ARTICLE 19

Brazil: Cyber-security strategy

April 2016

Legal analysis

Executive summary

In this document, ARTICLE 19 analyses the Strategy of Information and Cyber-Security Security and Communication of the Brazil Federal Public Administration for 2015-2018 (the *Estratégia).*

The *Estratégia* is a binding document within the broader framework of the general strategic planning of the Government of Brazil. It develops the Normative Instruction GSI/PR 01/2008 of the Chief Minister of the Cabinet of Institutional Security of the Presidency of the Republic regarding the management of security of information and communications in the Federal Public Administration. The *Estratégia* has been prepared and approved by the aforementioned Cabinet. The text has the stated aim of seeking best practice in the area of security of information and cyber-security and establishing the main strategic objectives and goals for the next four years, which will inspire and guide further and more specific actions.

ARTICLE 19 believes that since the *Estratégia* is relevant to the protection of wide range of human rights, and in particular the right to freedom of expression, it must be reviewed for compliance with international standards, as well as with domestic freedom of expression and human rights laws. The *Estratégia* proposes relevant principles regarding protection of human rights, multi-stakeholder approach, access to information and participation. However, our analysis finds that there are serious shortcomings. In particular:

- The Government fails to ground the *Estratégia* firmly in the international and domestic protection of human rights. There is minimal reference to domestic protection of human rights, especially those related to freedom of expression and digital technologies;

- Among the goals of the *Estratégia* is the achievement of certain results for the benefit of society, including transparency, the protection of privacy, the democratization of access to information, and the safeguard of confidential information assets. This objective is relevant to and quite in line with the applicable national and international legal standards. However, the *Estratégia* fails to elaborate further specific recommendations in this area. Moreover, the enumeration of the different concrete strategic objectives in the central part of the *Estratégia* does not mention or even take into account these important values and rights.

- While the execution of some of the guidelines set out in the *Estratégia* will require the involvement of different groups of private actors, those who will primarily apply and follow its directives will be the various departments and agencies of the Federal Administration. Significantly, it is the vagueness of the provisions guiding the actions of these public actors that is the most problematic part of the *Estratégia,* with strong implications for human rights.

- In the development of the *Estratégia,* no relevant consultations with stakeholders have taken place; it has been consulted only within the Federal Administration. We find it problematic that civil society, organizations, individuals and other Internet stake-holders were not given the chance to analyze and make contributions to the *Estratégia.* While this document formally establishes the cyber-security strategy of the Federal Administration, and acknowledges the main responsibilities of public institutions, it must not be mistaken for a mere "internal" set of directives. We also note that such consultations

have been organised previously around similarly important legislation, such as *Marco Civil da Internet*; these consultations have been broadly appreciated as a highly positive approach.

ARTICLE 19 calls on the Government of Brazil to revise the text of the *Estratégia* in the light of recommendations outlined in this analysis and ensure that a broad range of stakeholders are involved in the process.

Summary of recommendations:

- As a matter of principle, public policies – including those related to security of information and communications and cyber-security - should be open to a broad and comprehensive discussion among all the relevant stakeholders. This discussion must be based on clear and comprehensive documents and proposals elaborated by competent public bodies; the proposals should also take into account all relevant legislative parameters established at a national level, as well as international standards;
- Respect for human rights, especially the rights to freedom of expression and privacy, should be properly incorporated into the panoply of objectives and guiding principles of the *Estratégia*, as well as references to public participation, accountability, and access to information of public interest. A vision of cyber-security beyond internal administrative dynamics should also be integral to the premises and purpose of the document;
- All guiding principles and objectives should be drafted in a more precise way, incorporating the values clearly established in the national legislation as well as the language and aims included in several international documents;
- Guidelines on multi-stakeholders' discussions about decisions on national investment in SIC and SegCiber need to be introduced and developed;
- Any training or formative program in this area must not give disproportionate importance to the defence of national sovereignty as a component of cyber-security. National security concerns must be properly balanced with human rights, accountability and access to information;
- Research on SIC and SegCiber should be comprehensive and complete, and therefore go beyond technological issues to cover areas such as human rights and public policy, in the broadest sense of these terms;
- The governance model to be implemented regarding the SIC and SegCiber should be properly defined; more specifically, it should be developed in consultation with different actors and must incorporate among its priorities the adequate protection of human rights, full accountability and the adoption of a multi-stakeholder approach;
- References to partnerships to improve confidentiality or the integrity of information should be accompanied by more clear and specific directives vis-à-vis the protection of privacy and the adequate exercise of the right to freedom of expression;
- The *Estratégia* needs to be more specific on the actions to be taken regarding the protection of critical infrastructures; in particular, it needs to elaborate on the involvement of different stakeholders, citizens' right to information on these matters, and the establishment of proper safeguards for an adequate protection of human rights. It also needs also to set out clear guidelines regarding the cooperation between public institutions and private actors in this area;
- In order to achieve the strategic objective of promoting citizens' awareness about SIC and SegCiber, the *Estratégia* needs to establish mechanisms for the adequate dissemination of comprehensive information, particularly regarding the effective exercise and protection of human rights and the different mechanisms available to achieve such aims.

Table of contents

Introduction

In April 2016, ARTICLE 19 analysed the Strategy of Information and Cyber-Security Security and Communication of the Brazil Federal Public Administration for 2015-2018 (*Estratégia).*[1]

The *Estratégia* is a binding document[2] within the broader framework of the general strategic planning of the Government of Brazil which is based on the Normative Instruction GSI/PR 01/2008 of the Chief Minister of the Cabinet of Institutional Security of the Presidency of the Republic regarding the management of security of information and communications in the Federal Public Administration, and it is aimed at providing protection to its own networks and communications systems. The *Estratégia* as such has been prepared and approved by the Cabinet.

The purpose of the *Estratégia* is to establish a series of general strategic principles for providing protection; it is hoped that these principles will inspire and guide further and more specific actions, in order to achieve the main strategic objectives and goals for the next four years in the area of security of information and cyber-security.

ARTICLE 19 believes that the *Estratégia* – as a governmental policy addressing cyber-security – has serious implications for the protection of many human rights, particularly the right to freedom of expression and the right to privacy. Importantly, ensuring the security of the online transactions of public agencies and departments should facilitate the effective protection of broad range of human rights, since many relevant public services (such as health, security, public information, transportation and etc) are now performed online.

Hence, in this analysis, ARTICLE 19 reviews the *Estratégia*'s compliance with international standards and outlines how these should be properly reflected therein. We also believe that it is important to consider how the *Estratégia* is subsequently applied in practice. In our analysis of these issues, ARTICLE 19 actively seeks to offer constructive recommendations on how the *Estratégia* can be improved.

ARTICLE 19 urges the Brazilian Government to address the shortcomings identified in this analysis. We stand ready to provide further assistance in the process.

[1] The legal analysis is based on the original version of *Estratégia* in Portuguese, available at http://bit.ly/22T8EOs.

[2] The binding nature of the document should be understood without prejudice to the planning tools which provide the general background for this *Estratégia,* as well as the principles and rights established by national legislation and international standards.

Relevant international standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments that bind states, including Brazil; particularly pertinent are Article 19 of the **Universal Declaration of Human Rights (UDHR)**[3] and Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).[4]

Additionally, **General Comment No 34**,[5] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and means of dissemination, including all forms of electronic and Internet-based expression.[6] In other words, the protection of freedom of expression applies online in the same way that it applies offline. States parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[7] The legal framework regulating the mass media should take into account the differences between print and broadcast media and the Internet, while also noting the ways in which media converge.[8]

Similarly, the four special mandates for the protection of freedom of expression have highlighted, in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011, that regulatory approaches appropriate to the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[9] In particular, they recommend the development of regulatory approaches tailored to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

As a state party to the ICCPR, Brazil must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR, as interpreted by the HR Committee, and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must, however, be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination of whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **Be prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[10] Ambiguous,

[3] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[4] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[5] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[6] *Ibid.*, para 12.
[7] *Ibid.*, para 17.
[8] *Ibid.*, para 39.
[9] Joint Declaration on Freedom of Expression and the Internet, June 2011, available at http://bit.ly/1CUwVap.
[10] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).

vague or overly broad restrictions on freedom of expression are therefore impermissible;

- **Pursue a legitimate aim:** these legitimate aims are exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as: respect of the rights or reputations of others; protection of national security; public order; public health or morals. As such, it would be impermissible to prohibit expression or information solely on the grounds that it casts a critical light on the government or the political social system espoused by the government;

- **Be necessary and proportionate**. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[11]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[12]

National security and freedom of expression

The **Johannesburg Principles on National Security, Freedom of Expression and Access to Information**[13] (Johannesburg Principles), a set of international standards developed by ARTICLE 19 and international freedom of expression experts, are instructive on restrictions on freedom of expression that seek to protect national security.

Principle 2 of the Johannesburg Principles states that restrictions justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The restriction cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, concealing information about the functioning of its public institutions, or entrenching a particular ideology.

Principle 15 states that a person may not be punished on national security grounds for disclosure of information if

- the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or
- the public interest in knowing the information outweighs the harm from disclosure.

Further, the **Tschwane Principles on National Security and the Right to Information**[14] also consider extensively the types of restrictions that can be imposed on access to information.

[11] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[12] General Comment 34, *op.cit.*, para 43.
[13] Adopted on 1 October 1995. The Principles have been endorsed by the UN Special Rapporteur on FOE and have been referred to by the UN Commission on Human Rights in their annual resolutions.
[14] The Tschwane Principles, available at http://osf.to/1jag6nW.

Prohibiting incitement to discrimination, hostility or violence

It is also important to note that Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law. At the same time, "inciting violence" means more than just expressing views that people disapprove of or find offensive:[15] it is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At the international level, the UN has developed the Rabat Plan of Action, an inter-regional, multi-stakeholder process involving UN human rights bodies, NGOs and academia - which provides the closest definition of what constitutes incitement law under Article 20 (2) of the ICCPR.[16]

Surveillance of communications

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[17] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR,[18] which states, *inter alia*, that no one should be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In **General Comment no. 16** on the right to privacy,[19] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. The General Comment further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[20]

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism emphasised, while mainly referring to the "cyber-space," that besides a right in itself, privacy also serves as a basis for the exercise of other rights:

> Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively.[21]

---

[15] *C.f.* European Court, *Handyside v the UK*, judgment of 6 July 1976, para 56.

[16] See UN Rabat Plan of Action (2012), available at http://bit.ly/1T2efOV. It clarifies that regard should be given to six factors in assessing whether speech should can be considered as incitement, including the general context, the speaker, intent, content, the extent of the speech and the likelihood of harm occurring, including its imminence.

[17] *Ibid.*, para 84.

[18] Article 17 states: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks.

[19] General Comment 16, adopted 8 April 1988.

[20] *Ibid.*, para 8.

[21] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009, para 33; available at http://bit.ly/23NMPpo.

He has also argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test:

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under Article 17.[22]

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[23]

The Special Rapporteur on FOE has also stressed that

> The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas"[24].

Further, he observed:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.

Cyber-security and protection of human rights

Cyber-security, freedom of expression and privacy are clearly intertwined. However, there is no clear definition of cyber-security at the international level. National approaches to such concepts, meanwhile, may vary; they may also coincide or at least partially overlap with other similar concepts, such as cyber defence, IT security or prevention of cyber-crime.

The Special Rapporteur for Freedom of Expression of the Inter-American Commission for Human Rights (OAS SR on FOE) recommends the adoption of a clear and not overbroad definition of cyber-security, limited to the safeguarding of computer data and systems, or, in

[22] *Ibid.*, para 17.
[23] *Ibid.*, para 21
[24] The Report of the SR on FOE, A/HRC/23/40, 2013, para 2; available at http://bit.ly/1XMsDgk.

other words, the integrity of the web and the infrastructure of the Internet, including the confidentiality of the information that they contain.[25] According to the OAS SR on FOE, any state actions related to security in cyber-space

> [N]eed to be limited and proportionate, and designed to meet specific legal aims that do not jeopardize the democratic virtues that characterize the Web.[26]

The OAS SR Rapporteur has further stressed that the openness and decentralized nature of the Internet requires not only a multi-stakeholder approach to governance, but also the acknowledgment of shared responsibilities regarding the protection of communications and infrastructure. In addition, States should be aware of the impact on human rights, and particularly on freedom of expression, of any measure adopted in this area. States also

> [O]ught to aim to have that policy ensure the integrity of the infrastructure and the information online, so that it protects users from cyber-attacks that infringe upon their rights to privacy or freedom of expression and related rights.[27]

Any cyber-security policy or legal objective should be weighed against human rights before its adoption.[28]

- In the light of the stated objectives of the *Estratégia,* the following international principles are also relevant: A high-level meeting of the General Assembly, reviewing the implementation of the outcomes of the World Summit on the Information Society of 2015 (WSIS +10), clearly recognized the leading role that governments and other state authorities have in cyber-security matters relating to national security, acknowledging as well the important contributions of all stakeholders, in their respective roles and responsibilities. It also stressed that building confidence and security in the use of information and communications technologies should be consistent with human rights.[29]

- The OAS SR on FOE has also emphasized that cyber-security policies and measures should be fully accountable and subject to sufficient public scrutiny and debate. This recommendation also refers to actions and measures adopted by private actors and intermediaries assisting State authorities in such policies. Accountability requires not only respect for a general principle of transparency, but also the involvement of citizens, civil society organizations and other relevant stakeholders in the task of policy definition and implementation. Last but not least, public decisions and actions – even those delegated to third parties - need to be subject to proper control by mechanisms of the rule of law, and by the judiciary in particular.[30]

---

[25] Freedom of Expression and the Internet, 2013, paras 118 and 119, available at http://bit.ly/1SyvDM3. See also the chapter on the intersections between surveillance, cyber-security cybercrimes and cyber-war, in ARTICLE 19, *Da cibersegurança à ciberguerra. O desenvolvimento de políticas de vigilança no Brasil*, available at http://bit.ly/1YKG7cJ.

[26] *Ibid.*, para 120.

[27] *Ibid.*, para 121.

[28] *Ibid.* para 124.

[29] Draft Resolution submitted by the President of the GA, A/70/L.33, para 50, available at http://bit.ly/1VGHJH2.

[30] Report on Freedom of Expression and the Internet, *op.cit.*, paras 126-129. In particular, the report stated that "states should make known, among other things, the general guidelines of the policies, the agencies that are in charge, and what their responsibilities are. In the face of imminent risks or attacks, States should provide detailed information or order investigations to determine the magnitude of the events."

- Although there is no international standard on cybercrime, some regional standards have been adopted. Among these regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has become the most recognised and relevant.[31] The Cybercrime Convention provides definitions for relevant terms, including: computer data, computer systems, traffic data and service providers. It requires States parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data. Finally, and importantly, the Convention makes clear that the above measures must respect all conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

[31] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further eight states have signed the Convention but have not ratified it.

The *Estratégia* and its context

As noted above, the *Estratégia* is a binding document within the broader framework of the general strategic planning of the Government of Brazil. It has been prepared and approved by the abovementioned Cabinet. A previous overall strategy on cyber-security was approved by the Government in 2010 (the Green Paper on Cyber Security in Brazil[32]). The preparation of the draft text was undertaken by a Working Group within the Cabinet of Institutional Security, in consultation with the Management Committee of Information Security. This Committee (*Comitê Gestor de Segurança da Informação e Comunicaçōes*) is a consultative body to the Presidency of the Republic formed by representatives of different Ministries and several major State institutions).[33]

The following facts will provide a useful general context in which to properly understand the background and aims of the *Estratégia*:

- Brazil has been playing a very active role at an international level regarding the establishment of new principles and parameters in the areas of cyber-security, protection of privacy and multi-stakeholder governance of the Internet. The origin of this political stance is closely connected to Edward Snowden's famous revelations on massive surveillance by US intelligence agencies;
- Brazil has recently been at the centre of international attention as the host of the 2014 World Cup; it will continue to be in the spotlight as the host of the 2016 Olympic Games. Such events raise important challenges related to Internet access, security, and other online issues;
- The Federal Public Administration in Brazil is of considerable size. Different agencies and public offices, making extensive use of the Internet, have already created a large and potentially vulnerable infrastructure. According to the *Estratégia*, the Federal Administration covers 39 Ministries,[34] around 6000 public bodies, more than 1,000,000 civil servants, 320 digital networks and 12,000,000 websites. At present, there seem to exist some deficiencies in the coordination of SIC and SegCiber actions, with no central authority implementing a systematic and multi-stakeholder approach.
- The so-called "Plano Brasil 2022" (the grand strategic plan for Brazil over the next decade)[35] includes among its objectives the deployment of broadband networks, the universality of access to culture, and the proper protection of the right to public information, as well as the consolidation of the Internet as a platform for free speech.

Additionally, several national laws provide a normative framework for the *Estratégia*:

- **The Marco Civil da Internet**[36] sets out a series of basic principles, safeguards, rights and responsibilities regarding the use of the Internet in Brazil. It has gained prominent recognition beyond Brazilian borders and its enactment was presented as a strong political commitment in favour of an open, diverse and democratic Internet. The law establishes

[32] Presidency of the Republic, Institutional Security Office, Executive Secretary, Department of Information Security and Communications, *Green paper: Cyber-security in Brazil*, 2010, available at http://bit.ly/1I5AtRt.
[33] The Committee was created by Decree number 3505 of 13 June 2000; more information available at http://bit.ly/1SomJhX.
[34] The Ministry of Planning, Budget and Management launched a plan to reduce the number of Ministries. A recent Cabinet reshuffle has indeed eliminated 8 of them.
[35] Federal Government, the Presidency of the Republic, Department of Strategic Matters, Brazil 2022, available at http://bit.ly/1VpRSaH.
[36] The Law No. 12.965 of 23 April 2014 (also known as Marco Civil da Internet).

that Internet regulation in Brazil must be founded on respect for freedom of expression, and human rights in general, as well as the idea of citizenship.[37] The Internet performs a clear social function which should be preserved accordingly. Freedom of expression and privacy are established as basic principles governing the web, and the need to preserve its stability, security and functionality is acknowledged. Responsibilities in these areas need to be proportionally shared by all actors, preserving always the participatory nature of the Internet. The Internet is also recognised as a key instrument in the promotion of access to information and participation in public affairs. The Law stipulates that proper protection of the rights to privacy and freedom of expression is a pre-condition for the full exercise of the right to access to the Internet.[38] Finally, the Law establishes a series of very clear principles applicable to the policies and activities of public bodies in relation to the Internet. In particular, the Marco Civil states:[39]

- Public authorities need to establish mechanisms for a multi-stakeholder, transparent, collaborative and democratic governance of the web, with the participation of the Government, the entrepreneurial sector, civil society and academia;
- Public sector data and information should be publicized and disseminated in an open and structured way.
- Citizen participation in public policies must be strengthened.

- **The Law on Access to Information**[40] is also an important instrument to be taken into consideration. The aim of the Law was to change the traditionally secretive behaviour of Brazilian Government and other public bodies, behaviour which was a negative legacy from a previous authoritarian period; however, there remain serious challenges in its implementation. The Law establishes the general principle of publicity, so that secrecy and confidentiality have now become the exception in legal terms; it also promotes the use of information technologies as a means to facilitate transparency and access to information, as well as social oversight of public administration.[41] The Law also
  - Assigns a series of responsibilities to public authorities vis-à-vis the safeguarding of the availability, integrity and authenticity of public information, as well as the confidentiality of personal data (Article 6);
  - Provides that citizens have the right to obtain information about all activities undertaken by public bodies including those related to their own organization and internal service; under this law, citizens also have the right to know about the implementation and results of programs, projects and actions undertaken by public entities, as well as their objectives and aims (Article 7);
  - Addresses the secrecy or confidentiality of certain sensitive information regarding national defence, international relations, and other matters (Articles 23-29). The Law seeks to define the scope of such exceptions to publicity, as well as an appropriate procedure for the adoption and revision of decisions in this area. The Law also insists on the fact that secrecy or confidentiality should be only be declared after taking into account the public interest of certain information and the need to adopt the least restrictive measure possible. However, the implementation of these particular provisions has been very problematic.

[37] *Ibid.*, Articles 2-4.
[38] *Ibid.*, Article 8.
[39] *Ibid.*, Chapter IV.
[40] The Law No. 12.527 of 18 November 2011 (Law on Access to Information).
[41] *Ibid*, Article 3.

Methodology, goals, values and guiding principles of the *Estratégia*

ARTICLE 19 makes the following general observations about the *Estratégia*:

- **The lack of clear provisions guiding the actions of public bodies**: Although the *Estratégia* is a binding document, it is not a normative legal text: it does not include clear rules or direct provisions. Essentially, the document aims at establishing a series of general strategic principles which will inspire and guide further and more specific actions. Despite the fact that, as will be shown, the execution of some of its guidelines will require the involvement of different groups of private actors, those who will primarily apply and follow its directives will be the different departments and agencies of the Federal Administration. Significantly, it is the vagueness of the provisions guiding the actions of these public actors that is the most problematic issue raised by this document, with strong implications for human rights.

- **Specific methodology used in the drafting of the *Estratégia***: the document refers to the planning and strategic methodology called *Balanced Scorecard*, developed by Robert Kaplan and David Norton. This is a managerial tool, working within technical parameters and procedures applicable to different sorts of organizations; it is a methodology essentially aimed at improving the effectiveness and efficiency of strategic plans. Here, it has been adapted to the specific context of public policy, and one of the main goals defined by the *Estratégia* refers to the achievement of certain results for the benefit of society. These societal goals include transparency, the protection of privacy, the democratization of access to information and the safeguard of confidential information assets (pages 35-36). These objectives are relevant to and quite in line with the applicable national and international legal standards as detailed above. However, it is difficult to find in the *Estratégia* a more specific plan to achieve these goals. Moreover, the establishment of the different concrete strategic objectives in the central part of the *Estratégia* does not mention or even take into account any of these important values and rights.

- **Main objective**: The main, stated objective of the *Estratégia* is to secure the use of cyberspace, impeding or obstructing actions against the interests of the country or society. This general objective seems to be a legitimate one. However, references to the protection of the exercise of human rights and to the broad participation of citizens are also needed at this point.

- **Overall goal**: Another main goal of the *Estratégia* focuses on measures and actions to be undertaken by public authorities. These not only relate to internal coordination and organization, but also include legislative and other normative changes. For this reason, although the document does not contain provisions drafted as specific norms, it is very important that it emphatically establishes a series of principles, values and rights which must be protected in the adoption of further administrative and legislative measures.

- **The lack of public participation in the development of the *Estratégia*:** The methodology section of the *Estratégia* contains a short explanation of the different stages in the elaboration of the document, detailing the actors that participated at each stage (p. 36). According to this description, the process was essentially undertaken at the "internal"

level of the Federal Administration, with the formation of a technical committee composed of personnel from the Cabinet of Institutional Security; consultations were held with the Management Committee of Information Security. It appears from this that in the elaboration of this important document no relevant consultations with actors placed outside the Federal Administration have taken place. Civil society organizations, Internet stake-holders and general public in Brazil were not given the chance to analyze and make contributions to the *Estratégia*. As explained above, we believe that this is no mere "internal" set of directives, and as such should not be developed without external consultation.

- **Failure to ground the *Estratégia* in the protection of human rights principles:** the values and guiding principles of the *Estratégia* (pages 37-41) focus exclusively on administrative and managerial concerns, such as professional ethics, collaboration, effectiveness, leadership and support for public policies. There are no clear references to citizenship, human rights, multi-stakeholder approach to Internet security, access to information or public participation. ARTICLE 19 finds it disappointing that the guiding principles refer to the implications of cyber-security only in terms of national sovereignty, centralization of decisions, resilience, or engagement by high public offices. Vague references to the need for a "strong connection between multiple actors" and the promotion of cooperation with the "productive sector and the academia" do not seem an adequate engagement with the full complexity of cyber-security strategies. Finally, this part of the *Estratégia* stresses the fact that the document will have a direct influence in the elaboration of new legal instruments in this area, making clear, once again, the vital importance of a comprehensive approach to these matters and the negative influence the deficiencies of the document may have on future measures.

  ARTICLE 19 also highlights that the only reference in the *Estratégia* to the Law on Access to Information (see above) is made vis-à-vis the special treatment of "confidential information assets whose publicity is sensitive for the country" (page 17). The *Estratégia* stresses that these provisions "have a direct impact on the strategy adopted by the Government vis-à-vis SIC and SegCiber." It is thus relevant to note that the *Estratégia* seems to provide legitimacy to secret decisions regarding cyber-security measures and actions. Despite the fact that some information in this area may indeed be sensitive and require some degree of confidentiality, there is a clear disproportion between the attention given to these considerations and the total absence of references to other transparency, access to information and accountability principles included in the Law.

  As a final observation, and despite the fact that this *Estratégia* only refers to cyber-security issues of the Federal Administration apparatus, Article 19 takes this opportunity to emphasize that neither this nor any other documents can be used to legitimize any further actions involving massive and unjustified surveillance of citizens. Moreover, the concerns reflected in the *Estratégi*a cannot be used to justify the implementation of surveillance practices against the citizens of Brazil in order to prevent social mobilization and obstruct the right to protest.

Recommendations:

- As a matter of principle, public policies – including those related to security of information and communications and cyber-security - should be open to a broad and comprehensive discussion among all the relevant stakeholders. This discussion must be based on clear and comprehensive documents and proposals elaborated by competent

public bodies; the proposals should also take into account all relevant legislative parameters established at a national level, as well as international standards;

- Respect for human rights, especially the rights to freedom of expression and privacy, as well as public participation, accountability and access to information of public interest should be properly incorporated into the panoply of objectives and guiding principles of the *Estratégia*, as well as references to public participation, accountability and access to information of public interest. A vision of cyber-security beyond internal administrative dynamics should also be incorporated into the premises and spirit of the document.
- All guiding principles and objectives should be drafted in a more precise way, incorporating the values clearly established in the national legislation, as well as the language and aims included in several international documents.
- References to secrecy and the need to protect sensitive information need to be put in the context of general rules of publicity, access to information and accountability regarding cyber-security policies.

Analysis of the specific strategic objectives

Institutionalization of SIC and SegCiber within national planning and federal budget decisions

Prioritization and proper consideration of SIC and SegCiber within the context of major policy decisions appears to be a generally positive objective. It is also worth mentioning that the *Estratégia* here refers to the need for a broad discussion with "key actors in the Government, academia, private sector and civil society" about the percentage of GDP which should be established as the minimum investment in these areas. These can be seen as good general principles, but no procedural guidelines are mentioned, nor is there any detail on what factors might be taken in to account in such debates.

Recommendation:

- Guidelines on multi-stakeholder participation in decisions on national investment in SIC and SegCiber need to be introduced and developed.

Quantitative and qualitative improvements in SIC and SegCiber personnel

The *Estratégia* indicates the need to develop training programs to improve the dedication and expertise of public officials in these areas. The document suggests the establishment of an official degree in SIC and SegCiber in the public sector. It also declares that these areas belong exclusively to the State, as they have a strategic importance in the protection of national security.

Recommendations:

- References to the training of personnel in the field of SIC and SegCiber should necessarily incorporate a strong human rights component and invoke broader citizen issues, including the accountability of public officials;
- Any training or formative program in this area must not give disproportionate or overbroad importance to the defence of national sovereignty as a component of cyber-security. National security concerns must be properly balanced with human rights, accountability and access to information.

Promotion of research in SIC and SegCiber areas

The *Estratégia* makes a general reference to the reinforcement and prioritization of research, development and innovation in the areas of SIC and SegCiber. It also refers to the need to create partnerships between universities, the private sector, and the public administration, in order to develop the best solutions. The fact that technological research will improve confidentiality of communications and therefore facilitate better protection of privacy is also mentioned. However, the text's promotion of research is limited to technology and management; even in these areas, the *Estratégia* is extremely vague with regards to identification and promotion of specific research themes and objectives. ARTICLE 19 reiterates that cyber-security demands the consideration of broader perspectives, and that development will require a multi-disciplinary approach that involves human rights and public policy, in the broadest sense of these terms.

Recommendations:

- Research in SIC and SegCiber should be comprehensive and complete, and therefore cover areas which go beyond technological issues, such as human rights and public policy, in the broadest sense of these terms;
- The document must promote the multi-participant elaboration of a complete research agenda and indicate the instruments and resources available to develop specific projects and activities.

Improvement in public governance and coordination with regards to SIC and SegCiber, including the presence of a "central" organ

The *Estratégia* highlights the need to adopt an effective governance model in these areas. This model will have a central coordination organ –the Cabinet of Institutional Security - and be based on a series of policy priorities: supporting management, agreeing on directives, bringing harmonization, increasing maturity, improving resilience, reinforcing security of information assets and protecting critical infrastructures. ARTICLE 19 finds it problematic that these priorities neither contemplate the participative and multi-stakeholder nature of cyber-security governance, nor its human rights implications.

Recommendations:

- The *Estratégia* needs to properly define the governance model that is to be implemented in SIC and SegCiber areas. This governance model should be elaborated through the participation of different actors and must incorporate among its priorities the adequate protection of human rights, full accountability, and the adoption of a multi-stakeholder approach;
- Despite the need for some sort of centralized coordination organ, cyber-security governance models should be properly adapted to the diverse and pluralist nature of the web. Transparency and access to information ought to be major guiding principles.

Alignment with the strategic planning of other organs and entities within the Federal Public Administration

The *Estratégia* stresses the fact that, in addition to good planning in the SIC and SegCiber areas within the Federal Public Administration, it is also necessary to coordinate such actions with the overall planning and strategic policies of the Government. ARTICLE 19 reiterates that the need for alignment of SIC and SegCiber actions with federal strategy must incorporate a reference to specific public policies regarding the protection of human rights, access to information, improvement of citizen participation and accountability of public authorities

Recommendation:

- The *Estratégia* must also incorporate a reference to specific public policies regarding the protection of human rights, access to information, improvement of citizen participation and accountability of public authorities, alongside the alignment with strategic policies and planning at the federal level.

Reinforcement partnerships with public and private sectors and civil society, both at a national and an international level

According to the *Estratégia*, the main objective of such partnerships would be to exchange experience and best practice to secure the availability, integrity, confidentiality and authenticity of information, thus guaranteeing the availability and continuity of public

services. ARTICLE 19 finds that these very broad principles – presented in this part of the document as strategic objectives - are already mentioned in previous parts of the text and are not here subject to any further development or specification.

Recommendation:

- References to partnerships to improve confidentiality or integrity of information should be accompanied by clearer and more specific directives vis-à-vis the protection of privacy and the adequate exercise of the right to freedom of expression.

Increased focus on SIC and SegCiber in departments of the Public Federal Administration

The *Estratégia* provides that the different departments and agencies in the public administration will establish their own plans regarding SIC and SegCiber issues, involving a series of self-diagnosis mechanisms. Such mechanisms will be generally defined by the Cabinet of Institutional Security as the central organ with responsibility in this area. However, ARTICLE 19 believes that specific SIC and SegCiber plans and self-diagnosis mechanisms need to incorporate human rights, accountability and public participation components. The Estratégia must be more clear and detailed in this area.

Recommendation:

- The *Estratégia* should further develop specific sections on how SIC and SegCiber plans and self-diagnosis mechanisms will incorporate human rights, accountability and other democratic components.

Reinforcement of SIC and SegCiber as a high priority on the Government's agenda

ARTICLE 19 observes that once again, the *Estratégia* refers to the importance of SIC and SegCiber for the political activity of the Government. In this section, it specifically points to Article 91 of the Constitution, which regards the functions of the National Defence Council. However, no mention of other important constitutional values, regarding human rights, participation, and accountability, is made at all.

Recommendation:

- Strategic objectives regarding the political planning and strategy of the Government in the areas of SIC and SegCiber should also refer to and incorporate constitutional mandates related to human rights, participation and accountability of public officials.

Improvements to reinforce the security of critical infrastructures

This strategic objective addresses a very significant area of concern: the protection of critical infrastructures. The issue is complicated by the fact that these information infrastructures are not exclusively owned and managed by the State but by private actors as well (telecommunications, electricity, etc.). The *Estratégia* acknowledges the need to take "cooperative actions" with academia and the private sector, together with the implementation of proper investments measures to guarantee the security of public infrastructures.

ARTICLE 19 notes, however, that this objective is formulated in very vague terms, and that no specific reference is made to the policy mechanisms, such as public discussion and participation, that will be adopted; human rights and accountability issues are not mentioned

at all. In addition, the eventual imposition of specific duties on private actors is a very sensitive matter: on the one hand, it can hinder investment; on the other, this process may delegate into private hands important powers which might directly interfere with the rights and activities of citizens.

Recommendation:

- The *Estratégia* needs to be more specific on the actions to be taken regarding the protection of critical infrastructures, particularly on the involvement of different stakeholders, citizens' right to access to information on these matters, and the establishment of proper safeguards for an adequate protection of human rights. It also needs to establish very clear guidelines regarding the cooperation between public institutions and private actors in this area.

Promotion of mechanisms to increase citizens' awareness about SIC and SegCiber

ARTICLE 19 finds that raising awareness among citizens is, without doubt, a powerful way to improve cyber-security, reduce risks and increase the effectiveness of measures adopted by public authorities. However, we also observe that this policy must, first, be based on the dissemination of complete and easily comprehensible information and, second, refer to the different perspectives and considerations that are involved in the notion of cyber-security. This second concern is only vaguely mentioned in the document, in relation to the prevention of cybercrimes and the protection of privacy.

Recommendation:

- The effective implementation of the strategic objective consisting of promoting citizens' awareness about SIC and SegCiber requires establishing mechanisms for the dissemination of comprehensive information among citizens, information which includes references to the effective exercise and protection of human rights.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about the ARTICLE 19's work in Brazil, please contact Paula Martins, Director of ARTICLE 19 Brazil and South America, at paula@article19.org.