or administrative penalties, the violation of the principles established in Articles 10 and 11 shall be subject, as appropriate, to the following sanctions, applied individually or cumulatively:*
>
> *I - warning, with a deadline for taking corrective action;*
>
> *II - fine of up to 10per cent of the gross income of the economic group in Brazil in the last fiscal year, taxes excluded, considering the economic condition of the offender and the principle of proportionality between the severity of the breach and the size of the penalty;*
>
> *III - temporary suspension of activities that involve the activities specified in Article 11; or*
>
> *IV - prohibition of engaging in the activities that involve the acts referred to in Article 11.*
>
> *Sole paragraph. In the case of a foreign company, its subsidiary, branch, local office or entity in Brazil will be joint and severally liable for the payment of the aforementioned penalties.*

5 How does your jurisdiction define cybersecurity and cybercrime?

The Brazilian government, through the GSI/PR, defines cybersecurity as 'the art of ensuring the existence and continuity of a nation's information society, guaranteeing and protecting, in the cyberspace, their information assets and critical infrastructures.'

Although the GSI/PR provides a definition of cybersecurity, there is no specific definition of cybercrime in the country and the case law understanding is that cybercrimes refer to any and all offences committed using computers or the internet, through a public, private or domestic network.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

As mentioned, there is no specific law that regulates cybersecurity in Brazil. As a result, the existing patchwork of rules and regulations has not defined specific measures that should be implemented by organisations in order to protect data systems and information technology from cyberattacks.

There are, however, specific security measures that certain industries must adopt to protect their customers' data. This is particularly true with regard to the banking and financial sectors, which must implement certain security measures in electronic banking transactions and require the use of multiple encrypted passwords, depending on the value and nature of the transaction.

It is also important to note that the Office of GSI/PR is currently working with various stakeholders to map the challenges of cybersecurity and to build a single and uniform document, to be discussed within Congress as the legal framework on cybersecurity.

In addition, there are independent initiatives being carried out by certain sectors of the economy to discuss cybersecurity. The Brazilian Central Bank, for instance, promoted an open consultation on matters involving cloud computing and the storage of data, as well as important aspects related to cybersecurity.

Once a general law on the subject has been approved, it will be the responsibility of the regulators to discuss and approve specific provisions with respect to each regulated sector, so that the principles and guidelines set out in the general norm are fully implemented.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Brazil does not have a law that deals specifically with cybernetic threats to intellectual property; however, Law No. 9,610/1998 determines that any type of intellectual product, regardless of being registered or published, is protected.

The above-mentioned law regulates copyright, which is managed by the Directorate of Intellectual Rights of the Ministry of Culture. Works and inventions that are not literary, artistic or scientific, such as computer programs, although protected by copyright, are under the responsibility of the Ministry of Science and Technology (MCTIC) and are regulated by Law No. 9,609/1998, which provides for the protection of the intellectual property of a computer program, its commercialisation in the country, and other measures.

There is a general understanding that these laws do not generally apply to the digital world, which has different manners of recording and reproducing works and inventions. As a consequence, there have been discussions regarding the revising of the copyright law, with the goal of adapting its provisions to expand, decentralise and create a system to register works on a digital platform. However, given the bureaucratic hurdles, it will take time for Brazil to create and approve such law.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The National Strategy on Cybersecurity addresses critical infrastructure, but only in a general manner. Although it recognises the need to protect critical infrastructure, this has become a highly sensitive and debated topic in Brazil, given that infrastructure is not necessarily managed by the state, but also by the private sector (eg, telecommunications, electricity).

Nevertheless, the National Strategy puts forth the need to carry out 'joint actions' between public and private entities, in addition to adequate investment to ensure the security of critical infrastructure.

Moreover, the Green Paper considers that cybersecurity relates to the protection of cyberspace, its information assets and its critical infrastructure. The concept of 'critical infrastructure' has a wider

connotation than 'critical internet resources.' Critical infrastructure relates to 'installations, services, goods and systems that if completely or partially interrupted or destroyed would cause a serious social, economic, political, environmental, or international impact, or implications to the security of state and society'. For example, it includes energy, transport, water, telecommunication, finance, information and other sectors. Critical internet resources are part of the critical infrastructure.

It is important to observe that, while there are guidelines regarding critical infrastructure, these provisions are extremely vague and no reference is made to specific mechanisms of these policies, public participation or human rights, accountability or transparency, or specific rights and obligations for the private sector.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Yes, the Brazilian Civil Rights Framework for the Internet, Law No. 12,965/2014 sets forth, in Chapter 2, the rights and guarantees of the internet user, and highlights in its article 7 that:

> *Art. 7. Internet access is essential to the exercise of citizenship, and the users are guaranteed the following rights:*
>
> *III - inviolability and confidentiality of their stored private communications, except by judicial order;*
>
> *VII - non-disclosure to third parties of user's personal data, including connection records, and access to Internet applications, except by express and informed consent of the user or in the cases established by law;*
>
> *VIII - clear and complete information on the collection, use, storage, treatment and protection of the user' personal data, which may only be used for purposes that:*
> *justify their collection.*

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

With the enactment of the Carolina Dieckmann Law, which amended the Brazilian Criminal Code, several cyberactivities were defined as crimes. With regard to organisations, the following cybercrimes are the most relevant:

- espionage;
- conspiracy;
- crimes against means of communication;
- tapping of communications;
- violation of the secrecy of correspondence;
- breach of confidence (disclosure of secrets);
- unauthorised access to computer systems;
- document falsification;
- threats against peace and security;
- fraud;
- extortion; and
- operations using illegal resources (money laundering).

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Although the Brazilian Congress initially considered the possibility of requiring, in certain circumstances, that data be necessarily stored in Brazil, the government ultimately opted not to do so, given the logistical challenges of the digital economy and its evolution.

In fact, this issue is already addressed in a different way in other provisions that regulate the matter, namely:

- the Brazilian Civil Rights Framework for the Internet;
- Supplementary Norm 14/IN01/DSIC/GSIPR;
- Decree No. 8.638/2016;
- Decree No. 8.135/2013; and
- Interministerial Ordinance 141/2014.

All of these reiterate the need for data related to Brazilian users to be submitted to national legislation.

There is a very large movement, however, of entities linked to the digital ecosystem, seeking a decentralised internet policy based on the argument that such an act has allowed the growth of cross-border data flows and the digital world sector, generating a virtuous cycle of economic and social development, enabling the digital inclusion and greater security of data in the cloud.

It is important to bear in mind that certain regulators (such as the Brazilian Central Bank) are discussing the cybersecurity policies, which may include the need to maintain the cloud (or a copy of the cloud) within the country, as a way to ensure security.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

In general, under Brazilian law, the obligations are the same for national and foreign organisations. There are no barriers in Brazil for foreign companies that want to do business in the country; the only requirement is that they comply with the country's laws and regulations.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As mentioned, Brazil does not have specific laws on cybersecurity and, as a consequence, the authorities do not recommend additional protection. Private organisations dealing with the digital sector recommend that data controllers adopt binding self-regulatory regimes. Self-regulation may include codes of ethics or good practices, privacy policies, binding corporate rules or other mechanisms that harmonise the processing of data by self-regulating entities that facilitate the exercise of the rights of data owners.

14 How does the government incentivise organisations to improve their cybersecurity?

There is no specific government incentive for organisations to improve their cybersecurity, given that Brazil does not yet have specific laws on the matter; however, some private organisations have been promoting a series of courses and lectures for corporations on how to update their cybersecurity measures, especially after the attacks of the WannaCry virus.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In Brazil, the standards and codes of practice that promote cybersecurity are not regulated or publicly available. It is up to each organisation to create and promote its own internal standards.

16 Are there generally recommended best practices and procedures for responding to breaches?

Brazil adopted the Green Paper on Cybersecurity, which establishes key aspects of cybersecurity in the country and constitutes a first attempt to set out the principles for a future cybersecurity policy (see question 8). Although the Green Paper does not establish clear recommendations regarding breach situations, it makes reference to international best practices, such as:

- security assessment and road map assessment of cyberthreats, current state of maturity, definition of goal to be achieved, gap analysis and roadmap implementation programme, aligned with best practices, such as ISO 27001;
- obtaining board support for redefinition of cybersecurity governance matters (for example, allocating cybersecurity outside the IT function);
- reviewing and updating security support policies, procedures and standards;
- implementing an information security management system (ISMS), creating a security operations centre, monitoring of known cases and response procedures in case of incidents;
- planning and deploying cybersecurity controls to evaluate the effectiveness of data loss and AMI prevention processes, enhancing the security of IT assets such as servers and firewalls, network components and databases; and
- testing business continuity plans and incident response procedures and encouraging regular network intrusion testing, entry points and applications, as well as weaknesses that can be exploited.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

There are currently no legal or policy incentives targeting the voluntary sharing of information relating to cyberthreats.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Brazil has shown a relative concern for cybersecurity and, although more cooperation is needed between the government and private sector, several actions have been carried out, as highlighted below:

- the creation of the Internet Steering Committee (CGI), with the participation of the various segments of society; although cybersecurity is not the central concern of the CGI;
- the enactment of Decree No. 3,505/2000, which established the Information Security Policy (PSI) to be implemented by the GSI/PR; however, there was no definition on how such policy should be implemented;
- the creation of the DSIC at the GSI/PR, in 2006, with the objective of coordinating normative and operational actions within the scope of the Federal Public Administration (APF) in PSI;
- the creation of the Information Security and Cryptography Community and the National Network for Information Security and Cryptography at the GSI in 2008 to take care of the aspects of science and technology promotion in all areas of cybersecurity, also provided in PSI; this initiative transcends the APF and was established in coordination with the MCTIC; and
- the publication of the National Defence Strategy, which stipulates cybersecurity as one of its priorities.

It is also noteworthy to mention the creation of the Special Commission on Information Security and Computational Systems, which is one of the Special Committees of the Brazilian Computer Society, the implementation of the Public Keys Infrastructure, the updating and creation of standardisation on the subject, training of human resources, development of cryptographic products and creation of technical groups to deal with the security of critical infrastructure.

In addition, there have been initiatives such as the specialisation of Federal Police agents to deal with cybercrimes, the strengthening of financial systems, which are the most frequent targets of these types of crime, and the actions of large companies, which are considered targets of cyberattacks.

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

A few companies in Brazil are offering a cybersecurity insurance policy against cyberattacks and cybercrime. In the financial sector, some banks offer customers their support in the event of a cybersecurity threat or if their information or bank funds are compromised. However, insurance policies for cybersecurity breaches are still not common in Brazil.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

At the macro level, the main regulatory authorities involved with cyber defence in Brazil are the GSI/PR, the Ministry of Defence and the Ministry of Justice. The latter is the competent authority for enforcement of cybersecurity rules via dedicated units and task forces within the Federal Prosecutors' Office and the Federal Police department.

In addition to these authorities, Brazil also has several regulatory agencies and departments that participate in cybersecurity policy development and regulation:

- the National Defence Council: an advisory body of the President of Brazil on matters related to national sovereignty and security;
- the GSI/PR: directly linked to the office of the President and responsible for matters involving cybersecurity (civil-related aspects), military affairs and cyber defence;
- the DSIC: a subordinated branch of the GSI/PR, responsible for guaranteeing the availability, integrity, confidentiality and authenticity of information and communication for the federal public administration;
- the Secretariat of Strategic Affairs (SAE) and the Chamber of Foreign Affairs and National Defence of the Council of the Government (CREDEN): advisory bodies to the office of the President, which are also in charge of, inter alia, cybersecurity issues. In 2010, the DSIC, SAE and CREDEN drafted the Green Paper on cybersecurity in Brazil; and
- the Ministry of Defence: the Ministry of Defence is responsible for the armed forces and, within such branch, the joint staff of the armed forces coordinates cyber response. The Brazilian army's Centre for Cyber Defence (CDCiber) is the first dedicated military cyber unit in Latin America. It is the coordinating agency for cyber defence in Brazil and operates directly with the Ministry of Defence, which, in turn, implements the directives of the GSI/PR. The CDCiber coordinates the activities of all the divisions of the armed forces dealing with technology and intelligence. It is also tasked with protecting the military and public networks from cyberattacks and, in the long term, it will be in charge of protecting the entire national informatics structure.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Brazilian law enables government authorities, including both law enforcement and administrative agencies, to require internet service providers to disclose customer data upon a search and seizure warrant or direct disclosure order. Upon a request from a competent government authority, a judge will consider issuing a warrant or order on the basis that it will be used to conduct an investigation regarding a violation of law or legal right. According to the Brazilian Civil Rights Framework for the Internet, the legal requirement to obtain search and seizure warrant or direct disclosure order should not limit law enforcement and administrative agencies from accessing personal data such as name, marital status, address and other qualification information when they are legally authorised to do so.

Under the Brazilian Communications Statute, law enforcement authorities can also seek an interception order for electronic communications, including data travelling to and from a cloud service provider, for instance. Interception orders are more closely regulated than search and seizure warrants or direct disclosure orders, requiring law enforcement to demonstrate to a judge that: (i) there is a reasonable indication that the investigated person participated in a crime; (ii) the evidence cannot possibly be obtained by any other available means; and (iii) the crime under investigation is a felony punishable by detention.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The Brazilian government has not been focused on expanding law enforcement capabilities to identify and respond to cybercrime in Brazil. The country is considering investing in upgrading military cyber capabilities, but such investments are likely focused on cyberwarfare, rather than addressing more realistic threats, such as cybercrime and law enforcement.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

According to the Carolina Dieckmann Law, which amended the Brazilian Criminal Code and defined certain cybercrimes, the invasion of computer equipment is punishable with imprisonment from three months to one year, in addition to a monetary fine.

Further, it is important to mention that, in addition to the criminal liability established under the Brazilian Criminal Code, as amended by the Carolina Dieckmann Law, the Brazilian Civil Code sets forth the civil liabilities that may arise from cybercrimes, such as the need to repair the damage resulting from said cybercrimes, in addition to any moral damage.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

There are no specific rules on reporting threats or breaches and, consequently, there are no reporting obligations.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Given that there is no national data protection authority in the country, it is fairly common for victims of data breaches to file a complaint against a data controller or data processor. Such controller or processor will then be subject to the penalties established in the Brazilian Civil Rights Framework for the Internet and in the Carolina Dieckmann Law in addition to civil liability.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The legislation does not set forth any rules and regulations that organisations must follow in order to protect data or information technology systems from cyberthreats. Best practices and international standards are usually adopted by entities to protect their systems and information.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

According to the Brazilian Civil Rights Framework for the Internet, internet application providers incorporated as a legal entity that provide internet services in an organised, professional and economic manner must maintain records of access to internet applications, under confidentiality, in a controlled and secure environment, for a period of six months.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

There are no laws or regulations requiring organisations to report data breaches to the authorities. However, data breaches that significantly affect users' assets or cause moral damage are usually reported to data owners.

29 What is the timeline for reporting to the authorities?

There is no clear rule obliging companies to inform either the public or the authorities about a data breach incident.

However, consumer protection bodies understand, based on the interpretation of the Brazilian Consumer Protection Code, that companies must present complete information to their consumers regarding their products and services in order to guarantee their rights to safety and to prevent damage or loss.

Based on the interpretation of the Brazilian Consumer Protection Code, companies have an obligation to disclose a breach if there is a reasonable chance that the breach could eventually impact or damage an individual's or company's rights or assets.

Nonetheless, a data breach event should only be disclosed: (i) to consumers; (ii) following the concrete and certain discovery of the event; and (iii) if the disclosure can assist in the prevention of loss and damage to consumer. If an organisation is able to address the threat or breach and prevent damage to consumers, there will be no obligation to report it.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no specific rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Hogan Lovells

Rafael Mendes Loureiro **rafael.loureiro@hoganlovells.com**

Rua Santa Luzia, 651
26º andar – Centro
20030-041 Rio de Janeiro
Brazil

Tel: +55 21 3550 6675
Fax: +55 21 3550 6671
www.hoganlovells.com

ALMEIDA ADVOGADOS

Leonardo A F Palhares **lpalhares@almeidalaw.com.br**

Av. Brig. Faria Lima, 1461
16º andar – Torre Sul
01452-002 São Paulo
Brazil

Tel: +55 11 2714 6900
Fax: +55 11 2714 6901
www.almeidalaw.com.br

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-912377-38-1