ARTICLE 19

Brazil: Draft Cybercrimes Law

January 2012

Legal analysis

Executive summary

In January 2012, ARTICLE 19 analysed the Brazilian Senate's Substitute Act to the House Bill No.89 of 2003 ("Draft Law"). The Draft Law proposes the creation of new provisions relating to the prevention, detection and punishment of crimes committed with the use of the Internet. ARTICLE 19 is seriously concerned that a number of these provisions are antithetical to the rights to freedom of expression and information and therefore makes a number of recommendations to bring the Draft Law into compliance with international standards.

The Draft Law provides no guarantees for the right to freedom of expression or information. We are also concerned that provisions not only undermine these rights, but are also incompatible with legislation pending before the Brazilian legislature that attempts to secure fundamental rights online.

The Draft Law retains a number of provisions that would transform private companies responsible for delivering Internet services into an online police force. It is possible that the Draft Law would require these entities to report to the police alleged violations of the criminal law and impose criminal liability on parties that fail to exercise those responsibilities. The same provisions require the mass surveillance and data retention of all online communications by the same unaccountable private bodies for a period of three years, with few restrictions on the circumstances under which a court could order the disclosure of that data. Similar provisions have already been found unconstitutional in numerous European countries, and the Brazilian government seems eager to set the stage for a similar clash in its own courts.

The Draft Law also contains vague prohibitions on "treason" through the sharing of electronic data as well as broad provisions on the protection of personal information. Both of these provisions potentially restrict the ability of whistleblowers to disclose information in the public interest. Other problematic provisions include ambiguous restrictions on access to computers and the acquisition and transfer of data that do not require a showing of intent for the imposition of criminal liability. These potentially criminalise everyday uses of computers that cause no harm. Similarly, crimes related to the "dissemination of malicious code" also lack intent requirements.

ARTICLE 19 urges the Brazilian Government to substantially revise a number of provisions in the Draft Law to ensure respect for the right to freedom of expression and information in the country.

Recommendations

1. The Draft Law should assert the application of the rights to freedom of expression and information to all electronic forms of communication, including on the Internet.
2. Intermediaries cannot be required to monitor and report upon alleged violations of the criminal law online. Likewise, these entities should not be subject to criminal or civil liability for failing or refusing to engage in that conduct.
3. Blanket requirements for Internet intermediaries to collect and retain data relating to online communications must be removed.
4. Provisions prohibiting "access" to computer systems and the acquisition or transfer of data in violation of security measures must require a showing of intent for the imposition of criminal liability.

Table of Contents

About the Article 19 Law Programme

The ARTICLE 19 Law Programme advocates for the development of progressive standards on freedom of expression and access to information at the international level, 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 Law Programme 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 online 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 work of ARTICLE 19 in Brazil, please contact Paula Martins, Director of ARTICLE 19 Brazil at paula@article19.org or Laura Tresca at laura@article19.org or +55 11 3057 0071.

Introduction

The Brazilian Senate's Substitute Act to the House Bill No.89 of 2003 (the "Draft Law"),[1] sponsored by Representative Eduardo Azeredo, will amend Brazil's Penal Code[2] and numerous other laws to create new provisions relating to the prevention, detection and punishment of cybercrimes. ARTICLE 19 remains seriously concerned that the final version of the law will retain provisions that are antithetical to the rights to freedom of expression and information. This analysis therefore makes several recommendations to ensure the law adequately protects the rights to freedom of expression and information.

ARTICLE 19 has extensive experience of working on freedom of expression and access to information issues in Brazil. With our regional office for South America based in São Paulo, we campaign on a number of freedom of expression and freedom of information issues in Brazil; we recently submitted a report on Brazil as part of the United Nations Universal Periodic Review[3] and also made a number of recommendations to aid the development of the country's new access to information law.[4] Also in 2011, ARTICLE 19 welcomed a decision by the Supreme Court of Brazil defending the right to advocate for controversial ideas.[5] On the issue of cybercrime legislation, the ARTICLE 19 Law Programme has also recently produced analyses of cybercrimes legislation in Iraq and Iran.[6]

While there have been positive developments for the right to freedom of expression in Brazil recently, there have also been a number of recent judicial decisions that have allowed for the censoring of news, blog posts and public interest information. According to Google's transparency report, the Brazilian government ranked forth worldwide for the number of requests it made to the search engine to remove content from the Internet in the period January to June 2011. The Brazilian Government also ranked second worldwide for the number of requests it made from Google for the identities of Internet users.[7] ARTICLE 19 is concerned that the Draft Law will encourage the Brazilian government to further restrict the free flow of information on the Internet.

This legal analysis highlights numerous problems with the Draft Law that require addressing. No provision in the law guarantees or even references the importance of safeguarding free expression and information rights on the Internet. The Draft Law retains a number of provisions that would

---

[1] This analysis is based on the unofficial translation of the Draft Law from Portuguese to English in December 2011. ARTICLE 19 takes no responsibility for the accuracy of these translations or for comments based on mistaken or misleading translation. The text of this translation is available on request from the Law Programme of ARTICLE 19 (legal@article19.org).

[2] Decree-Law No. 2848 of December 7 1940 (The Penal Code)

[3] ARTICLE 19 "Brazil: ARTICLE 19's submission to the UN Universal Periodic Review", 29 November 2011, see: http://www.article19.org/resources.php/resource/2880/en/brazil:-article-19's-submission-to-the-un-universal-periodic-review

[4] ARTICLE 19 "Brazil Adopts Access to Information Law", 22 November 2011, see: http://www.article19.org/resources.php/resource/2862/en/brazil-adopts-access-to-information-law

[5] ARTICLE 19 "Supreme Court defends right to freedom of expression", 20 June 2011, see: http://www.article19.org/resources.php/resource/1823/en/brazil:-supreme-court-defends-right-to-freedom-of-expression

[6] These analyses are available from the ARTICLE 19 law programme on request.

[7] See Google Transparency Report, Accessed on 21 December 2011: http://www.google.com/transparencyreport/governmentrequests/BR/

transform private companies responsible for delivering Internet services into an online police force. It is possible that the Draft Law would require these entities to report to the police alleged violations of the criminal law and impose criminal liability on parties that fail to exercise those responsibilities. The same provisions require the mass surveillance and data retention of all online communications by the same unaccountable private bodies for a period of three years, with few restrictions on the circumstances under which a court could order the disclosure of that data. ARTICLE 19 notes that similar provisions have already been found to be unconstitutional in a number of European Countries.

The Draft Law also contains vague prohibitions on "treason" through the sharing of electronic data as well as broad provisions on the protection of personal information. Both of these provisions potentially restrict the ability of whistleblowers to disclose information in the public interest. Other problematic provisions include ambiguous restrictions on access to computers and the acquisition and transfer of data that do not require a showing of intent for the imposition of criminal liability. These potentially criminalise everyday uses of computers that cause no harm. Similarly, crimes related to the "dissemination of malicious code" also lack intent requirements.

The Draft Law is currently in the advanced stages of the legislative process. It has been approved by the Brazilian Senate and is now being re-analyzed by the ICT commission of the Chamber of Deputies. ARTICLE 19 notes that the Draft Law Rapporteur has already suggested a number of amendments that will greatly improve the law if adopted. However, we also recommend a number of further revisions to ensure that the law is brought into compliance with international standards on freedom of expression and information.

International Freedom of Expression Standards

The rights to freedom of expression and information are fundamental and necessary conditions for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights in a democratic society. This section identifies international and regional standards for the protection of freedom of expression and information, in particular in relation to the penal regulation of the use of information communication technologies (ICT). These standards form the basis of the legal analysis that follows.

Universal Declaration of Human Rights

Article 19 of the Universal Declaration of Human Rights (UDHR)[8] guarantees the right to freedom of expression in the following terms:

> "Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers."

The UDHR, as a UN General Assembly Resolution, is not directly binding on states. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948.[9]

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the UDHR. The ICCPR binds its 167 states party to respect its provisions and implement its framework at the national level.[10] Brazil acceded to the ICCPR on 24 January 1992 and is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19 of the ICCPR:

1. Everyone shall have the right to freedom of opinion
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

On 21 June 2011, the HR Committee, as treaty monitoring body for the ICCPR, issued General Comment No.34 in relation to Article 19.[11] General Comment No.34 constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 ICCPR. ARTICLE 19 considers General Comment No.34 to be a progressive and detailed elucidation of international law related

[8] UN General Assembly Resolution 217A(III), adopted 10 December 1948

[9] *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit)

[10] Article 2 of the ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967)

[11] HR Committee, General Comment No. 34, 21 June 2011, CCPR/C/GC/34

to freedom of expression and access to information.[12] It is contemporary to and instructive on a number of freedom of expression concerns raised by the Draft Law.

Importantly, General Comment No.34 affirms that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[13] States party to the ICCPR are required to take account of the extent to which developments in information technology have substantially changed communication practices around the world. General Comment No.34 calls on States party to take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.[14]

As a state party to the ICCPR, Brazil must ensure that any of its laws attempting to criminalise or otherwise regulate electronic and internet-based modes of expression, including accessing and disseminating information, comply with Article 19 ICCPR.

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. Article 19(3) of the ICCPR permits the right to be restricted in the following respects:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order, or of public health or morals.

Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. Determining whether a restriction is narrowly tailored is often articulated as a three-part test. It is required that restrictions are i) provided by law, ii) pursue a legitimate aim; and iii) that they conform to the strict tests of necessity and proportionality.[15] General Comment No.34 states that restrictions on Internet-based, electronic or other such information dissemination systems are only permissible to the extent that they are compatible with Article 19(3) of the ICCPR.[16] This includes restrictions on Internet service providers.

i) "Provided by law"

Article 19(3) of the ICCPR requires that restrictions on the right to freedom of expression must be provided by law. This requires a normative assessment; to be characterised as a law a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[17] Ambiguous or overly broad restrictions on freedom of expression deficient in elucidating the exact scope of their application are therefore impermissible under Article 19(3).

---

[12] ARTICLE 19 statement on HR Committee Comment No.34 http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression

[13] Paragraph 12, HR Committee General Comment No.34

[14] Paragraph 15, HR Committee General Comment No.34

[15] Velichkin v. Belarus, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[16] Paragraph 43, HR Committee General Comment No.34

[17] Leonardus J.M. de Groot v. The Netherlands, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).

ii) "Legitimate aim"

Interferences with the right to freedom of expression must pursue a legitimate protective aim as exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR. As such, it would be impermissible to prohibit information dissemination systems from publishing material solely on the basis that they cast a critical view of the government or the political social system espoused by the government.[18] Narrow tailoring requires that permissible restrictions be content-specific, e.g. it would be impermissible to close a website when it is possible to achieve a protective objective by isolating and removing the offending content. Where a State does limit freedom of expression, the burden is on that state to show a direct or immediate connection between that expression and the legitimate ground for restriction.

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information[19] (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 sought to be 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, to conceal information about the functioning of its public institutions, or to entrench a particular ideology. Principle 15 states that a person may not be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

General Comment No.34 also notes that extreme care must be taken in crafting and applying laws that purport to restrict expression to protect national security. Whether characterised as treason laws, official secrets laws or sedition laws they must conform to the strict requirements of Article 19(3) of the ICCPR.

iii) "Necessity"

States party to the ICCPR are obliged to ensure that legitimate restrictions on the right to freedom of expression are 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 and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result. General Comment No.34 states that generic bans on the operation of certain websites and systems are never proportionate and are therefore incompatible with Article 19(3) of the ICCPR.

American Convention on Human Rights

The Inter-American legal framework arguably provides the greatest scope of regional protection for freedom of expression. The American Convention on Human Rights (ACHR) was designed to reduce to a minimum the restrictions on the free circulation of information, opinions and ideas as

[18] HR Committee Concluding observations on the Syrian Arab Republic CCPR/CO/84/SYR

[19] Adopted on 1 October 1995. These Principles have been endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and have been referred to by the United Nations Commission on Human Rights in each of their annual resolutions on freedom of expression since 1996.

a result of the "importance that the authors of the Convention attached to the need to express and receive any kind of information, thoughts, opinions and ideas".[20]

According to the Office of the OAS Special Rapporteur on Freedom of Expression, the "Inter-American case law has explained that the inter-American legal framework places this high value on freedom of expression because it is based on a broad concept of autonomy and dignity of the individual, and because it takes into account the instrumental value of freedom of expression for the exercise of all other fundamental rights, as well as its essential role within democratic systems."[21]

Brazil became a state party to the ACHR on 9 July 1992, and is therefore legally bound to respect Article 13 guaranteeing the right to freedom of expression:

> 1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.
>
> 2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:
>
> a) respect for the rights or reputations of others; or
>
> b) the protection of national security, public order, or public health or morals.
>
> 3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.
>
> 4. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
>
> 5. Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law."

The Inter-American Declaration of Principles on Freedom of Expression (2000)[22] elaborates upon key elements of the right to freedom of expression in the Inter-American legal framework. In its fifth principle, it states that "[p]rior censorship, direct or indirect interference in or pressure exerted upon any expression, opinion or information transmitted through any means of oral, written artistic, visual or electronic communication must be prohibited by law."

---

[20] See Report No 11/96 Case 11.230 (Merits) *Francisco Martorell v Chile* Inter-Am Comm HR, 3 May 1996, para 56.

[21] Office of the Special Rapporteur on Freedom of Expression, The Inter-American Legal Framework regarding the Right to Freedom of Expression (2010) at p 2.

[22] Adopted by the Inter-American Commission of Human Rights at its 108th Regular Period of Sessions, held in October, 2000.

Joint Declaration on Freedom of Expression and the Internet

In June 2011, the four International Special Rapporteurs on Freedom of Expression[23] issued a Joint Declaration on Freedom of Expression and the Internet (Joint Declaration) in consultation with ARTICLE 19.[24] The four International Rapporteurs represent the Americas, Europe, Africa and the United Nations. In paragraph 1(a) the Joint Declaration affirms the application of freedom of expression rights to the Internet. Paragraph 4(b) of the Joint Declaration emphasises that the imposition of criminal liability for expression-related offenses must take into account the overall public interest in protecting both expression and the forum in which it is made.

Cyber Security and Respect for Human Rights

International resolutions and instruments on cyber security recognise the importance of balancing security imperatives with fundamental human rights, in particular the right to freedom of expression. The UN General Assembly Resolution on the "Creation of a global culture of cyber security" states that "security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency."[25]

From a comparative perspective, ARTICLE 19 also notes that the preamble to the Council of Europe Convention on Cybercrime (2001) states that parties must be "mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights ... which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy."[26] This is supported by Article 15 of the Cybercrimes Convention, which states that the powers and procedures provided for within the Convention "shall provide for the adequate protection of human rights and liberties", also referencing both the ICCPR and the European Convention for the Protection of Human Rights and Fundamental Freedoms.

It is noteworthy that the Council of Europe Convention on Cybercrime contains no content-based restrictions other than those relating to child pornography. The potential for domestic Cybercrimes laws to target political dissent is recognised in the Convention at Article 27(4)(a), which allows states to refuse assistance to other states party if that request is perceived to relate to a politically motivated prosecution. With 32 states party, the convention has the largest membership of any international legal instrument on this topic. Brazil is currently consulting on whether or not to join the Convention.

---

[23] The United Nations Special Rapporteur on Freedom of Opinion and Expression, Frank LaRue; the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the Organization of American States, Catalina Botero Marino; the Organization for Security and Cooperation in Europe Representative on Freedom of the Media, Dunja Mijatoviæ; and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression, Faith Pansy Tlakula

[24] Joint Declaration on Freedom of Expression and the Internet (1 June 2011); available at http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf

[25] See A/RES/57/239, Jan. 31, 2003; available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[26] Convention on Cybercrime, Budapest, 23.XI.2001; available at http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

Surveillance of Communications

Guaranteeing the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

From a comparative perspective, the European Union has grappled with the issue of protecting the privacy of communications online in its E-Privacy Directive.[27] Article 15 of this Directive provides that any infringement of privacy rights must be "necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data]."

Furthermore, the Resolution on Surveillance of Communications and Freedom of Expression, 5 June 2009, signed by 30 International Freedom of Expression Organisations, including ARTICLE 19, highlights that:

> Governments (should) fully recognize that under existing international law all persons have a right to privately communicate without interference except in the most limited circumstances (…). No surveillance should be conducted without legal authority.
>
> Governments should not adopt laws for anti-terrorism or protection of public order or security which allow for surveillance of communications or obtaining telecommunications records without adequate legal process and oversight which respects the fundamental human rights of free expression and privacy of communications.
>
> Governments should not require that telecommunications providers routinely collect and retain records of all users' activities.
>
> Governments should not require that all persons are required to pre-register or identify themselves before they are allowed to use telecommunications networks.
>
> Governments should review and revise as necessary existing legislation to ensure that rights are protected.

[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

Analysis of the Cybercrimes Law

The Senate's Substitute Act to the House Bill No.89, of 2003 ("the Draft Law") proposes to insert a number of supplementary provisions to Brazil's Penal Code that are problematic from a freedom of expression perspective. The Draft Law Rapporteur has recommended a number of amendments to the Draft Law that the Chamber of Deputies will now decide whether or not to adopt in the final version of the Law. This analysis reviews each supplementary provision, highlighting reforms recommended by the Draft Law Rapporteur, as well as recommending further reforms that are necessary to bring the Draft Law into compliance with international standards on freedom of expression and information.

Guarantees of the Right to Freedom of Expression or Information

The Draft Law states that its purpose is to amend the existing criminal law to "specify actions carried out by use of electronic, digital or similar system, computer network, or that are intended to cause harm to communication devices or computerized – and similar – systems, and sets forth other provisions." No provision in the Draft Law guarantees the rights to freedom of expression and information or makes any reference to them.

ARTICLE 19 believes that integrating protections for fundamental rights into the Draft Law would ensure that its implementation does not undermine these rights. As noted above, the UN General Assembly[28] and the Council of Europe[29] have both recognised that cyber security should not be achieved at the expense of the enjoyment of fundamental human rights. Again, the four Special Rapporteurs on Free Expression have noted that good faith efforts to regulate for cyber security too often result in undue restrictions on the right to freedom of expression;[30] the potential for this certainly exists with the Draft Law.

ARTICLE 19 notes that a Civil Rights Framework for the Internet (also known as the "Marco Civil da Internet") is also currently under consideration by the Brazilian Government. While a review of the Civil Rights Framework is beyond the scope of this analysis,[31] a cursory assessment of it shows that it provides a progressive framework for striking the appropriate balance between criminal law enforcement and respect for fundamental human rights.[32] While ARTICLE 19 welcomes the initiative of the Civil Rights Framework, we remain concerned that its adoption is likely to follow and not precede the adoption of the Draft Law, which creates several new crimes that illegitimately restrict online freedoms. There is the potential that the disparities between these two bills will lead to confusion, and that individuals may be found criminally liable for conduct that ought to be safeguarded by the Civil Rights Framework.

Recommendations

- The purposes of the Draft Law should, at a minimum, affirm the protection of fundamental human rights, including the right to freedom of expression and information.
- A civil rights framework for the Internet should comply with international standards on

[28] *Ibid,* footnote 25.

[29] *Ibid*, footnote 26, Article 15.

[30] *Ibid,* footnote 23.

[31] ARTICLE 19 is reviewing the Civil Rights Framework for the Internet (the Marco Civil da Internet) in a separate analysis. For more details, contact ARTICLE 19 Brazil.

[32] Insert link to new translation.

freedom of expression and information and be adopted before or simultaneously with the creation of any new offences related to the use of the Internet.

Crimes Against the Security of Computer Systems

The Draft Law amends Article 2, Title VIII of the Penal Code by adding Chapter IV, titled "[c]rimes against the security of computer systems."

Article 285-A of Chapter IV will make it a crime to "access through a security breach a computer system, protected [by] a security clearance system." Article 285-B prohibits the acquisition or transfer of data or information "without authorisation or failure to comply with the requirement for authorisation of the rightful owner of the computer system, protected by a security clearance system." Sentences of between one and three years imprisonment are available for both offences, in addition to a fine without a specified ceiling. Sentences may be increased by a sixth if, in relation to Article 285-A access is facilitated by identity fraud, or in relation to Article 285-B information is communicated to a third party.

ARTICLE 19 finds the following aspects of the Law are highly problematic and in violation of the international freedom of expression guarantees.

1. **Lack of definitions**: Neither Article 285-A nor 285-B have the qualities of clarity or accessibility to be "provided for by law" under Article 19(3) of the ICCPR. Key elements of the offences are not defined, including what is meant by "access", "security breach", or a "security clearance system". ARTICLE 19 notes that, for example, in the equivalent Canadian and British provisions on cyber-crimes, comprehensive definitions of technical terminology is provided in the body of the law for the sake of clarity.[33] It is recommended that definitions of these terms in the Draft Law be considered and added to the list of definitions contained in Article 16 of the Draft Law.

2. **Requisite mental state**: Additionally, the requisite mental state for imposing liability for either of these offences is not specified, allowing a person to be found guilty without having intended to breach the security measures in question or acquiring or transferring the information in question. From a comparative perspective, the Council of Europe Convention on Cybercrime provides for an offence of "illegal access" at Article 2 and only allows criminal liability to be imposed where the act is "committed intentionally... without right."[34] This largely reflects the Canadian provision, which requires the act to be committed "fraudulently" "without colour of right".[35] Similarly, the equivalent British criminal provision also requires a showing that the accused intended to access the computer system and had knowledge at the time of access that it was unauthorised.[36] Both Articles of the Draft Law could be strengthened by requiring intent to access the computer system, acquire or transfer data, as well as a showing of knowledge that access to that information was either unauthorised or constituted a security breach.

---

[33] The Computer Misuse Act (United Kingdom) 1990, section 1, Canadian Criminal Code, Article 342

[34] Convention on Cybercrime, Budapest, 23.XI.2001 at Article 2 – "Illegal access: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

[35] Canadian Criminal Code, Article 342.1

[36] The Computer Misuse Act (United Kingdom) 1990, section 1. Article 342.1(1) to the Canadian Criminal Code requires a showing of fraudulent intent "without the colour of right."

3. **No legitimate aims specified**: ARTICLE 19 is further concerned that both Articles 285-A and 285-B impose limitations on freedom of expression and information without specifying a legitimate aim, as required by above-mentioned three-part test in respect of Article 19 of the ICCPR and Article 13 of the ACHR. In their current form, the prohibitions could feasibly allow individuals to be prosecuted for innocuous everyday conduct related to computer use for no apparent purpose and are therefore unnecessary. In addition to the absence of an intent requirement, the provisions do not require a showing that harm was caused by the security breach or the unauthorised acquisition or transfer of information. This contradicts the statement by the National Congress of Brazil in the opening portion of the Draft Law, which outlines its purposes as the creation of offences that relate to specific actions "*intended to cause harm*." Legitimate aims for these prohibitions may include the protection of privacy or the protection of national security (e.g. data held on government or military computers). However, the Draft Law should indicate these protective interests clearly, in order to prevent the application of these laws to restrict expression or access to information where such legitimate interests are not engaged.

4. **Criminalising the circumvention of Digital Rights Management systems**: ARTICLE 19 is concerned that these broad provisions may be used to criminalise the circumvention of digital rights management (DRM) systems. DRM systems are technological measures that allow producers of electronic content to control how that information is used in perpetuity, and may fall within the meaning of "security clearance systems" under Articles 285-A and 285-B of the Draft law. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising absolute control over the sharing of information in perpetuity is contested. DRM systems prevent individuals from engaging in trivial and non-commercial acts of copyright infringement and therefore limit the dissemination of information and freedom of expression. They prevent, for example, an individual transferring data between their own electronic devices, or from using copyrighted works in a way ordinarily protected in intellectual property regimes by the defences of "fair use", e.g. for educational purposes. This potential application of Articles 285-A and 285-B demonstrates how their broad scope may unnecessarily restrict free expression and information.

5. **Disproportionate sentences**: The proportionality of the sentences imposed by these two provisions is also concerning. Minimum custodial sentences of one year, in practice, deny the sentencing judge the discretion to ensure the proportionality of sentences. As these provisions are so broad, they feasibly cover conduct for which it would be grossly disproportionate to impose custodial sentences at all. In many circumstances civil remedies or administrative sanctions would be far more appropriate.

The Draft Law inserts similar supplementary offences into Article 13 Title VII of the Special Part of Book I of the Military Penal Code.[37] The language of Articles No. 339 and Article No. 339A largely reflect Article 285-A and Article 285-B of the Penal Code (Civilian) revisions respectively. The Military Penal Code provisions, however, both contain the proviso "as long as this action causes harm to the military services administration". Although there is a requirement that harm be shown, there is no guidance on what "harm to the military services administration" would look like. It could feasibly include harms that are trivial; for example, any unintended breach of security measures could be framed as harm even if it is merely an administrative inconvenience.

Recommendations

- Articles 285-A and 285-B of the Draft Law (relating to the Civilian Penal Code) and

[37] Decree-Law No. 1.001, dated October 21, 1969

Articles 339 and 339A of the Draft Law (relating to the Military Penal Code) should require a showing that the accused intended the prohibited conduct and had knowledge that they were either breaching a security clearance system or acquiring or transferring information or data without authorisation.

- Articles 285-A and 285-B should require a showing of harm for the imposition of criminal liability that relates to a legitimate aim under Article 19 (3) of the ICCPR. Articles 339 and 339A in the Military Penal Code should define in narrower terms what is meant by "harm to the military services administration."
- Key terms, particularly technical language, in each of the provisions highlighted in this section should be clearly defined in Article 16 of the Draft Law.
- The sentencing provisions in each provision should remove mandatory minimum custodial sentences and provide fines or other less punitive measures as alternatives.

Law Enforcement Responsibilities of Intermediaries

Article 22 of the Draft Law recommends a number of obligations for parties "responsible for providing access to the worldwide computer network, in the commercial or public sector." These entities ("intermediaries") provide the technological infrastructure for electronic communications, and therefore play an integral role in facilitating the exercise of the right to free expression.

i) *Article 22, Subsection I*

Article 22 subsection I of the Draft Law requires intermediaries to **retain and store Internet browsing data that can be used to identify Internet users**:

> I – keep, in a controlled and safe environment, for a period of 3 (three) years, with the goal of providing the means for a formal public research, the electronic address data associated with the source, timing, date and GMT reference of the connection made through the computer network, and provide them only to the investigating authority by prior court order;

ARTICLE 19 believes the imposition of blanket data retention requirements on intermediaries to be unnecessary and disproportionate infringements on the right to freedom of expression and the right to privacy. Blanket data retention regimes, requiring no suspicion of wrongdoing, damage the preconditions of an open and democratic society by undermining the confidence individuals have in the privacy of their communications and by creating the permanent risk of data loss and data abuse. There appears to be no evidence to suggest that the practical advantages of a blanket data retention regime cannot be delivered as effectively through more targeted restrictions that do not infringe the rights of all Internet users on such a massive scale. Moreover, the enormous cost of implementing a data retention system on this scale would likely be passed onto the consumer, further restricting access to the Internet, particularly for low-income individuals.

From a comparative perspective, the data retention regime advanced by the Draft Law is much broader than the regime advanced by the EU in its Data Retention Directive (2006/2) (EU Directive), which is also severely problematic from a freedom of expression perspective.[38] Under the EU Directive, a member state may only require intermediaries to retain data for between six months and two years, rather than the mandatory three-years required by the Draft Law. We note that the longer an entity is required to hold an individuals' private data for, the greater danger there is that the privacy of that data will be compromised. The Draft Law is also much broader as it provides no restraint on the power of the Courts to order the disclosure of this private information. The EU Directive, however, at least restricts the use of such court orders to the "investigation, detection and prosecution of serious crimes." Despite these higher protections in

[38] 22 June 2010 letter to the European Commissioner for Home Affairs, co-signed by ARTICLE 19, see: http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf

the EU Directive, the EU member states of Germany, Romania and Sweden have each ruled the Directive's provisions to be incompatible with their domestic constitutions. The EC Commission is currently reviewing the necessity of the Data Retention Directive as part of its standard procedures, but numerous concerns have been raised over its compatibility with fundamental human rights. It is also noteworthy that the Council of Europe Convention on Cybercrimes does not place any reliance on a blanket data retention system for the achievement of its objectives, further bringing into doubt the necessity of Article 22, Subsection I.

ii) Article 22, Subsection II

Subsection II of Article 22 of the Draft Law provides for the Courts to order the **expedited preservation of any computer data by Internet intermediaries** "as required while the investigation is in progress". It is unclear from the text of Article 22 subsection II what categories of investigations give rise to the power to request an expedited preservation order from the judiciary, nor which authorities are competent to make such requests. Furthermore, no restriction is placed on the type of information an ISP would be requested to preserve. **An ISP may therefore be requested to store the content of communications** if the Court feels that these are "required while the investigation is in progress." The provision also fails to indicate the criteria against which a Court should judge requests for expedited preservation orders, and the circumstances under which the protection of fundamental rights would require the denial of such a request. Similarly, once a preservation order is granted, it is unclear what standards govern the circumstances under which information preserved under that order can be disclosed to the requesting party, and again how fundamental rights are protected in that situation. In summary, a huge amount of discretion is left in the hands of the judiciary to determine when expedited preservation orders may be made and for whose benefit, without any limitations on their permissible scope, including their duration.

ARTICLE 19 believes that while judicial oversight is a positive feature in Article 22 subsection II, the provision's current formulation is far too vague to provide sufficient safeguards against abuse. From a comparative perspective, Article 16 of the Council of Europe Convention on Cybercrimes contains a similar expedited preservation procedure, but this is subject to a duration limitation of 90 days, during which the requesting party may request the disclosure of that information by a separate judicial order. While ARTICLE 19 does not recommend Article 16 of this Convention as a model, we recommend that Article 22 Subsection II of the Draft Law is redrafted so that the circumstances under which a Court may make an expedited preservation order are clear and narrowly tailored to a legitimate purpose.

iii) Article 22, Subsection III and Paragraph 2

The Draft Law Rapporteur has recommended that the most problematic provision in the Draft Law, Article 22 Subsection III and Paragraph 2, be deleted. If it were retained, subsection III would require **Internet intermediaries to perform certain law enforcement functions**, under the following terms:

> "[S]ecretly report to the authorities, any situation in which a complaint has been received, which contains indication of crimes subject to inconditional [*sic*] public prosecution, as long as such crimes have occurred within the computer network under his or her purview."

Paragraph 2 provides for the imposition of criminal fines between R2,000 and R100,000 for intermediaries that fail to meet their obligations under Article 22. Sentences are increased for repeat offences with no specified ceiling.

ARTICLE 19 strongly recommends that Subsection III and paragraph 2 of Article 22 be removed, as per the recommendation of the Draft Law Rapporteur. The adoption of these two provisions

would represent a significant regression in the protection of freedom of expression and information in Brazil. The International Special Rapporteurs for Free Expression specifically warned against placing such obligations on Internet intermediaries in their Joint Declaration on Freedom of Expression and the Internet (2011):

> "[a]t a minimum, intermediaries should not be required to monitor user-generated content… [g]reater attention should be given to developing alternative, tailored approaches which are adapted to the unique characteristics of the Internet, for responding to illegal content, while recognizing that no special content restrictions should be established for material disseminated over the Internet".

From a comparative perspective, Article 15 of the EU E-Privacy Directive[39] requires any infringement of privacy rights to be "necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data]." In the context of criminal violations of intellectual property on-line, we also note that the Court of Justice for the European Union recently ruled that it would violate fundamental human rights for a state to require internet service providers to implement filtering systems to monitor and prevent illegal downloading on peer-to-peer networks.[40] The imposition of monitoring and reporting requirements on intermediaries in the context envisaged by the Draft Law is equally problematic.

There are numerous reasons why intermediaries, as mere conduits of communications and as private entities, should not be made responsible for law enforcement in relation to the content of communications they process. The same reasoning applies to protect postal services and telecommunications companies from being held liable for the content of letters or telephone calls they process. Firstly, there are significant implications for the privacy and freedom of expression rights of Internet users. The mass-surveillance of online communications these provisions would require would undermine individuals' confidence in the privacy of their communications, discouraging individuals from fully exercising their social and political rights online. Furthermore, the fines provided by Paragraph 2 would likely incentivize intermediaries to engage in broader surveillance operations than legally required and may even encourage the prior-censorship of communications by these entities in an attempt to avoid litigation. These provisions may also have implications for access to the Internet by low-income individuals, as any costs associated with implementing a private monitoring and reporting system would likely be passed on to the consumer. Moreover, it is unclear how intermediaries, as private bodies, will be held to account for the exercise of their functions and the degree of transparency their activities would be subject to. Furthermore, these private entities do not have the institutional expertise to make the complex determinations of fact and law that would be required for reporting upon alleged on-line crime. Lastly, it is unclear what level of judicial oversight these functions would be subject to.

Recommendations

- Article 22 Subsection I of the Draft Law should be deleted. Intermediaries should not be required to automatically collect and retain data related to all communications.
- Article 22 Subsection II of the Draft Law should be amended to make the circumstances under which a Court may grant an expedited preservation order clear,

[39] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

[40] For ARTICLE 19's statement on the case of *Scarlet Extended SA v SABAM*, see: http://www.article19.org/resources.php/resource/2872/en/landmark-digital-free-speech-ruling-at-european-court-of-justice

and to ensure that such orders are narrowly tailored and limited in scope to their stated objective.

- Article 22 Subsection III and Paragraph No.2 of the Draft Law should be deleted, as recommended by the Draft Law Rapporteur. Brazilian law should specifically protect intermediaries from both civil and criminal liability for the content of third party communications.

Protection of Personal Information

The Draft Law also amends Article 3 to Title I of the Penal Code to protect personal information and data from "disclosure or misuse." Under Article 154-A, custodial sentences of between one and two years may be imposed upon anyone who has disclosed, used, marketed, or made available personal data and information contained in a computerised system, for any purpose other than what it was entered on record for, except in cases provided for by law or by the consent of the person associated with that data. Sentences may be increased by one sixth if the crime is facilitated by the use of a false identity.

This absolute prohibition on the disclosure of personal information fails to anticipate circumstances in which the public interest in disclosure of that information may outweigh an individual's right to privacy in it. Article 19 of the ICCPR permits limitations on the right to freedom of expression to protect the privacy rights of others, but only to the extent that this is necessary and proportionate. For example, where the information disclosure demonstrates unlawful or unethical conduct by corrupt public officials, the privacy interest in that information must be made subservient to the public interest in information disclosure.

In their 2004 Joint Statement, the International Special Rapporteurs on freedom of expression called on governments to provide better protections for those who release "information on violations of the law, on wrongdoing by public bodies, on a serious threat to health, safety or the environment, or on a breach of human rights or humanitarian law should be protected against legal, administrative or employment-related sanctions if they act in good faith."[41] Article 33 to the United Nations Convention on Anti-Corruption requires states to consider incorporating into their domestic legal systems protections against any unjustified treatment of any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences established in accordance with this convention.[42] Brazil signed this Convention on 9 December 2003 and ratified it on 15 June 2005 and is therefore bound to abide by its provisions in the implementation of its domestic laws.

Recommendations:

- Article 154-A should incorporate a public interest defence that allows for the disclosure of information where the public interest in that disclosure outweighs the individuals' interest in maintaining the confidentiality of the information.

Dissemination of Malicious Code

A number of provisions in the Draft Law appear to be designed to protect individuals' and the military's ICT systems from the harm caused by "malicious code" (computer viruses).

ARTICLE 19 observes that several of these provisions lack intent requirements for the imposition of criminal liability, and therefore may lead to prosecutions where an individual did not knowingly

[41] Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression. December 2004.

[42] Adopted in General Assembly Resolution 58/4 of 31 October 2003

or intentionally transmit the malicious code. Such provisions include: "insertion or dissemination of malicious code" (Penal Code Article 163a and Military Penal Code Article 262a) and "insert or broadcast malicious code followed by damage" (Penal Code Article 163a paragraph no.1, Article 262A paragraph no.1 Military Penal Code). As computer viruses are often transmitted via communications, imposing criminal sanctions for the dissemination of viruses without requiring a showing of intent to cause harm may have arbitrary results and potentially discourage individuals from engaging in online communication.

Recommendations:

- Liability should not be imposed for the insertion, dissemination or broadcast of malicious code without a showing of specific intent to disseminate that code.

Treason

Article No.15, Subsections II and III of Article No. 356 of Chapter I of Title I of Book II of the Military Penal Code creates two new offences under the heading "favouring the enemy":

> II – delivering to the enemy, or placing … electronic data or any other military asset in harm's way, as a consequence of such action;
>
> III – losing, destroying, disabling, causing the impairment of, or placing … electronic data or any other military asset in harm's way.

As both these provisions contain references to "electronic data", they potentially restrict the right to free expression and access to information. Both provisions must therefore comply with Article 19 (3) of the ICCPR.

These provisions do not have the qualities of certainty or accessibility to be considered "provided by law" under Article 19 of the ICCPR. Key terms of these offences are not defined, including what is meant by "enemy" or "placing … in harm's way." Again, these provisions do not provide a requisite mental state for the imposition of liability, meaning a person can be found guilty without any showing that they intended to commit the prohibited conduct.

As outlined above, the protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is prescribed by law, necessary in a democratic society and proportionate. The Johannesburg Principles provide authoritative guidance on narrow tailoring for provisions related to national security. Principle 2 states that the genuine purpose and demonstrable effect of a provision must be 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. International standards, reflected in the Johannesburg Principles, also require that there be a causal link between the prohibited expression and the national security threat that is averted by that prohibition. Principle 6 provides a model three-part test for this purpose, allowing expression to be punished as a threat to national security only if a government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence. Article 15 Subsections I and II do not meet the requirement of narrow tailoring. "Delivering electronic data to the enemy" or "causing the impairment of data", allows for the imposition of liability without requiring a showing of a causal link between the information sharing and the threat sought to be protected against. Similarly, the provision does not specify a threat level equivalent to the incitement of imminent violence, and therefore allows information sharing that is harmless to be subject to severe criminal sanctions. This is neither necessary nor proportionate, and therefore violates international standards on freedom of expression and information.

Furthermore, subsections II and III to Article 356 of the Military Penal Code fail to provide a

defense for the disclosure of electronic data held by the military where the public interest in that disclosure outweighs competing interests in keeping that information confidential. As explained above, the obligation on governments to protect whistleblowers in these circumstances is well established in international law, and should therefore be reflected in provisions of the Military Penal Code that attempt to restrict the free flow of information.

Recommendations

- Article 356 should incorporate an intent requirement and require a causal connection between the dissemination of military electronic data and a threat to Brazil's existence or its territorial integrity.
- Article 356 of the Military Penal Code should incorporate a public interest defence for disclosing information where the interest in disclosure outweighs the individuals' interest in maintaining the confidentiality of the information.