Chapter 4

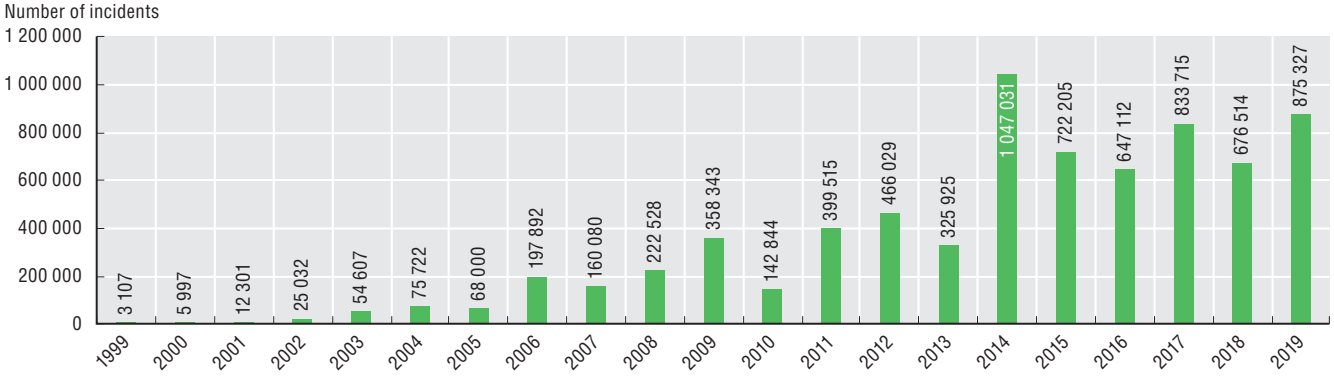
ENHANCING TRUST IN THE DIGITAL ECONOMY

Digital security policy in Brazil

Brazil is increasingly being targeted by digital security attacks. CERT.br, the private sector Brazilian National Computer Emergency Response Team (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) maintained by the executive branch of the Brazilian Internet Steering Committee (Núcleo de Informação e Coordenação, NIC.br), received over 875 000 incident notifications in 2019, 78% of which originated from Brazil (Figures 4.1 and 4.2). The Brazilian Government Computer Security Incident Response Team (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, CTIR) also reports an increasing number of incidents (Figure 4.3). A brief analysis of data from other sources confirms this situation. In 2018, EUROPOL found that Brazil is both a leading target and source of attacks in Latin America, and further noted that 54% of digital security attacks reported in Brazil originate from within the country (EUROPOL, 2018) According to the LexisNexis Threatmetrix (2019), Brazil is the sixth country from which attacks originate globally (in volume).

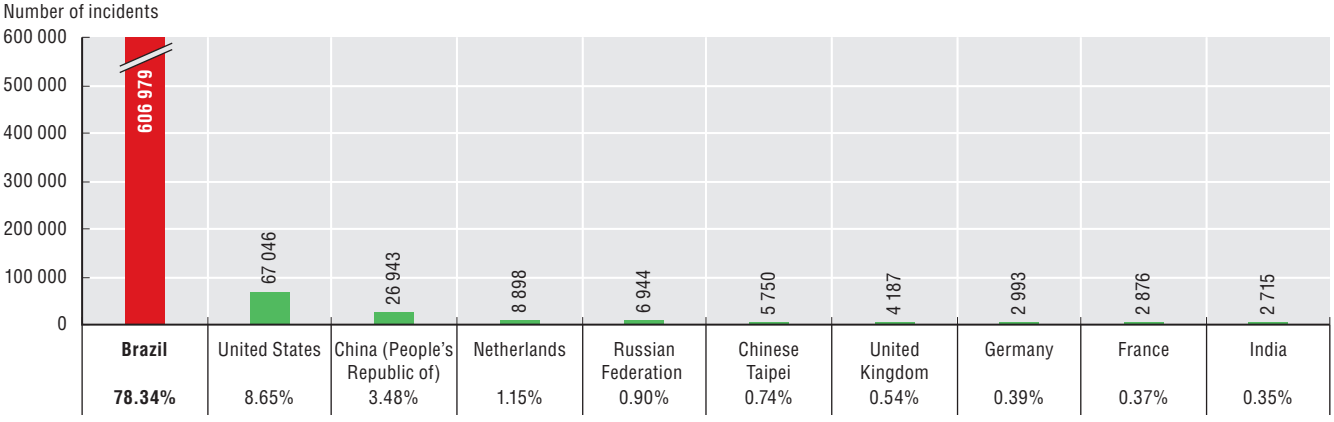
The 2018 Norton Survey showed that 89 million Brazilians have been a victim of cybercrime, with 70.4 million in the last year alone (Norton, 2018). A Ponemon Institute's 2017 survey of 36 Brazilian companies in 12 sectors showed that they suffered an average of USD 1.1 million in losses for each digital security attack (Ponemon, 2017). The Marsh JLT13 Cyber Review 2019 survey, conducted with 200 medium and large Brazilian companies, found that 55% of these companies are totally dependent on the use of technology in their activities and that 35% may suffer severe downtime in the event of a technology-related problem (Insurancecorp, 2019).

Figure 4.1. Total number of incidents reported to CERT.br per year, 1999-2019



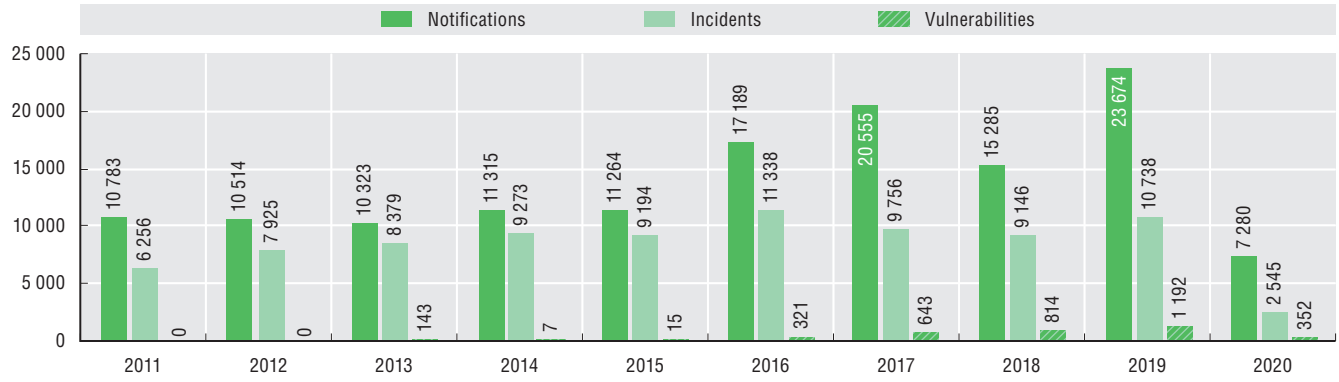
Source: Cert.br (2020), *Estatísticas dos Incidentes Reportados ao CERT.br*, *https://www.cert.br/stats/incidentes* (accessed on 8 March 2020).

Figure 4.2. Top 10 countries from which cyberattacks originate, 2019



Source: Cert.br (2020), *Estatísticas dos Incidentes Reportados ao CERT.br*, *https://www.cert.br/stats/incidentes* (accessed on 9 March 2020).

Figure 4.3. Number of notifications and incidents registered by the CTIR, 2011-20



Source: CTIR.br (2020), *Estatísticas Resultantes do Trabalho de Detecção, Triagem, Análise e Resposta a Incidentes Cibernéticos*, *https://emnumeros.ctir.gov.br* (accessed on 9 March 2020).

However, 44% of companies surveyed did not have contingency plans or budgets to combat incidents and did not foresee, in their budgets, a response to a possible crisis.Eighty per cent of respondents estimated that a digital security incident would have significant operational impact across the enterprise (Insurancecorp, 2019). According to a survey of ICT practices in the health sector by Cetic.br (2018), only 23% of public and private health establishments had a document defining an information security policy in 2018.

To address this issue, Brazil is in the process of developing a broad digital security framework, starting with the adoption of its first National Cybersecurity Strategy.

This section provides an overarching description of digital security policies in Brazil and discusses their strengths and limitations from the perspective of the 2015 OECD *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity* (hereafter "Security Risk Recommendation") (OECD, 2015) and the 2019 *Recommendation of the Council on Digital Security of Critical Activities* (OECD, 2019b). Unless specified otherwise, "digital security" refers to the management of economic and social risks resulting from breaches of availability, integrity and confidentiality of hardware, software, networks and data. This chapter does not cover policies directly related to criminal law enforcement (i.e. cybercrime), national defence or national security.

The emergence of digital security policy in Brazil

Digital security is not a new policy area in Brazil. Since 2000, digital security policy has been evolving along three main phases.

2000-12: The first steps of digital security policy in Brazil

This period was characterised by the establishment of the fundamental building blocks focusing on digital security in the public administration (Box 4.1). In 2000, the government established an information security policy for the federal public administration and created and Information Security Management Committee (Comitê Gestor da Segurança da Informação, CGSI) tasked with advising the Executive Secretariat of the National Defence Council about its implementation.[1] The Brazilian Public Key Infrastructure (PKI) was created in 2001 (ICP-Brasil). The Government Computer Emergency Response Team (CITR Gov) was established in 2004. As of 2006, the Institutional Security Cabinet of the Presidency of the Republic (Gabinete de Segurança Institucional/Presidência da República, GSI/PR) was designated as the primary agency for digital security matters and, over the years, adopted 3 general instructions and 22 supplementary standards (as of 2019). The Federal Court of Accounts (Tribunal de Contas da União, TCU) monitored their implementation by the federal public administration through surveys followed by recommendations. The 2010 GSI/PR Green Paper on Cybersecurity in Brazil (GSI/PR, 2010), which included recommendations for the establishment of a national cybersecurity policy, can be viewed as the first attempt to approach digital security policy from a holistic and strategic perspective.

Box 4.1. The first steps of digital security policy in Brazil

2000: Establishment of an information security policy for the public administration and creation of the Information Security Management Committee (CGSI), co-ordinated by the Institutional Security Cabinet of the Presidency of the Republic (GSI/PR).

2001: Creation of the Brazilian PKI (ICP-Brasil).[1]

2003: Creation of the Internet Steering Committee in Brazil (CGI.br).

2004: Creation of the Government Computer Network Incident Handling Team (CTIR.Gov).

2005: First Government Security Conference.

2006: Creation of the Department of Information and Communications Security (DSIC) within the GSI/PR; creation of a partnership led by the GSI/PR to facilitate the co-ordination of various public sector bodies, including public companies (e.g. Petrobras, Bank of Brazil, etc.), and adoption of a budget to facilitate information security training in the public administration.

2008: First survey of digital security in the public administration and recommendations by the Federal Court of Accounts (TCU). Adoption of the National Defence Strategy, which establishes the "cybersector" as one of the three strategic sectors considered essential for national defence.

2008-18: Publication by the GSI of 3 general instructions and 22 supplementary standards for digital security in the public administration, covering various topics such as risk management methodology, business continuity management, use of cryptography, biometrics, cloud computing technologies and procurement of secure software.

2009: Establishment of a "Cyber Security Technical Group" to propose guidelines and strategies for cybersecurity.

2010: Second TCU survey. Publication of the GSI/PR Green Paper on Cybersecurity in Brazil.

2011: Law on Access to Information, which establishes a principle of transparency of information within the public administration (entering into force in 2012).

2012: TCU publishes recommendations.

1. *https://www.iti.gov.br/icp-brasil/icp-brasil-18-anos*.

Source: GSI (2015), *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018*, *http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view*.

2012-17: Increased attention to and focus on national security aspects

As of 2012, key events created the conditions for increasing the country's operational digital security capacity while emphasising the national security dimension of digital security and raising awareness about privacy and civil liberties related to the Internet.

Between 2012 and 2016, the government significantly expanded its operational digital security capacity to protect several mega-events hosted in Brazil, such as the United Nations Conference on Sustainable Development (Rio+20 in 2012), World Youth Day (2013), the football Confederations Cup (2013) and the World Cup (2014), and the Olympics and Paralympics (2016). The Ministry of Defence played an important operational role, including by establishing a Cyber Monitoring Centre (Demetrio, 2012), and co-operating with several agencies as well as public and private incident response teams to successfully manage the situation (Hurel and Cruz Lobato, 2018).

In 2013, revelations of foreign espionage activities affecting Brazil led to the creation of a Parliamentary Committee of Inquiry on Espionage (CPI da Espionagem), which underlined weaknesses in the country's cybersecurity from a national security perspective. The committee's final report recommended the development of a National Cybersecurity Strategy, the adoption of measures to co-ordinate public

and private actions in this area, and the creation of a cybersecurity agency within the federal public administration to address the issue in an overarching and more effective manner.

During the same period, a considerable amount of public attention was dedicated to privacy and civil liberties issues related to the Internet, in particular through the public consultations for and adoption of the Internet Civil Legal Framework (Marco Civil da Internet), establishing principles, guarantees, rights and duties for the use of the Internet in Brazil (April 2014).[2]

However, in 2014, the results of an audit carried out by the TCU emphasised a relatively low level of implementation of existing digital security requirements by the federal public administration. According to the TCU, most of the federal public administration was not aware of its exposure to IT risks, the likelihood of their occurrence or their possible impact on the achievement of their objectives, and many public organisations, despite being aware of IT risks, did not keep them at acceptable levels or costs by treating them appropriately. The TCU stressed the low level of maturity with respect to the risk management process in the public administration. The TCU underlined that this situation increased the likelihood of IT not delivering results to business in the agreed time, cost and level of quality, consequently affecting the achievement of the business objectives of the entities. For example, only 25% of audited organisations had established guidelines for the management of IT risks, and only 8% were fully aligned with existing requirements. Only 13 out of 355 audited organisations had formally defined their acceptable levels of IT security risk (i.e. risk appetite).[3]

In this context, the GSI/PR developed the Strategy for Information and Communications Security and Cybersecurity in the Federal Public Administration, 2015-2018. After describing the background and context, this document set the strategic mission and vision, defined 7 strategic values, 11 guiding principles, and 10 strategic objectives with targets to be reached by 2018.

2018 to present: Digital security in the context of the digital transformation of Brazil

A new phase started in March 2018 with the publication of the Brazilian Digital Transformation Strategy (see Chapter 1), which includes a thematic axis focusing on "building trust and confidence in the digital environment", with the objective of "making the Internet a safe and reliable environment that enables services and business transactions while respecting citizens' rights". This thematic axis addresses "defence and security in the digital environment" and the "protection of rights and privacy".

According to the Digital Transformation Strategy, important progress in the area of "cyber defence" has been accomplished over the years, but Brazil still needs to improve its regulatory and institutional framework to match the challenge of digitalisation of the society and economy. The strategy claims that digital security should be regarded as a national priority and that a comprehensive "strategy for cybersecurity and defence" should be developed. The Digital Transformation Strategy points out that co-operation between the public and the private sectors is a crucial factor for the effectiveness of the actions envisaged in the future strategy and plans. It identifies several strategic actions, including the need to enhance digital security in the public administration; protect national critical infrastructure; raise the awareness of the population; enhance digital security skills in the public and private sectors; invest in research and development; develop metrics and information sharing models; as well as increase international co-operation.

In December 2018, the government published a decree establishing the National Information Security Policy (Política de Segurança da Informação, PNSI).[4] Developed by the GSI/PR, this decree sets out 16 principles and 7 objectives. It establishes the legal basis for the development of a national information security strategy and of national plans detailing its implementation, such as planning, organisation, use of resources and attribution of responsibilities. The PNSI also includes measures related to roles and responsibilities with respect to information security within the public administration (see below).

In 2019, the GSI/PR started a process to draft the National Cybersecurity Strategy called for in the PNSI. To inform the development of the strategy, it organised a consultation process inspired by the one carried out for the digital strategy. The process included a 7-month, 31 meeting-long consultation of 40 experts from government agencies, businesses and academia gathered into 3 working groups. Based on this input, the GSI/PR developed a draft National Strategy for Cybernetic Security – E-Ciber, released in September 2019 for a 20-day public consultation through the participative government platform.[5]

Forty-one participants, including 31 individuals and 10 organisations, posted a total of 166 comments on the platform. The final strategy was adopted on 5 February 2020.[6]

The strategy's vision is for Brazil "to become a country of excellence in cybersecurity". The objectives of the strategy are to: make Brazil more prosperous and reliable in the digital environment; increase Brazilian resilience to digital security threats; and strengthen Brazil's performance in cybersecurity in the international scene.

The strategy focuses on the following ten actions:

1. **Strengthening digital security risk management governance in public and private sector organisations**. This action includes holding fora, establishing minimum requirements in contracts with the public sector, promoting GSI/PR standards and norms, promoting international standards for security by design and default, nominating a chief information security officer, recommending digital security certification in accordance with international standards, etc.
2. **Establishing a centralised governance model at the national level**. A national digital security system will be created to promote co-ordination of actors beyond the federal administration, promote the joint analysis of the challenges faced in combating cybercrime, assist in the formulation of public policies, create a national cybersecurity council, create discussion groups in different sectors, etc.
3. **Promoting a collaborative, participatory, reliable and secure environment involving the public sector, private sector and society**. This action aims to encourage information sharing about incidents and vulnerabilities, carry out exercises, strengthen the national CERT (CTIR Gov), issue alerts and recommendations, encourage the use of cryptography, etc.
4. **Raising the level of government protection**, including by encouraging the use of secure communication devices, keeping information systems' security up to date, recommending the use of backup mechanisms, including digital security requirements in privatisation processes, etc.
5. **Raising the level of protection of national critical infrastructures** by promoting interactions between sectoral regulatory agencies, encouraging the adoption of enhanced digital security policies by operators of critical infrastructures, encouraging their participation in exercises and the notification of incidents to CTIR Gov.
6. **Enhancing the legal framework on digital security**, including by reviewing the existing framework, modifying the penal code to include cybercrimes, creating incentives to reduce the cybersecurity skills shortage, preparing a draft law on cybersecurity.
7. **Encouraging the design of innovative digital security solutions** in order to align academic projects with the economic demand. For example, include digital security in research programmes, encourage the creation of research and development centres on digital security, stimulate the creation of digital security start-ups, encourage the adoption of global standards to facilitate international interoperability, establish minimum requirements for 5G technology.
8. **Expanding Brazil's international co-operation on digital security**. This includes promoting discussions in international groups of which Brazil is a member, expanding relations in Latin America, promoting international events and exercises, expanding co-operation agreements, etc.
9. **Expanding digital security partnerships between the public sector, the private sector, academia and society**. Possible actions include partnerships to encourage private investments in digital security, meetings with leading digital security actors, etc.
10. **Raising the level of digital security maturity in society**. For example, carrying out public awareness initiatives; encouraging public and private sector organisations to carry out internal awareness-raising campaigns; integrating digital security in basic education; encouraging the creation of higher education courses; creating professional training courses; improving mechanisms for integration, collaboration and incentives between universities, institutes, research centres and the private sector, etc.

The strategy includes a diagnostic distinguishing between thematic and transformative axes:

- Thematic axes: national cybersecurity governance, incident management and strategic protection, i.e. protection of the government and critical infrastructures identified in the National Policy for the Security of Critical Infrastructures (telecommunications, energy, transport, water, finance).
- Transformative axis: normative dimension, research, development and innovation, international dimension and strategic partnerships, and education.

In July 2019, the government expressed its intention to adhere to the Convention on Cybercrime (Budapest Convention). In December 2019, the Committee of Ministers of the Council of Europe invited Brazil to join the Convention (Ministry of Foreign Affairs, 2019).

Governance

According to the PNSI, the GSI/PR is the primary government body in charge of digital security in Brazil, a role it has been playing since 2000. According to the 2020 National Cybersecurity Strategy, the GSI/PR will continue to co-ordinate digital security at the national level.

The GSI/PR is at the centre of digital security governance

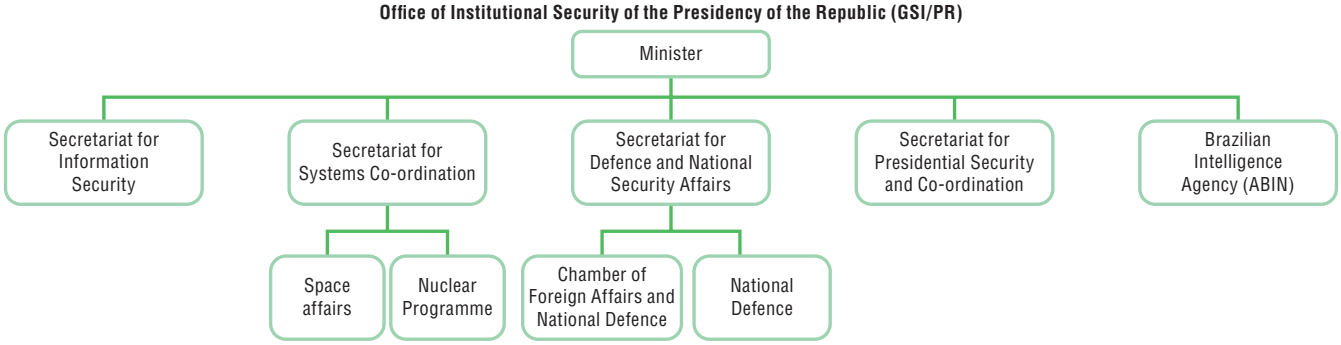
The GSI/PR's responsibility covers three areas:

- Information security standards and their implementation: establishing information security risk management standards for federal government agencies and entities; approving guidelines, strategies, norms and recommendations; and elaborating and implementing information security programmes aimed at raising awareness and training for the public administration and society.
- Public policy: following the doctrinal and technological evolution at national and international levels; elaborating and publishing the National Information Security Strategy, in collaboration with the Inter-ministerial Committee for Digital Transformation (see below); supporting the elaboration of national plans related to the National Information Security Strategy; establishing criteria for evaluating the execution of the PNSI; and proposing the publication of the normative acts necessary for its execution.
- Products: establishing minimum security requirements for the use of products incorporating information security features, which are binding for the federal administration; these requirements are not binding for the wider Brazilian market and only serve as a recommendation.

The GSI/PR is one of the organs of the Presidency of the Republic. It is led by a minister who reports directly to the President, as do all other Brazilian ministers. The Institutional Security Cabinet is responsible for analysing and monitoring issues related to potential risks of institutional stability; co-ordinating federal intelligence activities, and providing advice on military and security issues, in addition to other supporting functions for the President.[7] Until 2019, digital security matters were addressed by the GSI/PR's Department of Information and Communications Security (Departamento de Segurança da Informação e Comunicações, DSIC), within the Secretariat for Systems Coordination, which also addresses nuclear and space issues.

In 2019, the DSIC was elevated from a department to a secretariat. In contrast with a department, a secretariat reports directly to the minister, manages its own budget and has more resources. Figure 4.4 shows where the Secretariat for Information Security stands within the broader structure of the GSI/PR. This important evolution reflects the increased awareness of the importance of digital security in the government. With a budget of USD 433 000 (BRL 1.7 million), the secretariat comprised 30 staff in January 2020 (including 8 working for CTIR.gov, see below), which represents a 100% increase compared to the previous year.

Figure 4.4. Institutional governance for information security in Brazil



Note: This simplified overview of the Institutional Security Cabinet of the Presidency of the Republic structure does not include all of the entities of the office.

Source: OECD, based on *www.gsi.gov.br/sobre/estrutura*.

Most senior positions in the GSI/PR are held by high-ranking military officers.[8] The GSI/PR also hosts the Brazilian Intelligence Agency (Agência Brasileira de Inteligência, ABIN) and the Secretariat for Defence and National Security Affairs addresses issues related to the security of critical infrastructures, co-ordinates crisis management and carries out actions related to crisis prevention. However, many of the newly created positions created at the Secretariat for Information Security are filled by staff from other ministries, Anatel and public companies.

The Secretariat for Information Security is responsible for:[9]

- planning and supervising information security within the federal public administration, including incident management, data protection,[10] security accreditation and the handling of confidential information
- formulating and implementing the public administration's information security policies
- elaborating normative and methodological requirements related to information security in the federal public administration
- managing the government CSIRT (CTIR.Gov), co-ordinating and carrying out actions for the management of incidents, and co-ordinating the network of government agencies' and entities' CSIRTs
- proposing and participating in international treaties, agreements or acts related to information security
- acting as a central security accreditation body for the treatment of classified information
- supervising the security accreditation of individuals, companies, agencies and entities for the treatment of confidential information
- co-ordinating with the state, municipal and Federal District's governments; civil society; and organs and entities of the federal government, for the establishment of guidelines for information security policies for the public sector.

The secretariat includes three major branches:

1. The General Coordination of Security and Accreditation Centre (Coordenação-Geral do Núcleo de Segurança e Credenciamento, CGNSC),[11] which addresses issues related to information classification in the government.
2. The General Coordination of Information and Communications Security Management (Coordenação-Geral de Gestão da Segurança da Informação e Comunicações, CGSIC),[12] which elaborates proposals for information security guidelines, strategies, norms and recommendations; develops proposals for the National Information Security Plan; monitors its execution; plans and co-ordinates measures to guide information security implementation, such as for raising awareness and training; and monitors the doctrinal and technological evolution of activities related to information security at the national and international levels.
3. The General Coordination of Government Network Incident Handling Centre (CTIR.Gov), the government CSIRT[13] (described below).

The CGSI, gathering 21 ministries and government bodies covering a very large part of the federal public administration, provides advice to the GSI/PR. It meets at least twice a year and may establish up to four temporary sub-groups that cannot have more than seven members. The GSI/PR serves as the executive secretariat of the CGSI.[14] The further operationalisation of this committee and the creation of working groups is one of the secretariat's main objectives in 2020. For example, a working group within the Ministry of Economy is exploring the economic aspects of digital security in Brazil.

In November 2018, the Brazilian government published Decree 9.573 establishing the National Policy for the Security of National Critical Infrastructures. The policy aims to ensure the security and resilience of the country's critical infrastructure and the continuity of services. The policy's principles are: prevention and precaution; integration between government levels and branches, the private sector, and other segments of society; cost reductions benefiting the society resulting from investments in security; and safeguarding defence and national security. It also establishes the Integrated Critical Infrastructure Security Data System, the National Critical Infrastructure Security Strategy and the National Critical Infrastructure Security Plan. To address the complexity of digital security of critical infrastructures, a central organisation is expected to be established in order to co-ordinate all of the actors involved, public or private, as well as to call for accountability and action.

Each public sector entity is responsible for its digital security

The PNSI establishes a general principle whereby each organ and entity of the public administration is responsible for managing digital security in its own scope of action, including through the elaboration of its information security policy, designation of an internal information security manager, establishment of an information security committee, training, etc.[15]

The Ministry of Transparency and the Union Comptroller Office is tasked with auditing the implementation of the PNSI's activities under the responsibility of federal organisations and entities.

Central Bank of Brazil

In April 2018, the Central Bank of Brazil (BCB) published a resolution[16] to provide for the digital security policy and requirements on data processing and storage, including cloud computing. Such requirements shall be observed by financial institutions and other organisations authorised by BCB to operate in the financial market.

Financial institutions should implement and maintain a policy framework for digital security, respecting principles and guidelines for confidentiality, integrity, and availability of information systems and data.

The policy framework must include: the institution's digital security objectives; procedures and controls to reduce the institution's vulnerability; classification of data and information by relevance; definition of parameters to be used to assess incidents; mechanisms for dissemination of digital security culture in the institution; and information-sharing initiatives on relevant incidents.

BCB made other requirements, such as digital security policy disclosure to all employees; incident response and action plans; adoption of hard safety issues when contracting data-processing, storage and cloud-computing processes; and setting up monitoring and control mechanisms to ensure the implementation and effectiveness of the digital security policy.

BCB may rule out or restrict data-processing, storage and cloud-computing services contracts whenever it detects non-compliance with the provisions of the resolution or other BCB regulations. BCB may then establish a deadline for compliance.

BCB's technical digital security expertise relies in part on its CSIRT, which serves the financial sector and is in contact with large banks in the country.

ComDCiber (Ministry of Defence)

Issues related to national security and cyber defence, which are not in the scope of this section, are under the responsibility of the Cyber Defence Command (ComDCiber) and the Cyber Defence Centre (CDCIber), both specialised command bodies part of the Brazilian army. However, it is important to highlight the role played by ComDCiber, which has significantly more resources and staff than the GSI/PR, in particular at the technical level, and can take initiatives beyond the strict protection of the defence domain, such as the Cyber Guardian Exercise.

The second edition of the Cyber Guardian Exercise took place on 2-4 July 2019 at ComDCiber in Brasilia. About 200 members from 40 organisations participated in this simulated digital security exercise, including representatives from the financial, nuclear, electrical and telecommunications sectors. ComDCiber conducted the simulated training in a shared environment with other agencies. The initiative fostered collaborative action between government agencies, academia, private sector organisations, and the wider security and defence community.

The virtual simulation used the Cyber Operations Simulator (SIMOC) programme, which emulated computer systems used by participating agencies and companies. The constructive simulation used information technology, media, legal and senior management crisis offices, which provided solutions for security events which could impact those organisations. Discussions in crisis offices resulted in action at the decision-making and management level (crisis management) as well as at the technical level (incident response). Through SIMOC, attack situations against critical infrastructures were reproduced in electrical, telecommunications, financial and nuclear environments.

For example, the nuclear exercise comprised three groups working in co-operation: the crisis cabinet, the nuclear regulatory framework implementation team and digital systems test team. The digital systems test team used a simulator to test digital systems installed in nuclear plants, which serves as a cyber training tool. The simulator is part of a project by the National Atomic Energy Agency, developed by the Navy Technology Centre in São Paulo and the University of São Paulo. It is used by 17 institutions from 13 countries.

Participants acted collaboratively to prevent and resolve incidents involving information assets relevant to national defence. With this exercise, ComDCiber aims to integrate government, the private sector and academia in enhancing the protection of the national cyberspace.

Other actors of Brazil's digital security governance

The National Institute of Information Security

The National Institute of Information Security (Instituto Nacional de Tecnologia da Informação, ITI) maintains and implements the policies of the Brazilian public key infrastructure (ICP-Brasil), including the operation of Brazil's root Certification Authority. The ITI is also in charge of accrediting, discrediting, supervising and auditing the other participants in the trust chain.[17] The ITI is a federal agency linked to the Chief of Staff of the Presidency of the Republic (Casa Civil). It follows the operating rules established by the ICP-Brasil Steering Committee, whose members are nominated by the President of the Republic and include representatives of public authorities, civil society and academia.[18] The ICP-Brazil's Steering Committee, the ITI and accredited entities perform audits of the Brazilian PKI.[19] There are currently 17 first-level certification authorities in Brazil,[20] and 8 time-stamping service providers.[21]

Anatel, the telecommunications regulator

As Brazil's telecommunications regulator, Anatel also plays a role with respect to digital security in the country. Currently, there is limited co-operation and information sharing within the private sector on digital security, apart from trusted personal relationships between key individuals. Until now, security in the telecommunications sector is mainly self-regulated. Anatel started to focus on this issue through a public consultation launched at the end of 2018, which may result in the establishment of a committee of experts composed of all actors (e.g. operators, equipment providers, etc.) to share experiences, collectively discuss possible issues to be addressed, identify minimum requirements and best practices, etc. Anatel is responsible for certifying telecommunications equipment, including with respect to security requirements.

Anatel has adopted regulation with respect to protecting critical infrastructure and co-operates with the Ministry of Defence on exercises (cf. Cyber Guardian).

Computer emergency response teams and computer security incident response teams

There are over 40 computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) in Brazil, which can be grouped into 8 categories: 1) national responsibility; 2) international co-ordination; 3) critical infrastructures; 4) corporate; 5) providers; 6) academic; 7) government; 8) military. They co-operate in a broad ecosystem with a mix of institutional and personal trusted relationships. Two of them have a national responsibility and act as international contact points: CTIR.gov (mentioned above) for the federal government and CERT.br for the private sector.

CERT.br is maintained by NIC.br, the executive branch of the Brazilian Internet Steering Committee (CGI). It is responsible for:

- Handling voluntary computer security incident reports and activity related to Brazilian networks connected to the Internet. CERT.br collects incident reporting from any organisation and citizens. It provides a focal point for incident notification in the country, as well as co-ordination and support for organisations involved in incidents.
- Increasing security awareness. Together with NIC.br and CGI.br, CERT.br contributes to the portal internetsegura.br, which provides a wide array of educational material for various target audiences (children, teenagers, teachers, the elderly, etc.). The portal also provides links to many other awareness-raising and educational activities carried out by other entities in Brazil.[22]

- Carrying out network monitoring and trend analysis activities, including by maintaining an early warning project to identify new trends and correlating security events, as well as alerting Brazilian networks involved in malicious activities. CERT.br is an Anti-Phishing Working Group Research Partner, and a member of the Honeynet Project, with the HoneyTARG Chapter.
- Training and capacity building. CERT.br helps new CSIRTs to establish their activities in the country and delivers training for public and private sector information security professionals.[23]
- Participating in international CSIRTs fora. CERT.br leads LACNIC CSIRT initiatives that foster co-operation in the Latin American region. It also participates in the Forum of Incident Response and Security Teams (FIRST) as a member and through initiatives to improve global incident handling capabilities. CERT.br's general manager served as a member of the FIRST Board in 2012/13 and CERT.br staff currently take part in three FIRST working groups (CSIRT Services Framework, Membership Committee and Ethics SIG).

The Brazilian Government Response Team for Computer Security Incidents – CTIR.Gov, a division of the Institutional Security Cabinet of the Presidency of the Republic – addresses incidents on federal administration networks in Brazil. CTIR.Gov acts on the implementation of co-operation agreements with other federal incident handling teams, as well as with other national and international public and private CSIRTs, aiming at technical co-operation and mutual assistance on treating security incidents. CTIR.Gov provides:

- Reactive services initiated as soon as a notification arrives, followed by proper analysis of the incident and interactions with the originator. Patterns and tendencies revealed by continuous event observation serve as input to security recommendations issued to the concerned entities.
- Proactive services designed to prevent incidents or to reduce the impact of supervening events. These services are composed of information assets analysis and constitutive structures from different information technology environments in the federal administration, and provide a broad view of the available resources, their values, and associated risks.

CERT.br and CTIR have respectively a staff of ten and eight. CTIR doubled its staffing in 2019. Both CERTs work co-operatively with other trusted CERTs in Brazil and abroad. The National Education and Research Network has its own Security Incident Response Centre (CAIS).[24] With over 20 years of experience, CAIS was one of the first security incident response groups to operate nationally in the detection, resolution and prevention of incidents on the academic network.

Key findings and challenges

Brazil reached a turning point in 2018-19 with the adoption of its Digital Transformation Strategy and National Information Security Policy, as well as the preparation of its National Cybersecurity Strategy. A review of existing policy documents combined with elements collected during interviews reveal several key findings.

Brazil's primary digital security focus on national security is evolving to include economic and social aspects

The focus of digital security policies in Brazil has evolved from a technical dimension in 2000-11, to a national security dimension in 2012-18, driven in part by the organisation of mega-events and the revelations by Edward Snowden about cyberespionage by the United States. The overarching mission of the Strategy for Information and Communications Security and Cyber Security in the Federal Public Administration 2015-2018, which was to "ensure and defend the interests of the state and society for the preservation of national sovereignty", illustrates this evolution.

The 2018 Digital Transformation Strategy, which aims to "embrace digital transformation as an opportunity for the entire nation to take a leap forward", is the first Brazilian policy document to address digital security as part of a broad prosperity agenda and not solely from the national security perspective. Digital security is presented as part of an enabling thematic axis on "trust and confidence" and the recommended strategic actions primarily focus on measures that can support the digital transformation in Brazil from an economic and social perspective. The thematic axis also addresses the "protection of rights and privacy", echoing the trust policy dimension of the OECD Going Digital Integrated Policy Framework (OECD, 2019a). The Digital Transformation Strategy can therefore be viewed as a first step towards broadening the scope of Brazilian digital security policies to economic and social prosperity.

Nevertheless, the PNSI, published later in 2018, includes national sovereignty and human rights as the first and second principles, but does not consider economic and social prosperity as an objective of digital security.

A comparison of these two documents shows that this evolution is progressive. It is likely that each document reflects the perspective of the bodies that have developed it, namely the Ministry of Science, Technology, Innovations and Communications for the Digital Transformation Strategy, and the GSI/PR for the PNSI. The content of the National Cybersecurity Strategy and the consultation process carried out by the GSI/PR for its development demonstrate that Brazil is heading towards a more holistic approach to digital security, placing more emphasis on the economic and social dimension.

Brazil is at an early stage of promoting digital security across society

The general perception among experts in Brazil is that the government is starting to elevate digital security as a priority for the economy and society and that, apart from very large firms and some specific public sector bodies, most public and private stakeholders are not giving enough attention and resources to this issue.

In addition, over time, policy documents in Brazil have been using different concepts and terms to cover different aspects of digital security, including information security, cybersecurity, cyber defence, data protection, as well as related terms such as information assets, critical infrastructure, cyberspace, etc. Where available, definitions have not always been consistent over time, which can be explained by many factors, including that the approaches themselves have been evolving. However, definitions are sometimes confusing. For example, the PNSI defines information security as including cybersecurity, cyber defence, physical security and protection of organisational data; as well as actions to ensure the availability, integrity, confidentiality and authenticity of information (Article 2). This suggests that actions to ensure availability, integrity, confidentiality and authenticity are different from cybersecurity and cyber defence, which themselves are not defined.[25]

In addition, interviews carried out for this Review have shown that, beyond a circle of "information security" experts, there is widespread confusion between digital security and "data protection" (i.e. privacy protection). Many actors do not distinguish between the two areas and do not understand their relationship, including how they can strengthen or undermine each other. This situation is likely to evolve following the full implementation of the data protection law in Brazil.

This shows that the conceptual basis for approaching digital security policy in Brazil has considerably evolved over the last decade and is entering a new phase with the adoption of the National Cybersecurity Strategy.

At this juncture, a key challenge for Brazil is to recognise that, although in theory, "cybersecurity" (or "information security", depending on terminological preferences) can be viewed as a monolithic challenge, it is in reality a multidimensional policy area. In practice, it can cover at least four dimensions: 1) national security; 2) economic and social prosperity; 3) technology; and 4) law enforcement (Figure 4.5).

Actors and communities addressing each dimension have different cultures, backgrounds and objectives and can sometimes converge, overlap or compete, depending on the context and precise issue. Cryptography policy is a typical example of competing objectives, with businesses, organisations and consumers promoting the unregulated use of cryptography to support trust and facilitate e-commerce, digital governments and innovation on line, while law enforcement and intelligence call for more regulation to facilitate access to encrypted data in order to combat criminals and terrorists. Digital security of critical activities and infrastructure is another example where tensions can appear between economic and social prosperity and national security objectives, depending on the situation.

Ideally, terminology should reflect distinctions between the dimensions of digital security. For example, to reduce confusion and potential misunderstandings, the 2015 Security Risk Recommendation uses the term "digital" instead of the prefix "cyber". The term "digital" is consistent with expressions that characterise the economic and social perspective of ICT policy, as in "digital economy", "digital transformation", "digitalisation", etc. It is also common in business environments. In contrast, the prefix "cyber" is often used in relation to law enforcement (cybercrime) as well as national/international

security (cyber warfare, cyber defence, cyber espionage, cyber command, etc.). The Security Risk Recommendation also uses the expression "digital environment" instead of "cyberspace", which is common in military doctrines as a domain of operations in addition to air, sea and land.

Figure 4.5. The four dimensions of "cybersecurity"

The main priority for Brazil is to raise awareness and promote the adoption of good digital security practices by all stakeholders

Brazil has made an important step forward with the acknowledgement of digital security as an enabler of economic prosperity in its Digital Transformation Strategy. In line with the first principle of the OECD Security Risk Recommendation (Box 4.2), the next step is to raise the awareness of businesses, public sector organisations and individuals about the importance of digital security to foster trust and support digital transformation; and to encourage them to adopt good digital security practices, enhance their digital security skills and empower them to manage digital security risk.

To do so, it is important to understand that, in organisations, digital security is primarily an economic and social challenge rather than only a technical issue and why digital security risk management should be a business, as opposed to a technical, process.

First, digital security incidents due to insufficient digital security risk management will potentially harm an organisation's economic and social objectives, operations, competitiveness, and reputation, as well as its customers' and users' trust and, potentially, privacy. Therefore, ensuring effective digital security risk management should be a business (as opposed to a technical) leadership's responsibility. To the extent that it can threaten the organisation as a whole, it should be owned by the highest level of leadership and followed at board level in an organisation-wide manner.

Second, although digital security measures aim to protect economic and social activities, they can also inhibit them by increasing costs, reducing performance and the openness and dynamic nature of the digital environment, which are essential to realising the full benefits of digital transformation. Business (as opposed to technical) decision makers should own digital security risk related to their business activities rather than delegate it to technical security experts. While technical security experts understand the technical aspects of digital security risk, they cannot assess the possible business impact of security measures on every line of their organisation's business and support activities. They should, however, support business decision makers as best they can to ensure their informed risk management decisions.

For example, one option to eliminate a virus from a system might be to shut down that system, clean it and turn it back on. While this may sound like a technical decision, it is in fact a business decision, because there might be negative business consequences in interrupting that system, such as stopping a production line or preventing customers from placing orders, etc. The decision maker owning the responsibility for shutting down the system should also own the responsibility for the possible negative consequences of doing it. S/he relies, however, on technical experts to most appropriately assess the technical risk and take the best-informed risk management decision.

Box 4.2. Principles of the OECD *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

The 2015 Security Risk Recommendation includes eight principles that describe how to approach digital security without inhibiting the economic and social benefits from digital technologies. It is based on the understanding that the overarching objective of digital security is to increase the likelihood of success of an economic and social activity rather than to create a state of security, i.e. entirely eliminating the risk. Security is an enabler for prosperity, not an end in itself, which is why it should be a business-driven rather than a technology-driven process. Decision makers in organisations should manage the economic opportunities and security risks from using digital technologies in tandem. To take the most appropriate risk management decisions from a business perspective, leaders and decision makers should own digital security risk management rather than delegating it to technical digital security experts. They should, however, work with them to understand the threats and vulnerabilities as well as the options to reduce the risk.

General principles

1. **Awareness, skills and empowerment**. All stakeholders should understand digital security risk and how to manage it.
2. **Responsibility**. All stakeholders should take responsibility for the management of digital security risk.
3. **Human rights and fundamental values**. All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.
4. **Co-operation**. All stakeholders should co-operate, including across borders.

Operational principles

5. **Risk assessment and treatment cycle**. Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.
6. **Security measures**. Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.
7. **Innovation**. Leaders and decision makers should ensure that innovation is considered.
8. **Preparedness and continuity**. Leaders and decision makers should ensure that a preparedness and continuity plan is adopted.

Source: OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, *https://doi.org/10.1787/9789264245471-en*.

Last, although they aim to create trust, digital security measures can also undermine confidence by raising suspicion related to human rights and fundamental values, in particular privacy. Digital security and privacy protection can reinforce or undermine each other depending on how they are managed. It is therefore essential that digital security and privacy protection be approached in a coherent manner, including from a legal and ethical perspective.

As a result, leaders and decision makers in organisations need to adopt a business-driven (as opposed to a technology-driven) approach that leads to the most appropriate selection and management of digital security measures, in light of the economic and social activities at stake as well as the need for trust and confidence. They should understand and be responsible for digital security risk and work in co-operation with technical security experts to take digital security decisions.

This means that public policies aiming at encouraging businesses and public sector organisations to step up their digital security should target leaders and decision makers as well as ICT professionals and experts, instead of only the latter.

Brazilian policies promote a risk management approach to digital security (e.g. the PNSI, Article 3-VIII) and encourage the implementation of information security risk management standards in the public administration. However, they primarily focus on the protection of information systems, networks and data rather than on the economic and social activities that rely on them. In other words, they

approach digital security as a technical rather than as an economic and social matter. Most countries have followed the same steps, at different paces, and many are struggling to shift from a technical to an economic and social digital security approach. The development of the National Cybersecurity Strategy provides an opportunity for Brazil to make progress in this area.

Brazil should establish more robust and better resourced governance for digital security

The Digital Transformation Strategy, the PNSI and the National Cybersecurity Strategy cover many key aspects of an up-to-date digital security policy framework. These include standards and norms for digital security in the public administration, awareness raising, education and skills development, research and innovation, the protection of critical infrastructure, etc. However, most of them are addressed at a very high level, and implementation measures have not yet been defined. Implementation plans are expected to fill the gap. The definition and implementation of many of these implementation plans will require collaboration across several federal government agencies, regional and local bodies, as well as non-governmental stakeholders.

The Digital Transformation Strategy and the PNSI also mention human rights, fundamental values and privacy, as well as multi-stakeholder collaboration. These areas are particularly important, and can be challenging for Brazil.

Since 2006, digital security governance has been co-ordinated by the GSI/PR, an entity that has developed a certain degree of expertise in this area but which is characterised by its national security/military culture. During this period, some have criticised

> *the excessive securitisation and accentuated militarisation of cybersecurity; the exclusion of non-state actors from the definition of terms relevant to the political agenda; the increasing preference for solutions which seek to block applications and remove content; and the continuous difficulty of co-ordinating action at the level of the federal public administration (Hurel and Cruz Lobato, 2018).*

The GSI/PR's Secretariat for Information Security reports to the same minister as the Brazilian Intelligence Agency.

A key challenge for the GSI/PR will be to build trust with other government agencies at different levels (e.g. federal, regional, local, etc.), businesses (including foreign companies) and other non-governmental stakeholders in order to establish a long-standing partnership to promote digital security for prosperity in Brazil.

The Department for Information Security at the GSI/PR has significantly evolved over time. It has more and diversified staff, is better recognised at the political level, in particular following its elevation to a secretariat. It has also adopted a more open culture, illustrated by the working groups organised to develop the first draft of the National Cybersecurity Strategy through the public consultation held to gather input for the document. Many stakeholders have praised this evolution, noting, however, that the consultation process could have benefited from more publicity in order to involve more stakeholders. This is definitely a step in the right direction.

A key challenge is that the GSI/PR does not have competence to regulate the private sector. Instead of regulating, it publishes standards, makes their implementation mandatory by the federal administration, and encourages their voluntary adoption by other stakeholders. This includes various means, such as requiring compliance with these standards for public procurement. The general Brazilian governance approach with respect to digital security regulation is decentralised: as illustrated by the Central Bank example above, sectoral regulators are competent to regulate digital security in their area. As there is no centralised digital security agency in Brazil, sectoral regulators are invited to build upon the standards and good practices provided by the GSI/PR. This approach is closer to that of Sweden and the United Kingdom rather than France.

There is no universal model for digital security policy governance. Centralised and decentralised approaches have different pros and cons. For example, the decentralised approach enables sectoral regulation carried out by sectoral regulators to be better tailored to the sector's specificities. However, it raises the issue of each sectoral regulator aggregating a sufficient critical mass of expertise in order to be able to issue balanced and effective regulation, as well as to supervise its implementation. It also

creates a situation where regulated entities may be reluctant to share digital security risk-related information with a government body tasked with regulating their activities more generally.

More generally, most governments have been struggling to set the most appropriate governance framework for cybersecurity, finding it difficult to strike the right balance between economic and social, national security, criminal law enforcement, and technical aspects. A good practice is to recognise the need for a whole-of-government approach co-ordinated at a high level of government with a view to balance the potentially competing objectives of each dimension. However, again, there is no one-size-fits-all model for how to implement this good practice. Governance frameworks and co-ordination mechanisms vary considerably, reflecting countries' history, style of government and maturity in this area.

For example, Australia, Japan and the United Kingdom have assigned policy co-ordination to the Prime Minister through the Cabinet Office. France established a national co-ordination agency within a pre-existing co-ordination body under the Prime Minister (ANSSI), and Israel created a national agency reporting directly to the Prime Minister (INCD); the United States established a Cybersecurity and Infrastructure Security Agency (CISA) in its Department of Homeland Security; Canada, Germany and the Netherlands have placed the main responsibility for digital security under an existing ministry (respectively Public Safety, Interior, and Security and Justice). In all of these cases, there are also different arrangements with respect to which agency or agencies) is/are responsible for policy and operational matters. For example, in the United Kingdom, the Department for Culture, Media and Sports is responsible for economic and social policy while the National Cyber Security Centre is responsible for operational aspects. In contrast, both aspects are addressed in a centralised agency in France. In Germany, the Ministry of Interior has the lead for public policy making but the Federal Office for Information Security has the technical competence and responsibility. Lastly, multi-stakeholder co-ordination is also concretely carried out differently across countries. In many countries, it took a couple of new versions of the initial cybersecurity strategy to set a relatively stable governance model.

Conclusions and recommendations

The new National Cybersecurity Strategy is clearly a step in the right direction. However, as the economic and social initiatives to promote digital security need to be scaled up to match the government's expectations reflected in the Digital Transformation Strategy, several issues arise.

Implementation of the strategy

The adoption of the strategy is an excellent first step, but it now needs to be translated into specific action items. In doing so, it is important to recognise that Brazil is at an early stage of development in this area and needs to take a step-by-step approach, distinguishing short-, medium- and long-term priorities.

Policy recommendations: To develop the agenda for the implementation of the National Cybersecurity Strategy, the government should build upon and expand the multi-stakeholder efforts undertaken to develop the strategy. For example, it could create a broad community of digital security leaders in the public and private sectors, academia, and civil society and hold annual meetings to develop the implementation plan and assess progress in its implementation over time. Such meetings would also provide an opportunity for the broader multi-stakeholder Brazilian digital security community to emerge, gather and dialogue, including through a national conference. It could aim at eventually becoming the main cybersecurity event in Brazil and Latin America, echoing, for example, the Israeli Cyber Week (Tel Aviv), the Dutch ONE Conference (The Hague), the French International Cybersecurity Forum (Lille) or the Singapore International Cyber Week.

Being at an early stage, awareness raising and education are particularly critical. In practice, Brazil should identify gaps in awareness and knowledge about digital security in society among businesses, governments and individuals. On this basis, it should develop an action plan to strengthen digital security training and education programmes at all levels (primary, secondary, higher education and vocational training), identify existing digital security experts who can teach and train the trainers, perhaps through a national register of digital security trainers; and encourage students to pursue carriers in digital security. The recently published National Cybersecurity Strategy points in this direction.

It will also be important for Brazil to periodically assess the effectiveness of its strategy, as experience from OECD countries demonstrate. Brazil would benefit from developing tools to evaluate the implementation of the strategy, assess progress and needs to revise the strategy.

Resources

To implement its National Cybersecurity Strategy and match the ambition of its Digital Transformation Strategy, Brazil will need to make a significant effort to allocate more resources to digital security. The government has doubled digital security resources at the GSI.PR in a single year. However, with only 30 staff addressing digital security, including 8 for incident response, more financial and human resources efforts will be needed over several years.

Policy recommendations: The government should consider allocating significantly more resources for digital security so as to ensure appropriate implementation of the National Cybersecurity Strategy. For example, each area covered by the implementation plan could be assigned a clear budget for a well-defined period in order to reach clear and measurable milestones. Resources should not be allocated only to technology, but also cover all other aspects. In addition, the government could work with the private sector and academia to better understand the cost of malicious digital security activities to the economy.

Co-ordination and decentralised responsibilities

According to the National Cybersecurity Strategy, the GSI/PR will continue to co-ordinate digital security at the national level. Is the GSI/PR the most appropriate institution to promote digital security risk management to the private sector, to encourage digital security innovation, to stimulate digital security education and training, etc.?

Policy recommendations: It seems that, to achieve the best results, Brazil should follow a co-ordinated decentralised approach, where different ministries and agencies would have the lead in their area of competence, leveraging their expertise and networks, with the GSI/PR having a co-ordination role. However, there is currently limited digital security expertise that can be leveraged outside of the GSI/PR to develop more tailored initiatives led by other ministries and agencies. One option would be for Brazil to train digital security policy experts to progressively enable each ministry and agency to start developing and implementing action plans in their respective areas.

Multi-stakeholder dialogue

Will the military and national security culture inherent to the GSI/PR be appropriate in the long run to promote digital security as an economic and social challenge and to facilitate trusted relationships with all economic and social actors? Digital security is an economic and social policy priority that requires the participation of all stakeholders. Sustainable trust between the co-ordinating government agency, other parts of the government and non-governmental stakeholders is essential. It aims to: establish a constructive public-public and public-private dialogue with a large number of stakeholders; ensure that policy measures are appropriately balanced and do not create unnecessary obstacles to the use of digital technologies for innovation and growth; create the conditions to share risk-related information with businesses; facilitate the promotion and dissemination of good practice throughout society by civil society; and ensure the protection of privacy and other human rights. The organisation and simplification of digital security governance in Brazil should aim at enabling digital security to grow while engaging all stakeholders in a sustainable manner.

Policy recommendations: One option might be to build on the lessons learnt from the Brazilian Internet governance model (CGI) to create a multi-stakeholder setting to facilitate debates and co-ordination. In addition, the government should encourage the establishment of a digital security governance structure for the private sector. It should also facilitate the creation of groups bringing together chief information security officers and other security professionals throughout Brazil, without necessarily taking part in their discussions. Such groups would then become discussion partners for the government, thereby facilitating the exchange of information on digital security threats, vulnerabilities, incidents, and risk management measures in both the public and private sectors.

Box 4.3. Policy recommendations for digital security policy in Brazil

In order to enhance digital security, Brazil should take action in the following areas:

- **Implementation of the National Cybersecurity Strategy**: Build upon and expand the multi-stakeholder efforts undertaken to develop the National Cybersecurity Strategy in order to build the agenda for its implementation.
- **Awareness raising and education**: Identify gaps in awareness, knowledge and digital security among businesses, governments and individuals, and develop an action plan to strengthen digital security training and education at all levels.
- **Resources**: Allocate significantly more resources for digital security in order to ensure appropriate implementation of the National Cybersecurity Strategy, covering all aspects rather than only technology.
- **Governance**: Follow a co-ordinated decentralised approach, where different ministries and agencies would have the lead in their area of competence, with the GSI/PR having a co-ordination role; and train digital security policy experts to overcome the current lack of experts in each ministry and agency.
- **Multi-stakeholder dialogue**: Build on the lessons learnt from the Brazilian Internet governance model to create a multi-stakeholder setting facilitating debates and co-ordination; encourage the establishment of a digital security governance structure for the private sector; facilitate the creation of groups bringing together chief information security officers and other security professionals.

Developing trust through greater privacy

Brazil passed the General Data Protection Law (Lei Geral de Proteção de Dados, LGPD) on 14 August 2018 (Law 13.709). It forms the main part of Brazil's legal framework for governing the collection, storage and use of personal data. Initially developed by the Ministry of Justice, the LGPD underwent extensive public consultation with a large number of stakeholders from civil society, academia and the business community over a seven-year period. Consultations were also held within government, involving different ministries and public organisations. Preliminary hearings and national consultations on the draft law were also subject to discussions in both the Senate and the Chamber of Deputies.

The LGPD was originally to become effective in February 2020. However, as a result of the enactment of the Executive Order MPV 869 of 27 December 2018, which was enacted into law as Law 18.583 of 8 July 2019, the term was extended to August 2020. On 3 April 2020, the Brazilian Senate approved a bill of law (PL 1179/2020) with several emergency measures to deal with the COVID-19 pandemic. The bill includes a specific rule that postpones the LGPD's entry into force until January 2021.

The next section examines in some detail the legal framework and how organisations (in both public and private sectors) are preparing for its implementation. In addition, it will review how the new law and existing data governance frameworks provide for the transfer of data to other countries.

Overview of Brazil's General Data Protection Law

Before the publication of the LGPD, Brazil's approach to privacy and data protection was either sector-specific or too broad. Privacy and data protection were regulated by different laws covering, for example, financial services, healthcare, telecommunications and consumer protection. At the same time, the Brazilian Constitution provides for a general level of protection. Enforcement was left to the discretionary powers of the national and local regulatory authorities and agencies.

The LGPD was drafted to create the conditions for greater consistency and uniformity in privacy and data protection legislation and the way individuals could exercise their privacy rights across the Brazilian territory. The law is largely based on the EU General Data Protection Regulation (GDPR) and the 1980 *OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy*

and Transborder Flows of Personal Data (hereafter "OECD Privacy Guidelines"; amended on 11 July 2013) (OECD, 2013), as well as in Convention 108 of the Council of Europe.

The LGPD takes a broad view of what data qualify as personal data, even more expansive than the GDPR and the OECD Privacy Guidelines. For example, the Brazilian law has a specific provision (Article 12, Paragraph 2) by which anonymous data may fall within the scope of the law if they are used to evaluate certain aspects of a natural person and create behavioural profiles (e.g. price discrimination methodologies).

Notably, the LGPD covers the collection and processing of personal data and information for both the public and private sectors. The processing of personal data has to be conducted in good faith and in accordance with the principles listed below, which are consistent with the principles of the OECD Privacy Guidelines:

- purpose specification
- suitability
- necessity
- free access
- data quality
- transparency
- secure safeguards
- prevention
- non-discrimination
- accountability.

Furthermore, the LGPD is concerned not only with an extensive qualification of consent, but also with empowering data subjects with meaningful control and choice regarding their personal information. The LGPD lists nine fundamental rights that data subjects have, which are essentially the same rights the GDPR mentions. Another similarity with the GDPR is that the LGPD applies to any business or organisation that processes the personal data of individuals in Brazil, regardless of where that business or organisation itself might be geographically located.

While the GDPR has six legal basis for processing personal data, Article 7 of the Brazilian LGPD lists ten (Box 4.4). There are, therefore, more legal authorisations for data processing, making it possible to interpret, at least theoretically, the LGPD as more flexible and less restrictive than the GDPR in relation to the processing of personal data.

Box 4.4. Legal basis of Brazil's General Data Protection Law

1. With the consent of the data subject.
2. To comply with a legal or regulatory obligation of the controller.
3. To implement public policies provided in laws or regulations or based on contracts or agreements.
4. To conduct studies by public research entities that ensure whenever possible the anonymisation of personal data.
5. To execute a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject.
6. To exercise rights in legal, judicial, administrative or arbitration procedures.
7. To protect the life and physical safety of the data subject or a third party.
8. To protect health.
9. To fulfil the legitimate interest of the controller or a third party.
10. To protect credit (referring to a credit score).

Data portability

One of the new data subject rights in the GDPR is the right to portability, which has also been imported into the Brazilian law. Such a right mandates the controller to transfer, at the request of the data subject, their personal data to other controllers. In the Brazilian law, this right is not limited to data provided based on the data subject's consent, making it different from the GDPR.

The right to data portability is not a new right under the legal framework of Brazil. Portability is also present in other instances in Brazilian law. In the telecommunication services sector, for example, this right is currently regulated under Resolution 460/07,[26] better known as the General Portability Regulation of Anatel. Under this resolution, users of telecommunications services have the right to request the portability of their contracts (and, therefore, the related personal data) in relation to land and mobile telephone lines from telecommunication service providers of collective interest.

The LGPD imported the right to data portability from Article 20 of the GDPR, defining that the data subject may exercise this right through an express request to the provider of goods or services, according to further regulation to be provided by the ANPD. Nevertheless, there are major differences. One of them is that the GDPR establishes a major threshold that requires the specific consent of the data subject or that the request to data portability be based on an existing contractual relation in order to be able to request this right from a data controller, and as long as this is technically feasible. Further, the GDPR establishes an exemption to exercise this right when the processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.

National Data Protection Authority

Provisional Measure 869[27] of 27 December 2018 created rules for co-ordination within the government, mandating the creation of a permanent communication forum for technical co-operation between governmental bodies responsible for sectoral regulation. According to the provisional measure, the National Data Protection Authority (Autoridade Nacional de Proteção de Dados, ANPD) is considered the central governmental body of the public administration responsible for interpreting the LGPD and in enforcing the sanctions created by the law.

Provisional Measure 869 was voted into law by the Senate and by the House of Representatives and became Law 13.853 of 8 July 2019. It creates the ANPD in charge of the oversight of the LGPD. The ANPD is an entity of the federal public administration created as part of the Presidency of the Republic, with "technical and decision-making autonomy" guaranteed by the law (Article 55-B). It is composed of six main entities:

a) Board of Directors
b) National Council for the Protection of Personal Data and Privacy (Conselho Nacional de Proteção de Dados e Privacidade, CNPDP)
c) Internal Affairs
d) Ombudsman
e) legal advisory body
f) administrative specialised units.

The Board of Directors will be composed of five directors, which are appointed by the President after approval by the federal Senate. Until the LGPD's entry into force, technical and administrative support will be provided by the Executive Office of of the Presidency of the Republic (Casa Civil).

The CNPDP will be composed of the representatives of 23 organisations and bodies from the public, private and academic sectors. Its main activities will include proposing strategic guidelines and providing inputs for the preparation of the National Policy for the Protection of Personal Data and Privacy and for the activities of the ANPD, and preparing annual reports to assess the implementation of the actions of the national policies for the protection of privacy and personal data in Brazil.

Article 55-J grants the ANPD a wide range of responsibilities, from handling complaints, enforcing the law and applying sanctions to producing educational materials and guidance. The ANPD's main competencies and regulatory powers under the LGPD are listed in Box 4.5.

It is worth pointing out that the executive branch has vetoed certain sections of the LGPD. Specifically, Law 13.853 of 8 July 2019 that creates the ANPD contains a total of nine vetoes, most of them related to the administrative sanctions dealing with the processing of personal information to be imposed by the ANPD.

In addition to the above competencies, Articles 55-J, VI, and 58-B, V of the LGPD (as worded by Law 13.853, from 8 July 2019), attribute responsibility to the ANPD and its NDPPC for disseminating knowledge regarding policies and norms on personal data protection and privacy to society.

Other entities have traditionally contributed to education and awareness on privacy and data protection. Notably the National Consumer Defence System (Sistema Nacional de Defesa do Consumidor, SNDC), which congregates entities such as the consumer protection and defence programmes (Procons), the public prosecutor's offices, the public defenders' offices, specialised police offices (Decons) and civil organisations aimed at protecting consumer's rights, including the right to privacy and data protection.

Box 4.5. Competencies of Brazil's National Data Protection Authority

1. Ensure the protection of personal data, in accordance with the legislation.
2. Elaborate guidelines for the National Policy for the Protection of Personal Data and Privacy.
3. Supervise and apply sanctions for the processing of data in violation of the legislation.
4. Promote knowledge among the population of norms and public policies on the protection of personal data and of the security measures.
5. Stimulate the adoption of standards for services and products that facilitate the exercise of data subjects regarding their personal data.
6. Promote international co-operation with the data protection authorities of other countries.
7. Prepare annual activity reports.
8. Amend regulations and procedures on the protection of personal data and privacy, and conduct privacy impact assessments on the protection of personal data in cases where the processing represents a high risk to the guarantee of the general principles of personal data protection.
9. Conduct audits, or determine their performance, within the scope of the inspection activity.
10. Enact simplified and differentiated rules, guidelines and procedures, including deadlines, so that micro and small enterprises, as well as incremental or disruptive business initiatives that declare themselves to be start-ups or innovation companies, can adapt to this law.
11. Communicate any criminal offences they become aware of to the competent authorities.
12. Implement simplified mechanisms, including by electronic means, to register complaints on the processing of personal data in violation of the law.
13. Maintain a permanent forum for communication, including through technical co-operation, with entities of the public administration responsible for regulating specific sectors of economic and governmental activity, in order to facilitate the regulatory, oversight and punitive powers of the National Data Protection Authority.

Also, the Brazilian Institute for Consumer Protection (Instituto Brasileiro de Defensa do Consumidor, IDEC)[28] has conducted activities to educate consumers on privacy rights and the protection of their personal data. Idec's website contains a section with news concerning the scope of the LGPD to national consumers and has drafted an Anti-Privacy Map,[29] which seeks to help consumers protect their personal information and to not be tracked on the Internet based on the provisions of the LGPD.

Another relevant aspect of the ANPD that should be considered according to Article 55-B of Law 13.853, is "technical and decision-making autonomy" from other entities of the executive, in particular the Board of Directors, which will be composed of five commissioners including a chair (each with an initial four-year mandate), who will rotate on a staggered basis.

It should be noted that administrative and legal frameworks that leave open even a small possibility of a privacy enforcement authority being instructed by another administrative body on how to exercise its functions do not satisfy the independence criterion. Independence may not be fully achieved if, as per Article 55-A of Law 13.853, the ANPD: will be an organ of the federal public administration; will be a member of the Presidency of the Republic; will have a transitory legal nature; "may be transformed by the executive power into an entity of the indirect federal public administration, submitted to a special autarchic regime and linked to the Presidency of the Republic"; and will not be guaranteed funding in the annual budget law.

The OECD's 2019 questionnaire of privacy enforcement authorities (PEAs) collected information on the funding sources of the respondent authorities and their composition. Twenty of the 28 countries that responded (excluding the United States) were entirely funded by government grants. The remaining countries reporting mixed funding explained that other sources come from chargeable services, registration or licensing fees, fines and penalties. PEAs require considerable financial investment from governments. In 2019, for example, the Australian PEA was funded by AUD 15.85 million in government grants. The Canadian PEA was granted CAD 29.47 million and the Irish PEA received EUR 15.2 million. The United Kingdom's Information Commissioner's Office (ICO) is primarily funded by organisations paying the data protection fee, which accounts for 85-90% of the ICO's annual budget. From 1 April 2019 to 31 March 2020, the ICO projects that it will collect roughly GBP 46.6 billion through the data protection fee. In 2018/19, it collected GBP 39.3 billion in fee income (ICO, 2020).

The modifications to the LGPD creating the ANPD differ from the rest of the statute. They were legally enforceable since the enactment of the Law 13.853 on 8 July 2019, meaning that the LGPD is already valid in what relates to the constitution and functioning of the ANPD, regardless of the *vacatio legis* of its substantial parts.

However, for the ANPD to actually exist, the federal government must act to physically create it, by means of a decree and further regulation nominating its directors and establishing its composition and functioning. As of March 2020, this had not yet occurred. The emergency caused by COVID-19 adds to the uncertainty of the situation, as proposals to postpone the entry into force of the LGPD are currently being considered in Congress.

Technical measures for data protection

Article 46 of the LGPD establishes that processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorised access and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing. The ANPD may provide minimum technical standards towards these measures, which shall be complied with from the conception phase of the product or service through to its execution.

Likewise, Article 13 of Decree 8.771[30] of 11 May 2016 that regulates Law 12.965 of 23 April 2014 (the Internet Civil Rights Framework, or Marco Civil da Internet) provides that connection and application service providers must observe guidelines on security standards in the custody, storage and processing of personal data and private communications. Among the obligations mandated by the guidelines are: the establishment of strict control over access to data, by defining responsibilities of persons who will have the possibility to access and exclusive access privileges for certain users; the provision of authentication mechanisms for access to records, by using, for example, dual authentication systems to ensure the individualisation of those responsible for data processing; the creation of detailed access logs to connection and applications records; and the use of records management solutions through techniques that guarantee the inviolability of data, such as encryption or equivalent protection measures.

Personal data breach notification

The notification of personal data breaches is a new right in Brazil, largely imported from Articles 33 and 34 of the GDPR, although with some major differences.

Article 48 of the LGPD establishes that the controller must communicate to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subject. The communication must take place within a reasonable time period and in observance of the following requirements:

a) A description of the nature of the affected personal data.

b) Information on the data subjects involved.

c) An indication of the technical and security measures used to protect the data, subject to commercial and industrial secrecy.

d) The risks related to the incident.

e) The reasons for delay, in cases in which communication was not immediate.

f) The measures that were or will be adopted to reverse or mitigate the effects of the damage. After the communication, the national authority shall evaluate the severity of the incident and adopt any appropriate measures.

Where the GDPR establishes that the notification of security incidents shall be made to the supervisory authority as well as to the data subjects involved within undue delay and within 72 hours when the data breach represents a risk to the rights and freedoms of individuals, the LGPD establishes only that the communication must take place within "a reasonable time period"; a major difference that perhaps merits further clarification in the regulation of the law in the future.

Although the ANPD will officially start to function in August 2020, there is currently a Special Unit for Data Protection and Artificial Intelligence at the state level that is already monitoring the rights of data subjects, as well as conducting investigations for incidents involving breaches of personal data and information. The unit is part of the Public Prosecutor's Office of the Federal District and has handled several cases related to personal data protection, and created a mechanism for reporting data breaches and security incidents.

Likewise, Brazil also counts on CERT.br and CTIR.gov. for handling cybersecurity incidents. CERT.br is responsible for co-ordinating Brazilian entities in response to security incidents. CERT.br is part of NIC.br and acts on a multi-stakeholder basis (public/private co-operation). CTIR.br is a governmental body and is part of the GSI/PR. CERT.br compiles and has annual statistics on incident reporting.

Privacy management programmes

The accountability principle is one of the original eight basic principles of the 1980 OECD Privacy Guidelines. The 2013 revision of the Privacy Guidelines included a new part – "Implementing accountability" – which fleshes out the elements required of data controllers to implement the accountability principle, notably introducing the concept of "privacy management programmes" (PMPs). Under the revised guidelines, PMPs are the primary operational vehicle through which an organisation is expected to give practical effect to the basic principles contained in Part II of the guidelines. Specifically, the added section provides that a data controller should give effect to the guidelines for all personal data under its control by implementing a PMP that is tailored to the structure, scale, volume and sensitivity of its operations and that provides appropriate safeguards based on privacy risk assessment, including plans for responding to inquiries and incidents. In addition, the data controller should be prepared to demonstrate its PMP and provide notice, as appropriate, to authorities and data subjects where there has been a significant security breach affecting personal data.

The LGPD contains a specific section on responsibility that applies to infringements of the law as a result of the processing of personal data by public agencies and national authorities. Article 31 allows national authorities to send a report to public agencies with the applicable measures to stop the violation, while Article 32 grants the national authority the power to request agents of the public authorities to publish impact reports on the protection of personal data and suggest the adoption of standards and good practices for the processing of personal data.

Article 50 Section 2 (I) of the LGPD partially provides for the implementation of a governance programme for privacy and operation of procedures that may include complaints and petitions from data subjects, security norms, technical standards and other specific obligations for the various parties involved in the processing of personal information, educational activities, internal mechanisms of supervision and risk mitigation, and other aspects related to the processing of personal data.

Furthermore, under Article 50 Paragraph 2, Section I, data controllers are encouraged to implement governance programmes for privacy that at a minimum: demonstrate the controller's commitment to adopt internal process and policies that ensure broad compliance; are adapted to the structure, scale and volume of his operations, as well as to the sensitivity of the processed data; establish adequate policies and safeguards based on a process of systematic evaluation of the impacts on and risks to privacy; are integrated into its general governance structure and establish and apply internal and external mechanisms of supervision, among others.

International data flows

International transfers of data have increased and become very relevant for policy makers, especially with the deployment of cloud computing services and the expansion and growth of big data in recent years. The LGPD contains a full chapter on international data transfers (Articles 33-36), which largely reflects the language of the provisions of Chapter V on transfers of personal data to third countries or international organisations of the GDPR. International transfers of personal data in Brazil are only allowed under certain conditions described in nine sections of Article 33 and listed in Box 4.6.

Box 4.6. Conditions for international transfers of personal data under the General Data Protection Law

The international transfer of personal data is only permitted in the following cases:

1. Countries or international organisations that provide an adequate level of protection of personal data as provided for by the law.
2. When the controller offers and proves guarantees of compliance with the principles and the rights of the holder in the form of:
   a. specific contractual clauses
   b. standard contractual clauses
   c. global corporate rules
   d. issued stamps, certificates and codes of conduct.
3. When the transfer is necessary for international legal co-operation between public intelligence, investigative and prosecutorial authorities in accordance with international law.
4. When the transfer is necessary to protect the life or physical safety of the holder or third party.
5. When the national authority authorises the transfer.
6. When the transfer results in a commitment undertaken in an international co-operation agreement.
7. When the transfer is necessary for the execution of a public policy or legal attribution of the public service.
8. When the holder has given his specific consent, distinct from the transfer, with prior information about the international nature of the operation, clearly distinguishing it from other purposes.
9. When the transfer is necessary to fulfil the conditions of Article 7, II, V and VI, namely fulfilment of a legal or regulatory obligation; execution of a contract or preliminary procedures related to a contract to which the holder is a party; and to exercise rights in judicial, administrative or arbitral procedures.

Furthermore, Article 34 of the LGPD establishes that the level of data protection in a foreign country or international organisation shall be evaluated by the national authority taking into consideration six particular circumstances. Article 35 establishes that the verification of all of the legal instruments enlisted under Article 33 Section II will be carried out by the national authority and Article 36 mandates that changes to the guarantees presented for compliance with the general principles of protection of data subject's rights shall be communicated to the national authority.

The European Commission has not yet declared Brazil as a country that provides an adequate level of protection of personal data pursuant to the GDPR.

Likewise, Brazil, as an observer, has not yet signed and ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol regarding supervisory authorities and transborder data flows nor the modernised version of the Council of Europe's Convention 108+.

Cross-border enforcement co-operation

Due to the increasing demand for products and services available on the Internet and social media, co-operation in the enforcement of data protection laws is an important and decisive element to help strengthen consumer trust. The OECD *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (OECD, 2007) represents a commitment of member countries to promote closer co-operation among privacy enforcement authorities to help them exchange information and conduct investigations with foreign counterparts. Section IV of the 2013 OECD Revised Privacy Guidelines highlights the importance of cross-border co-operation in the enforcement of privacy laws and facilitation of mutual assistance among privacy enforcement authorities.

Article 55-J, (IX) of the LGPD (as worded by Law 13.853 of 8 July 2019), attributes responsibility to the ANPD for promoting co-operation with international and transnational authorities on data protection. Since the ANPD has not formally been established, there are currently no bilateral or multilateral arrangements with other authorities or countries to co-operate in the enforcement of privacy laws.

Brazil is not yet part of the Global Privacy Enforcement Network[31] or similar international networks for the enforcement of privacy and data protection laws.

Data governance frameworks

Access to and sharing of data is crucial for innovation in the digital economy. For example, access to data can enhance public service delivery and facilitate the identification of emerging governmental and social challenges.

The legal frameworks and norms governing access to and sharing of personal data in Brazil presently consist of a complex regime of sector-specific laws and a patchwork of laws and regulations, including state and municipal laws that govern access to information and data protection in different sectors of the economy.[32] It should be clarified whether the aforementioned laws should coexist for some time or how they would be superseded once the LGPD fully comes into force, in order to avoid possible conflict of competencies across authorities and government agencies responsible for enforcing sectoral laws on data protection and the ANPD. For example, in Mexico, the Federal Law on the Protection of Personal Data Held by Private Parties contained a transitory article establishing that "state provisions on personal data protection are repealed, and other provisions opposing this law will be repealed" (Article 5). Although many of those provisions were not actually repealed, they are still written in law and in practice said laws should no longer be applicable.

Once the law enters into force, it will provide general rules that apply to all sectors of the economy as well as to federal, state and municipal governments. Thus, unless a provision expressly says that the LGPD is intended to pre-empt state and municipal laws that govern access to information and data protection in different sectors of the economy, one of the challenges of the ANPD would be to make sure that the old patchwork of federal laws governing the protection of information and personal data of citizens does not conflict with the LGPD. These efforts may consist of co-ordinating with the respective agencies and institutions responsible for the oversight and enforcement of the old legal framework, including the National Consumer Secretariat (Secretaria Nacional do Consumidor, Senacon)

and the entities that are part of the National Consumer's Defence System (NCDS), among other law enforcement agencies at the state level.

The Ministry of Justice and Public Security through the Department of Protection and Defence of Consumers (Departamento de Proteção e Defesa do Consumidor, DPDC) of Senacon announced, on 30 December 2019, that it had fined Facebook Inc. and Facebook Serviços Online do Brasil Ltda. BRL 6.6 million (approximately USD 1.65 million). The fine is the result of an investigation after reports that Facebook users in Brazil may have suffered from misuse of data by the political marketing consultancy Cambridge Analytica. Further, the Ministry of Justice and Public Security outlined that Facebook is considered a supplier in accordance with Article 2 of the Consumer Protection Code and noted that Facebook had failed to provide appropriate information to its users regarding the consequences of their default privacy setting, especially regarding the data of users, their friends and those shared with application developers.[33]

The commercialisation of personal data of Brazilian citizens has been an ongoing national concern. The Public Ministry of Federal Districts and Territories (Ministério Público do Distrito Federal e Territórios, MPDFT) announced, on 16 January 2020, that it had launched a civil inquiry into BaseUp for the commercialisation of personal data of more than 10 million Brazilian citizens. The MPDFT highlighted that BaseUp operated a database which includes information such as names, addresses, zip codes, emails and taxpayer identification numbers which were then available for sale in different packages. The MPDFT requested the Brazilian Network Information Centre (NIC.br) to take down the website and domain name of BaseUp and to provide information on the person who registered the domain name in the Whois directory.[34] At the time of writing this report, the website (baseup.com.br) had been completely taken down and was no longer accessible.

Concerning policy initiatives for enhancing access to and sharing of data, Law 12.527 of 18 November 2011 (also known as the Transparency Law) governs access to information to public entities that are part of the direct administration of the executive; legislative, including the Courts of Accounts; the judiciary and the public prosecutor's office. This law establishes the rules and procedures for access to information requests to said entities.

Likewise, Decree 8.777 of 11 May 2016 establishes the Open Data Policy for the federal executive branch, which has nine fundamental objectives, as listed in Box 4.7.

Box 4.7. Main objectives of Brazil's Open Data Policy

1. Promote the publication of data contained in databases of direct, local and foundational federal public administration agencies and entities in the form of open data.
2. Improve the culture of public transparency.
3. Grant citizens access, openly, to data produced or accumulated by the federal executive.
4. Facilitate the exchange of data between entities of the federal public administration and the different spheres of the federation.
5. Foster social control and the development of new technologies for the construction of a participatory and democratic public management environment and better provision of public services for the citizen.
6. Foster empirically based scientific research on public management.
7. Promote technological development and innovation in the public and private sectors and promote new business.
8. Promote the sharing of information technology resources, in order to avoid duplication of actions and waste of resources in the dissemination of data and information.
9. Promote the provision of digital public services in an integrated manner.

The management of the federal executive branch's Open Data Policy is co-ordinated by the General Comptroller of the Union (Controladoria-Geral da União) through the National Open Data Infrastructure (Infraestrutura Nacional de Dados Abertos, INDA) as established in Decree 9.903 of 8 July 2019.

In addition, Brazil is part of the Open Government Partnership (OGP) and as mentioned on the OGP's website:

> *Brazil is currently implementing 11 commitments from their 2018-2020 action plan. This action plan features commitments related to local open government, open data, open science, climate change and water, legislative transparency and social control to nutritional policies.*

Recent developments

Two major public data-processing enterprises (Serpro and Dataprev), which are controlled and partially owned by the federal government, were included in a group of public companies to be privatised by the federal government. However, both companies process a substantial part of personal data in the interest of the federal government and other public bodies. There is currently a major debate on whether data subjects will lose control over their personal data as a result of the privatisation or to what extent these data could be accessed and used for other commercial purposes, as the companies will be given access to the information in the original contracts with the public entities, which include personal data. Calls for greater attention to and assessment of the data protection impacts of the privatisation should be heeded by the federal government.

Voter identification in every election in Brazil is almost entirely made by biometry (fingerprints). The electoral body, the Superior Electoral Court (Tribunal Superior Eleitoral, TSE), has collected enough fingerprints that in the 2018 elections, more than 87 million voters could be identified by biometric means. The TSE's biometric database is at the core of the National Civil Identity (Identidade Civil Nacional, ICN), a resource created by Decree 9.278 of 5 February 2019 in order to provide a backbone for the new National Identity Document (Documento de Identidade Nacional, DNI).

Brazil is currently in the final phases of preparing its National Artificial Intelligence Strategy, which has been elaborated through a multi-stakeholder process and has undergone public consultation (closed in February 2020).

There are currently three major draft bills aimed at regulating artificial intelligence (AI) in the Brazilian parliament. These three draft bills may likely be consolidated into two bills: the first is currently being discussed in the federal Senate, the other in the House of Representatives. Both propose principles to be observed in the implementation of AI, and specifically to preserve human agency and control. Both bills also go as far as to propose a national policy on AI, which, for some of the conditions and terms, is not completely aligned with the current draft National Artificial Intelligence Strategy currently being elaborated by the Ministry of Science, Technology, Innovations and Communications.

Conclusions and recommendations

Brazil passed the General Data Protection Law on 14 August 2018. The law creates a normative framework seeking to harmonise and expand the right to personal data protection. It is largely aligned with the OECD Privacy Guidelines and the GDPR, although some important differences remain, notably in relation to the governance and oversight structures.

In particular, it is noted that provisions of the 2013 OECD Privacy Guidelines in Part V ("National implementation") call on member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to take decisions in an "objective, impartial and consistent basis" [Paragraph 19(c)]. This formulation, in the context of the guidelines, refers to the need for a privacy enforcement authority that is free from instructions, bias or conflicts of interest when enforcing laws protecting privacy.

The guarantee of the ANPD's independence is to ensure the effectiveness and reliability of the monitoring of compliance with the provisions of personal data protection and must be interpreted in light of that objective. It is established not to grant any special status to the authority or its agents, but in order to strengthen the protection of individuals and bodies affected by its decisions. It follows

that, when carrying out its duties, the ANPD must act objectively and impartially. For that purpose, it must remain free from any internal and external influence.

However, the ANPD is currently strongly linked to the executive. According to the law and as specified in Article 58-A Paragraph 1 of Law 13.853, the members of the National Council for the Protection of Personal Data and Privacy will also be appointed by the President, not by the Board of Directors. Paragraph 2 of the same article mentions that each of the representatives of the CNPDP (executive, Senate, deputies, National Council of Justice, National Council of the Public Prosecutor, Internet Steering Committee) will be appointed by the respectively responsible entities of the public administration.

Besides overseeing compliance with the LGPD, the ANPD will have the main task of co-ordinating a range of different entities and engaging with the CNPDP and the Ombudsman, and other legal entities, which are likely to be distributed across the country. These various entities all play a relevant role in fostering and promoting policies on privacy and data protection. Although essentially an advisory body, the CNPDP's responsibilities and particular tasks do not seem, however, clearly or sufficiently defined under the law.

In addition, the LGPD does not specifically mention how the Board of Directors will implement the decisions and recommendations of said bodies or how said entities will address disagreement when it arises.

The development of a coherent and well co-ordinated national strategy on AI in Brazil may generate new and relevant public policies with a significant impact on the economy and social landscape of the country in the years to come. However, the strategy should be conceived and deployed with caution, taking into consideration existing policy frameworks and in co-operation with national stakeholders from different sectors. It should be well aligned with and complementary to the obligations and rights enshrined in the LGDP and other relevant national legal frameworks, and take account of ongoing international discourse in the field of privacy and data protection.

Box 4.8. Policy recommendations for enhancing privacy and data protection

In order to enhance privacy and data protection, Brazil should:

- Re-evaluate and amend the conditions establishing the National Data Protection Authority (ANPD) in Article 55-A of Law 13.709 to ensure that the Authority operates with full independence from the date of its establishment.
- Ensure that the rules for appointing the ANPD's Board of Directors and the National Council for the Protection of Personal Data (CNPDP) are transparent, fair and based on technical expertise.
- Clarify the responsibilities and tasks of the CNPDP.
- Set clear decision-making rules within the ANPD and for their implementation by the Board of Directors.
- Guarantee an adequate and predictable budget to the ANPD through a transparent process.
- Align the National Strategy on Artificial Intelligence to the General Data Protection Law and other relevant legal frameworks, in co-operation with all stakeholders.

Protecting digital consumers

Around the globe, consumers today are able to fulfil a significant proportion of their goods and service needs through e-commerce channels, in both developed and developing economies. They can do so at any time and from anywhere, and in particular across borders. Despite the many benefits that global e-commerce can bring to consumers, the complexity of the environment and the continued emergence of new business models and involvement of a myriad of economic operators may put their interests at risk. Consumers' understanding of their rights and obligations in the digital transformation are often challenged when they acquire digital content products, such as apps or games; when they purchase products through mobile devices; and when they transact with businesses located in foreign jurisdictions.

Protecting digital consumers is at the core of the OECD's *Recommendation of the Council on Consumer Protection in E-commerce* (hereafter "E-commerce Recommendation") (OECD, 2016), whose main high-level principles are listed in Box 4.9.

Box 4.9. The OECD *Recommendation of the Council on Consumer Protection in E-commerce*: Selected general principles for protecting digital consumers

1. Fair business and advertising practices.
2. Appropriate disclosures.
3. Effective processes for transaction confirmation and payment.
4. Product safety across e-commerce supply chains.
5. Meaningful access to effective mechanisms to resolve disputes.
6. Consumer education and awareness.
7. Authorities' powers to investigate and take action at domestic level.
8. Authorities' ability to engage in international policy and enforcement co-operation.

Source: OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, *https://doi.org/10.1787/9789264255258-en*.

The E-commerce Recommendation was revised in 2016 to address a number of new and emerging e-commerce issues affecting consumers in the digital transformation. These include:

- growing consumer adoption and use of complex intangible digital content products and the related need for consumers to obtain clear, timely and conspicuous information about the limitations, functionality and interoperability of such products
- changing and more active consumer behaviour
- growing consumer use of mobile devices
- increasing risks associated with online and mobile payments and unsafe products.

The E-commerce Recommendation also highlights the need to provide redress to consumers involved in "free" transactions concluded in exchange for consumer data, and to address the privacy and security risks of e-commerce services, including payment methods.

E-commerce trends in Brazil

Growth of domestic and cross-border e-commerce

According to data from the Brazilian Consumer and Retail Association, B2C e-commerce sales are relatively small in Brazil, representing 3%[35] of all retail sales (export.gov, 2019; Administrative Council for Economic Defence of Brazil, 2018). Nonetheless, e-commerce sales in Brazil grew at an annual rate of 16% in 2019, far exceeding growth in the economy as a whole (Ebit Nielsen, 2020).

Brazil's e-commerce market, however, seems to offer outstanding opportunities for online retailers at local, regional and global levels. According to Euromonitor International, Brazil generates about 42% of all B2C e-commerce in Latin America. In 2017, an estimated 52.8 million people were shopping on line in the country, representing an increase of 11% compared to 2016 (Société Générale, 2019). A recent study conducted by PwC found that that 53% of Brazilians use their smartphones to research products, and 32% use online payments to purchase goods (export.gov, 2019). Increased consumer interest in, and adoption of, mobile devices to search and compare products on line, including on social media, is expected to further boost e-commerce transactions.

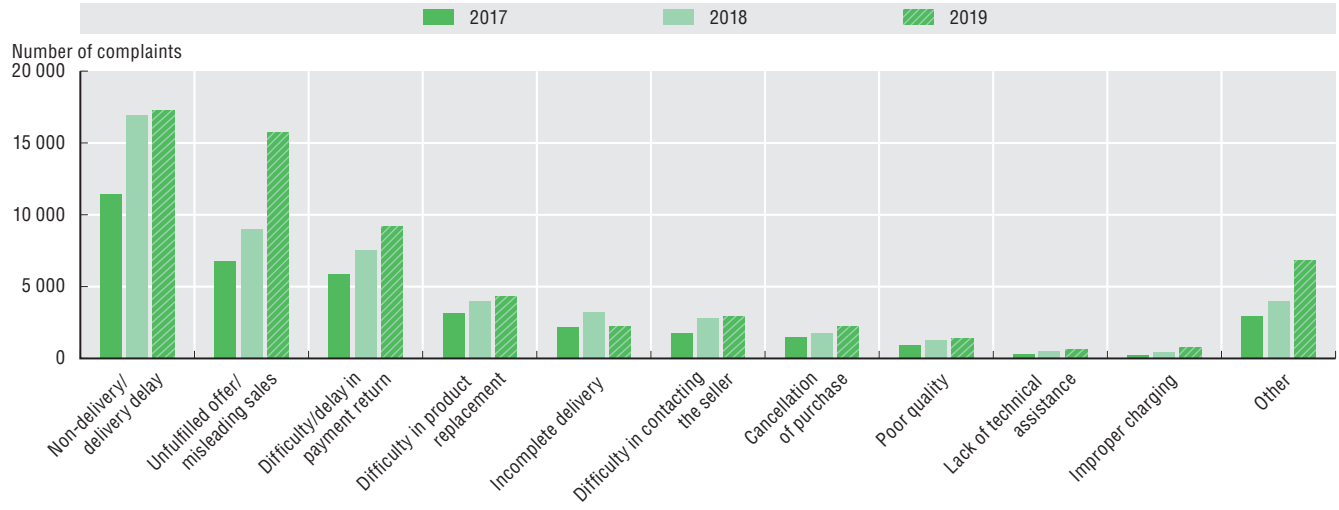
With respect to cross-border e-commerce, available data show that 23% of Brazilian consumers shop on US-based websites versus 9% of European consumers. Half of the Brazilian population (around 100 million people) has purchased through international websites, at least once. Chinese and other websites are also very popular, including AliExpress (45% of consumers), Amazon.com (40%), eBay (26%), DealExtreme (12%) and Apple Store (10%) (Société Générale, 2019).

Consumer complaints

Consumidor.gov.br[36] and the National Consumer Defence Information System (SINDEC)[37] are two main databases maintained by Senacon,[38] containing consumer complaint data about e-commerce transactions. As explained later in this report, while Consumidor.gov.br serves as an online dispute resolution system, SINDEC[39] provides all stakeholders with information concerning companies about which consumers have complained the most.

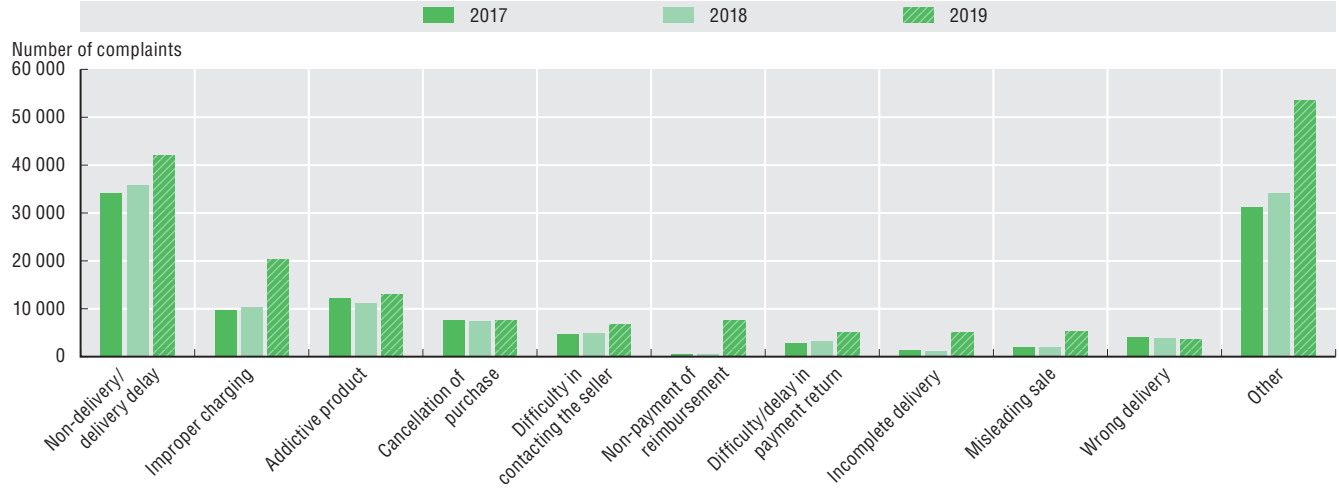
As shown in Figures 4.6 and 4.7, a growing number of e-commerce problems has been reported by consumers since 2017 on both platforms. The highest number of consumer complaints are related to non-delivery or late delivery of products. A number of consumers also experienced various problems throughout the transaction process, including payment confirmation and cancelling of transactions, and communicating with a business.

Figure 4.6. E-commerce complaints submitted to Consumidor.gov.br, 2017-19



Source: Consumidor.gov.br (2020), *Indicatores* (database), *https://consumidor.gov.br/pages/dadosabertos/externo/* (accessed in March 2020).

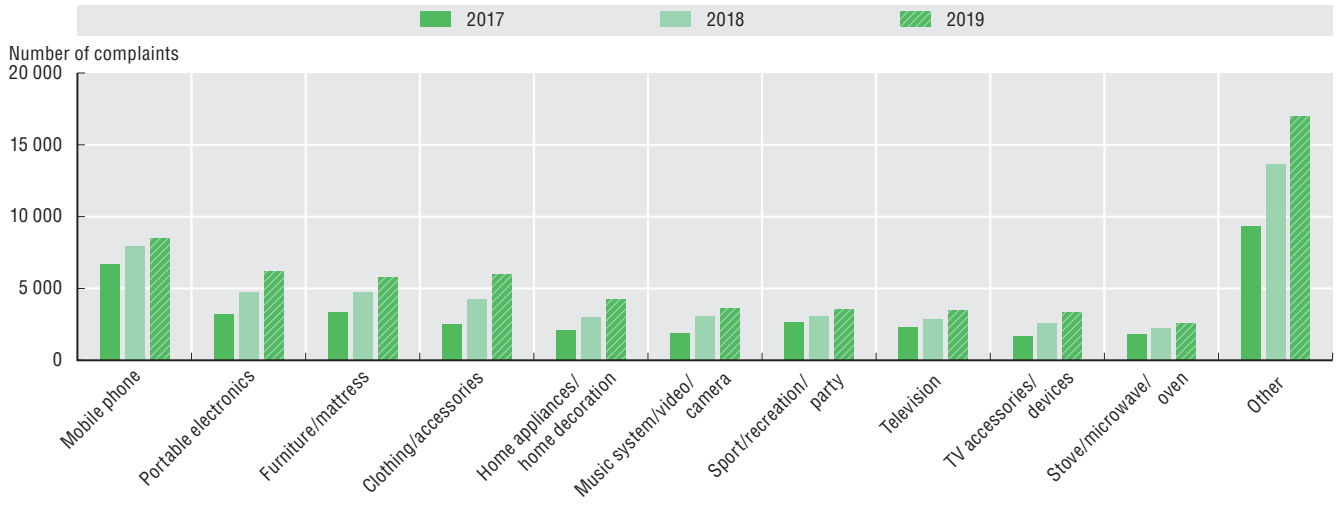
Figure 4.7. Major e-commerce complaints reported on SINDEC, 2017-19



Source: OECD, based on information provided by the National Information System for Consumer Protection (Sistema Nacional de Informações de Defesa do Consumidor, SINDEC).

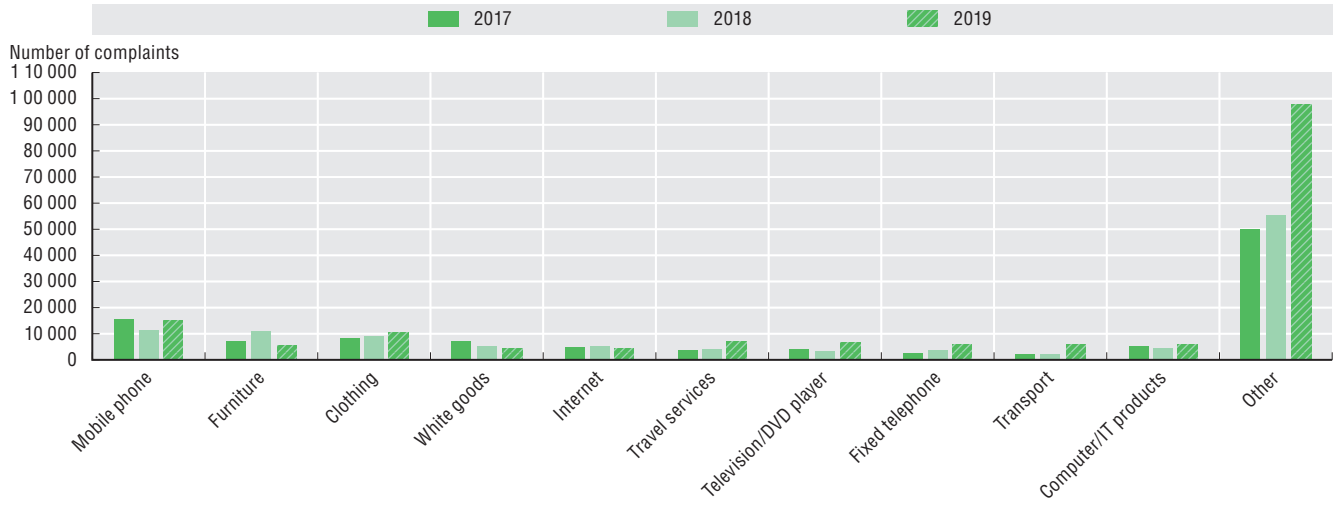
As shown in Figures 4.8 and 4.9, mobile phones attracted the highest number of consumer complaints on both platforms from 2017 to 2019. Consumers also encountered problems with a wide range of products, including furniture, electronic devices, clothing, and Internet and travel services. Figure 4.10 shows that a number of consumers faced problems with online retailers and marketplaces.

Figure 4.8. E-commerce complaints per product category submitted to Consumidor.gov.br, 2017-19



Source: Consumidor.gov.br (2020), *Indicatores* (database), *https://consumidor.gov.br/pages/dadosabertos/externo/* (accessed in March 2020).

Figure 4.9. E-commerce complaints per product category reported on SINDEC, 2017-19

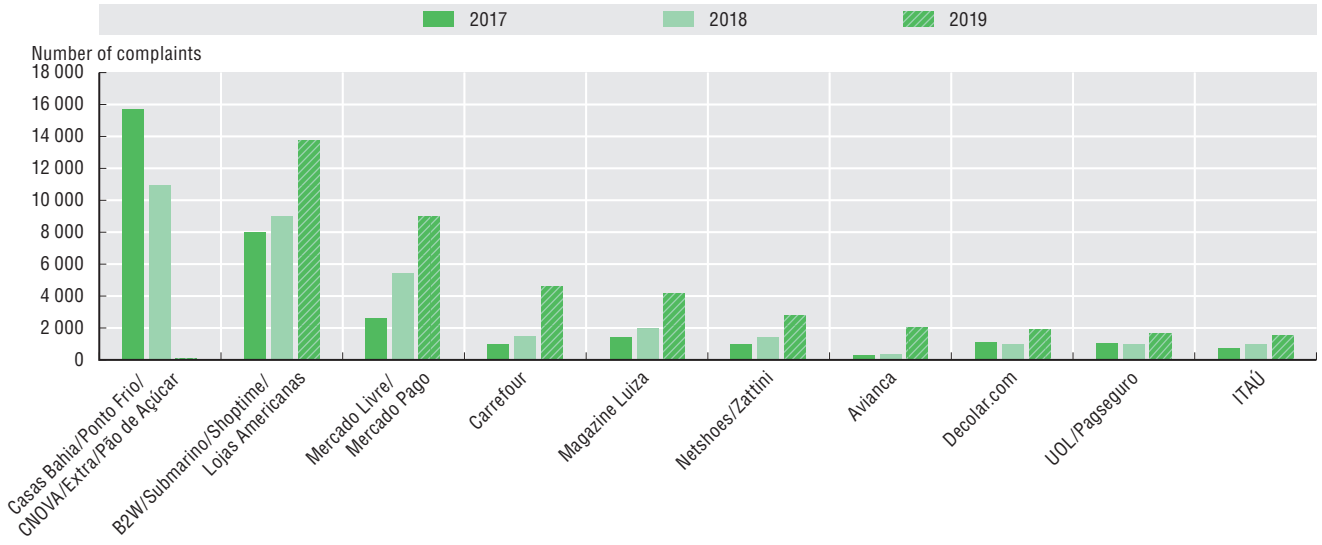


Note: IT = information technology.

Source: OECD, based on information provided by the National Information System for Consumer Protection (Sistema Nacional de Informações de Defesa do Consumidor, SINDEC).

With respect to cross-border transactions, issues associated with long delivery times (44% of consumers buying across borders) and a lack of security (31%) have also been reported by consumers (PagBrasil, 2018). However, it should be noted that neither Consumidor.gov.br nor SINDEC contains a specific issue category on cross-border transactions, thus information on available consumer complaint databases does not help to understand the degree to which Brazilian consumers experience problems with cross-border transactions.

Figure 4.10. Complaints by economic group reported on SINDEC, 2017-19



Source: OECD, based on information provided by the National Information System for Consumer Protection (Sistema Nacional de Informações de Defesa do Consumidor, SINDEC).

E-commerce policy framework

Over the past two decades, much has been done in Brazil to strengthen consumer trust in e-commerce. While most general consumer protection rights are enshrined in Brazil's Consumer Defence Code (CDC) adopted in September 1990, in recent years, a number of legislative developments have been implemented to strengthen the protection and engagement of digital consumers.

Under Article 6 of the CDC, consumers are to be provided by businesses with adequate and clear information about the goods and services on offer and the transaction. They should benefit from strong protections against misleading and fraudulent practices, including in the online advertising area. Consumers should have access to effective dispute resolution mechanisms, including at the judicial and administrative level, and should be provided with adequate redress in the case of financial and non-financial detriment.

The CDC was supplemented in 2013 by Decree 7.962 of 15 March 2013, specifically covering e-commerce. The decree identifies key information disclosures to be provided to consumers engaging in e-commerce and reinforces a right of withdrawal of seven days.

The protection of consumers on line has been further strengthened through the adoption in 2014 of the Internet Civil Rights Framework,[40] which provides the foundational principles, guarantees, rights and obligations for users of the Internet in Brazil, and lays out guidelines for action by the country's union, states, federal district and municipalities. More specifically, the law regulates the use of the Internet in the following areas: freedom of expression; privacy and data protection; net neutrality; preservation, stability, safety and functionality of the Internet; accountability of agents; preservation of the participatory nature of the Internet. Under Article 7, Internet access is essential to the exercise of citizenship and subsection XIII stipulates that citizens have the right to the correct application of norms for the protection and defence of the consumer in consumer transactions conducted through Internet.

With the entry into force on 20 December 2017 of Law 13.543/2017, rules on online advertising of goods and services sold through e-commerce have also been strengthened. The new law, which amends Law 10.962/2004 governing the establishment of prices for consumer goods and services, introduces new requirements for businesses to provide consumers with clear and conspicuous information about product prices, and with the image of the good or the description of the service.

In the area of consumer product safety, which is addressed under Chapter IV of the CDC, Brazil published two new ordinances in 2019 on product recalls (Ordinance 618/2019 on general rules, and Joint Ordinance 3/2019 on vehicle recalls). This updated recall legislation regulates the procedures for recalls of all products in Brazil, regardless of the medium or channel used by consumers to acquire the recalled product. Under the framework, a supplier who becomes aware of the unsafe nature of a good once placed on the market must immediately inform the authorities about it and alert consumers accordingly.

Institutional oversight

The E-commerce Recommendation highlights the need for authorities to have:

- the power to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively
- the ability to co-operate and co-ordinate their investigations and enforcement activities with their counterparts in foreign jurisdictions.

Authorities with powers to act at the domestic level

The main Brazilian consumer protection authority is Senacon, which sits under the Ministry of Justice and Public Security. Created in 2012, Senacon succeeded to the DPDC, which was established in 1990 by the CDC.

Senacon's main powers and attributions are provided in Article 106 of the CDC and Article 3 of Decree 2.181 of 20 March 1997[41] that regulates the NCDS. Senacon oversees the development, implementation and enforcement of consumer protection laws, including through co-ordination with the NCDS. Senacon also maintains Consumidor.gov.br, which is a free public out-of-court service that can be used by consumers and companies to resolve their disputes arising from online transactions. In addition, Senacon has the power to engage in international co-operation with authorities in other countries. It does so mainly through the UN Conference on Trade and Development's (UNCTAD) Informal Group of Experts on Consumer Protection, the Southern Common Market (Mercosur), the Ibero-American Forum of Consumer Protection Agencies, and the Organization of American States.

The NCDS encompasses a number of public entities at the federal, state and local level, such as the Consumer`s Protection and Defence Authorities (Procons), the public prosecutor's offices, the public defenders offices, specialised police offices (Decons), as well as private entities and civil organisations promoting programmes and assistance in protecting consumers rights. Procons are responsible for co-ordinating their own local or state consumer policies. Moreover, Procons provide support for consumers and investigate consumer problems, while Senacon does not carry out these functions. Senacon's main objective is to co-ordinate the functioning of the NCDS in order to promote harmonised national policies for consumer relations.

The entities of the NCDS contribute to Senacon's general task to design and promote policies regarding consumer protection, including in an e-commerce context. Some of the programmes promoted by Senacon are: the National School of Consumer Protection, the National Consumer Policy programme, the National Information System for Consumer Protection (SINDEC), and the National Consumer and Citizenship Plan (Plandec).

In recent years, Senacon has explored ways to improve the effectiveness of Brazil's institutional framework. The agency has, in particular, signalled that it would need more resources and expert staff to engage in international co-operation.

Senacon currently has 90 staff, of which about 30 are technical experts. It has an annual direct budget of USD 950 000. According to a 2018 OECD study on cross-border enforcement co-operation across 31 countries, on average (despite great variations among countries), consumer agencies have 369 employees and a budget of USD 33 million (OECD, 2018).

The need for resources to assist in the implementation of Brazil's consumer protection framework may increase as the country introduces new measures for consumer data protection. On 14 August 2018, Brazil enacted a new General Data Protection Law (Law 13.709) and is working towards the establishment

of a National Data Protection Authority (NDPA). Senacon is expected to co-operate with the NDPA to address consumer data-related issues. Moreover, following the adoption of Decree 10.197 in 2020, Consumidor.gov.br has become the official federal government platform for handling consumer dispute resolutions. As a result, issues associated with consumer data protection are within the scope of the platform, and consumer complaints regarding consumer data protection are filed at Consumidor.gov.br.

Cross-border co-operation

The E-commerce Recommendation puts a strong emphasis on enhancing and facilitating international co-operation in fights against fraudulent and misleading commercial practices across borders. The issue is becoming particularly important as global consumer complaint data show that the growing volume of cross-border transactions on line has been coupled with an increase in cross-border fraud, and a growing availability on line of unsafe products that have been banned or recalled from the offline marketplace.

In such a context, where new business models and technologies have made it easier to use virtual borders to evade regulations by setting up in one country and targeting consumers in another, deeper and more routine cross-border co-operation is needed. In 2018, more than 29 000 international complaints were reported to econsumer.gov,[42] a website dedicated to collecting cross-border complaints maintained by the International Consumer Protection Enforcement Network, which is an informal network comprised of consumer authorities from over 60 countries (including 14 G20 economies).

To date, there is no specific framework on cross-border co-operation in consumer protection in Brazil. Aside from the lack of resources to engage in cross-border co-operation, the lack of framework for cross-border co-operation has been identified as a barrier to international co-operation. Hence, Senacon should be equipped with the abilities and tools necessary to further enhance cross-border co-operation.

Senacon has signed a Memorandum of Understanding on consumer protection with seven countries, including Argentina, Germany, Korea, Paraguay, Peru, Portugal and Uruguay. Recently, it has also strengthened its engagement in cross-border co-operation within the framework of the OAS' Health and Safe Consumption Network, to address product recall issues. Senacon is one of the founders of the RCSS, which covers recalls of products, foods and medicines. Senacon has also co-operated with counterparts within the framework of the Mercosur in areas such as consumer complaints handling.

Until 2018, Senacon did not have the necessary resources to engage in cross-border co-operation with foreign consumer protection agencies nor to enhance its collaboration with the OECD and other fora, such as UNCTAD. Senacon is currently in the process of obtaining more resources (including budget and expert staff) to promote and engage in international co-operation, including to help enhance the capacity of the NCSD to collaborate with the international co-operation carried out by Senacon. Senacon has started a process for joining the International Consumer Protection and Enforcement Network, and intends to also participate in the econsumer.gov platform, once the Portuguese version of the platform is launched.

Role of industry associations

There is a large number of private associations and chambers involved in the development of guidance and policies related to information technology, including policies concerning digital issues and studies on e-commerce and Internet. These entities are not linked to the NCDS associations.

The most active private sector organisations focusing on e-commerce in Brazil are:

The Brazilian Chamber of Electronic Commerce (Camara e-net)[43] is the most representative Brazilian entity in the digital economy whose major role has been to promote security in electronic transactions, formulate public policies and improve sectoral regulatory frameworks that provide legal support to the incentive measures necessary for the development of the country. It also aims to encourage innovation, knowledge generation and the sustainable development of the digital economy. Camara e-net has eight special committees that companies may join and support their work: 1) Antifraud and Risk Management; 2) Trusted Digital Identities; 3) Insurtechs; 4) Legal; 5) Internet Payment Systems;

6) Micro, Small and Medium Enterprises; 7) Traveltech; and 8) Online Retail. Camara e-net also promotes consumer trustmarks like Clique e-Valide[44] and supports national campaigns to help consumers navigate and purchase safer on line, like Internet Segura[45] and DETONAWEB 2019.[46]

The Brazilian Electronic Commerce Association (ABComm)[47] is a non-profit organisation composed of a large number of national retail companies from the information technology sector. The association promotes the interests of technology companies with government institutions. ABComm's website contains useful information on e-commerce, including studies and surveys.

Senacon oversees the implementation of a number of co-regulation initiatives. For instance, in 2019, the telemarketing industry launched a "Do not call" initiative to ensure that businesses do not make unsolicited telemarketing calls to consumers. Similarly, in 2020, the Brazilian Federation of Banks will commence a "Do not call for credit offers" platform.

The role of consumer associations

Consumer associations play an important role in the development and implementation of Brazil's consumer policy framework. Some consumer associations, including Idec and Proteste, are members of the NCDS, and take part in the development and dissemination of consumer policy.

In addition, many consumer associations in Brazil help raise consumers' awareness through their website, publications and other promotional activities. For instance, a number of consumer associations have participated in annual consumer awareness campaigns in relation to Black Friday sales.

Dispute resolution mechanisms and redress for consumers

Dispute resolution schemes

Various private alternative dispute resolution schemes are available in Brazil to resolve disputes between consumers and businesses through the Internet. Among them is Reclame Aqui[48] ("Complain Here"), which has more than 15 million users and 120 000 companies registered.

In addition, in 2014, Senacon established Consumidor.gov.br, which is a free-of-charge public online dispute resolution scheme allowing consumers and businesses to resolve their disputes directly on line. The platform, which is monitored by Procons and the Ministry of Justice, contains a list of participating companies organised by area, including companies engaging in e-commerce. Consumers first need to register on the website or mobile app and file a complaint. Businesses have up to ten days to review it and provide a formal response to the consumer. Consumers have an additional 20 days to indicate whether they are satisfied with the feedback from the business.

It should be noted that if no settlement with a business has been reached through a private or public online dispute resolution, consumers retain the right to submit a complaint through the formal administrative procedures that are available via Brazil's government bodies in charge of consumer protection, such as the state and municipal Procons, public defenders, public ministries, and special civil courts.

According to a 2019 consumer survey conducted by Senacon, 97% of users of Consumidor.gov.br recommend the platform; and 80% of users reported that their problems were solved through the platform. However, there is a need for better communication to raise consumers' awareness of the platform. The same survey reveals that 59% of consumers did not know that the platform was also available as a mobile app; and only 25% considered the platform well publicised.

To address the issue and further promote and encourage the use of Consumidor.gov.br, Senacon has been co-operating with Brazil's national and state courts of justice. Such a strategic partnership between the judiciary and the executive has helped to reduce the volume of judicial disputes that included over 6 million consumer problems, even though the special civil courts were created to simplify legal processes. Senacon has already signed partnerships with 20 national courts of justice. In July 2019, it signed a technical co-operation agreement with the National Council of Justice to promote the integration between the Consumidor.gov.br and the PJe (electronic judicial process).

In addition, Senacon has engaged with businesses to expand the number of participating companies in Consumidor.gov.br. To broaden the membership, Senacon allows businesses to use a label "Participation Stamp" to indicate their participation in the platform.

Dispute resolution cases

In recent years, the DPDC of Senacon has opened the following administrative cases:

- Facebook Inc. and Facebook Serviços Online do Brasil Ltda (three *ex officio* cases opened discretionarily by the DPDC):
  - In one of the cases, the DPDC is in charge of verifying alleged illegal consumer data sharing by the above-mentioned Facebook companies. The case opened in 2018; the administrative process was launched in March 2019.
  - In another case, the DPDC found alleged illicit access of Facebook user accounts in Brazil through the Facebook platform collecting personal data, such as names, emails, phone numbers, visited places and Internet searches. The case was opened in 2018 and the administrative process launched in March 2019.
  - A third case concerns the verification of the use of sensitive personal data, including cardio-frequency and menstrual cycles, collected by associated apps, including from people that were not actual users of Facebook. The case started in February 2019 and is currently in a preliminary verification phase.
- Google Brasil Internet Ltda. The DPDC received a formal complaint by the Public Prosecutor's Office of the state of Piauí concerning access to personal emails sent via Gmail without the express consent of Gmail's users. An administrative procedure was launched in February 2019.[49]
- OI (TNL PCS S/A). The DPDC opened an investigation against the former Brazilian telecom company OI concerning alleged irregularities in the technology capable of mapping and tracking consumers' Internet browsing and purchasing history, for advertising purposes. The administrative process was launched in February 2019.

Education and awareness

One relevant instrument that Brazil developed in this area was the Foreign Consumer Guide[50] created by the Procon of the state of Parana under the supervision of the Brazilian Institute for Metrology, Standardisation and Industrial Quality (INMETRO).[51] The main purpose of the guide is to provide guidance to foreign consumers in Brazil on their rights and obligations in their relations with businesses and entities in different areas of the economy. The guide was drafted based on the rights and obligations of businesses and consumers in the CDC. It contained information such as where to file a complaint and how to obtain legal redress and provides a list of consumer and defence organisations and associations that may support consumers through their disputes. It has not, however, been updated.

The National School of Consumer Protection (NSCP)[52] was created on 13 August 2007, through Ministerial Ordinance 1.377. It is actively engaged in fostering knowledge and education on consumer protection by providing specially designed training to members of the NCDS across the country, as well as building specific knowledge on consumer relations, which are essential for the elaboration of public policies. The NSCP has a large number of digital manuals and guides to protect consumer rights. For example, it created a guide on data protection in consumer relations and credit information. The NSCP has a partnership with the University of Brasilia to implement an official certification system. It has expanded its public education programmes by engaging other national public agencies like the National Health Surveillance Agency; the National Civil Aviation Agency; the Central Bank of Brazil; the National Telecommunications Agency; the Ministry of Agriculture, Livestock and Supply; and the National Health Agency, among others.

New initiatives have been implemented in recent years to educate and raise consumer's awareness of their rights in e-commerce and to increase their digital competence. For instance, Senacon produced an educational video on consumer issues related to the digital economy.[53] In addition, educational programmes targeting vulnerable or disadvantaged consumers have been developed, which look at the impact of social media on the youths' consumption trends.[54]

Conclusion and policy recommendations

Box 4.10 contains proposed recommendations from the OECD for Brazil to enhance consumer protection and empowerment, and to improve its evidence base for consumer policy decision making.

Box 4.10. Policy recommendations for consumer protection and empowerment

In order to enhance consumer protection and empowerment, Brazil should:

- Establish a framework for analysing consumer complaints data and identify issues requiring policy and enforcement responses to protect digital consumers.
- Collect and analyse consumer complaints data that are specific to cross-border transactions to better understand the nature and scale of consumer issues associated with transactions across borders.
- Provide relevant domestic authorities, such as Senacon, with adequate powers, tools and resources to enhance their participation in cross-border co-operation for consumer protection. This could include participation in the activities of the International Consumer Protection and Enforcement Network.
- Improve the effectiveness of the government's dispute resolution and redress platform, Consumidor.gov.br, by evaluating consumer usage and satisfaction of the platform and further raising consumer awareness of the database, while looking into unresolved cases.

References

Administrative Council for Economic Defence of Brazil (2018), *Implications of E-commerce for Competition Policy: Note by Brazil*, *https://one.oecd.org/document/DAF/COMP/WD(2018)37/en/pdf*.

Baptista Luz (2017), *Current Legislation on Data Protection in Brazil*, white paper, Baptista Luz Advocados, *http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf*.

Cert.br (2020), *Estatísticas dos Incidentes Reportados ao CERT.br* [Statistics on the Incidents Reported to CERT.br], *https://www.cert.br/stats/incidentes* (accessed on 8 March 2020).

Cetic.br (2018), "A8. Estabelecimentos de saúde, por existência de documento que define uma política de segurança da informação" [Health establishments, due to the existence of a document that defines an information security policy], *TIC Saúde 2018*, Comitê Gestor da Internet no Brasil, São Paulo, *https://www.cetic.br/tics/saude/2018/estabelecimentos/A8*.

Consumidor.gov.br (2020), *Indicatores* [Indicators] (database), *https://consumidor.gov.br/pages/dadosabertos/externo/* (accessed in March 2020).

CTIR.br (2020), *Estatísticas Resultantes do Trabalho de Detecção, Triagem, Análise e Resposta a Incidentes Cibernéticos* [Statistics Based on the Work of Detection, Screening, Analysis and Response to Cyber Incidents], *https://emnumeros.ctir.gov.br* (accessed on 9 March 2020).

Demetrio, A. (2012), "Na Rio+20, Exército testa estratégias de defesa virtual em grandes eventos" [At Rio + 20, Army tests virtual defense strategies at major events], G1, *http://g1.globo.com/tecnologia/noticia/2012/05/na-rio20-exercito-testa-estrategias-de-defesa-virtual-em-grandes-eventos.html*.

Ebit Nielsen (2020), *Webshoppers* 41ª Edição [Webshoppers 41st Edition], *www.ebit.com.br/webshoppers*.

EUROPOL (2018), *Internet Organised Crime Threat Assessment (IOCTA) 2018*, European Agency for Law Enforcement Cooperation, *https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf*.

export.gov (2019), *Brazil: eCommerce*, *https://legacy.export.gov/article?id=Brazil-e-Commerce* (accessed on 27 January 2020).

GSI (2015), *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018* [Federal Public Administration Information and Communications Security and Cybersecurity Strategy 2015-2018], *http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view*.

GSI/PR (2010), *Livro Verde: Segurança Cibernética no Brasil* [Green Paper: Cybersecurity in Brazil], Presidência da República, Brasilia, *http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf*.

Hurel, L.M. and L. Cruz Lobato (2018), *A Strategy for Cybersecurity Governance in Brazil*, Strategic Note 30, Instituto Igarapé, Rio de Janeiro, *https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf*.

ICO (2020), "How we are funded", Information Commissioner's Office, Wilmslow, United Kingdom, *https://ico.org.uk/about-the-ico/who-we-are/how-we-are-funded*.

Insurancecorp (2019), *MARSH/JLT Lança Estudo Sobre Segurança Cibernética* [MARSH/JLT Launches Cybersecurity Study], *http://insurancecorp.com.br/pt/2019/05/14/marsh-jlt-lanca-estudo-sobre-seguranca-cibernetica/*.

LexisNexis Threatmetrix (2019), *LexisNexis Risk Solutions Cybercrime Report: Global Insights from the LexisNexis Digital Identity Network January-June 2019*, LexisNexis Risk Solutions, *https://www.threatmetrix.com/wp-content/uploads/2019/09/lnrs-cybercrime-report-1568230431.pdf*.

Ministry of Foreign Affairs (2019), *Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública* [Accession Process to the Budapest Convention – Joint Note from the Ministry of Foreign Affairs and the Ministry of Justice and Public Security], Note 309, *www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica*.

Norton (2018), *Cyber Safety Insights Report Global Results*, *www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2018-norton-lifelock-cyber-safety-insights-report-global-results-en.pdf*.

OECD (2019a), Going *Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264312012-en*.

OECD (2019b), *Recommendation of the Council on Digital Security of Critical Activities*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456*.

OECD (2019c), *Unpacking E-commerce: Business Models, Trends and Policies*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/23561431-en*.

OECD (2018), "Consumer protection enforcement in a global digital marketplace", *OECD Digital Economy Papers*, No. 266, OECD Publishing, Paris, *https://doi.org/10.1787/f041eead-en*.

OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264255258-en*.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264245471-en*.

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*.

OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352*.

PagBrasil (2018), *Brazil Ecommerce Report 2018*, PagBrazil, *https://www.pagbrasil.com/news/brazil-ecommerce-report-2018* (accessed on 27 January 2020).

Ponemon (2017), *2017 Cost of Data Breach Study: Brazil*, Ponemon Institute LLC, Traverse City, Michigan, *https://www.ibm.com/downloads/cas/EGGP7BBZ*.

Société Générale (2019), *Brazilian Market: E-commerce*, Société Générale, *https://import-export.societegenerale.fr/en/country/brazil/ecommerce?accepter_cookies=oui* (accessed on 27 January 2020).

Notes

Israel
The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1. Available at: *www.planalto.gov.br/ccivil_03/decreto/D3505.htm*.
2. Marco Civil da Internet, regulatory process of Law 12.965/2014, available at: *https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180*.
3. Judgment 3117/2014-TCU-Plenary of 12 November 2014, referring to TCU Case No. 003,732/2014-2, available at: *https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14D78C1F1014D794C57073235*.
4. Decree 9.637 of 26 December 2018, available at: *www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm*.
5. Available at: *http://participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber*.
6. Official Gazette, published on 6 February 2020, Vol. 26, Section 1, Page 6, Decree 10.222 of 5 February 2020.
7. Information available at: *www.brazil.gov.br/government/how-the-government-works/federal-executive-branch*.
8. Decree 9.668 of 2 January 2019, Article 26.
9. Decree 9.668 of 2 January 2019, available at: *www.gsi.gov.br/sobre/estrutura/secretaria-de-coordenacao-de-sistemas*.
10. Until the entry into force of the *General Data Protection Law*.
11. Information available at: *http://dsic.planalto.gov.br/coordenacoes-gerais/cgnsc*.
12. Information available at: *http://dsic.planalto.gov.br/coordenacoes-gerais/cggsic*.
13. Information available at: *www.ctir.gov.br*.
14. PNSI, Articles 9-11.
15. PNSI, Article 15.
16. Resolution No. 4.658 of 26 April 2018, available at: *www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf*.
17. Information available at: *https://www.iti.gov.br/icp-brasil*.
18. Information available at: *https://www.iti.gov.br/comite-gestor*.
19. Information available at: *https://www.iti.gov.br/auditoria*.

20. Available at: *https://estrutura.iti.gov.br*.
21. Available at: *https://www.iti.gov.br/icp-brasil/estrutura*.
22. Available at: *https://internetsegura.br/outras-iniciativas*.
23. Available at: *https://www.cert.br/cursos/index-en.html*.
24. Available at: *https://www.rnp.br/sistema-rnp/cais/tratamento-de-incidentes*.
25. Article 6 of the PNSI, which describes modules of the future National Cybersecurity Strategy, raises similar questions: cybersecurity; cyber defence; security of critical infrastructures; security of confidential information; and protection against data leakage.
26. Available at: *https://www.anatel.gov.br/legislacao/resolucoes/22-2007/8-resolucao-460*.
27. Available at: *www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm*.
28. *https://idec.org.br*.
29. Available at: *https://idec.org.br/ferramenta/anti-mapa-de-privacidade*.
30. Available at: *www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm*.
31. The Global Privacy Enforcement Network is an informal public network designed to promote cooperation on practical aspects of the enforcement of privacy and data protection laws. This network provides a list of official points of contact for participating authorities to facilitate investigations and enforcement co-operation on specific matters and to share experiences and best practices on enforcing issues and investigative techniques.
32. One study shows that Brazil currently has more than 40 sectoral laws and regulations that regulate data protection directly or indirectly (see Baptista Luz [2017]). For instance, the Civil Code sets forth the right to one's private life as a personal right that is neither assignable nor waivable by its subject in any circumstances. The Consumer Defence Code of 1990 establishes specific rules for the collection, processing, transfer, disclosure and storage of consumer data and the requirements for companies to obtain the unambiguous consent from consumers to conduct their activities, as well as specific data subject rights like access to information and the right to data rectification.

    The Internet Civil Legal Framework (Marco Civil da Internet) sets forth principles, rules, rights and obligations of Internet users in Brazil. The law contains specific rules on the collection, processing and storage of personal data and the transfer of data to third parties, as well as obligations on transparency, data minimisation and implementation of security measures by data controllers.
33. See the Ministry of Justice and Public Security's press release of 30 December 2019 at: *https://www.novo.justica.gov.br/news/mjsp-multa-facebook-em-r-6-6-milhoes*.
34. The MPDFT's Civil Inquiry No. 03/2020 of 16 January 2020 and its request to NIC.br for the takedown of the domain name is available at: *https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/11547-mpdft-investiga-empresa-que-vende-dados-de-cidadaos-na-internet*.
35. The OECD average in 2017 was around 9% (OECD, 2019c).
36. Available at: *https://www.consumidor.gov.br*.
37. Available at: *https://sindecnacional.mj.gov.br*.
38. Senacon is the National Consumer Secretariat of the Ministry of Justice and Public Security, and is in charge of developing, promoting, co-ordinating and implementing Brazil's consumer policy framework.
39. Senacon is introducing a new consumer complaint database "Pro Consumidor", which will gradually replace SINDEC from 2020.
40. Law 12.965 of 23 April 2014, available at: *www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm*.
41. Available at: *www.planalto.gov.br/ccivil_03/decreto/D2181.htm*.
42. Available at: *https://www.econsumer.gov/#crnt*.
43. Available at: *https://www.camara-e.net*.
44. Available at: *https://e-mpe.com*.
45. Available at: *www.internetsegura.org*.
46. Available at: *https://www.detonaweb.com.br/pme*.
47. Available at: *https://abcomm.org*.
48. Available at: *https://www.reclameaqui.com.br*.
49. A summary abstract of this case is available at: *https://globaldatareview.com/article/1180225/google-facing-proceedings-in-brazil-over-email-scanning*.

50. Available at: *https://www.justica.gov.br/seus-direitos/consumidor/educacao-para-o-consumo/guia-do-consumidor-estrangeiro/anexos-1/guia_eng.pdf*.
51. Available at: *www4.inmetro.gov.br*.
52. Available at: *https://defesadoconsumidor.gov.br/escolanacional*.
53. The video is available at: *https://www.defesadoconsumidor.gov.br/portal/ultimas-noticias/1165-mjsp-lanca-quarto-video-do-programa-se-liga-consumidor*.
54. More information is available at: *https://www.defesadoconsumidor.gov.br/escolanacional/cursos/lista-de-cursos-em-andamento*.