ARTICLE 19

Brazil: Draft Computer Crime Bill

July 2012

Legal analysis

Executive summary

In July 2012, ARTICLE 19 analysed the draft Bill PLC35/2012 of Brazil (the Draft Bill). The Bill has been proposed by Deputy Paulo Teixeira and others (hence, it has also been referred to as "Teixeira Bill") as an alternative to the Cybercrime Bill, which received significant criticism from civil society organisations for its disproportionate criminalization of "everyday" internet use. ARTICLE 19 analysed the Cybercrime Bill in January 2012, stating that a number of its provisions violated international standards on freedom of expression and information.

This analysis applies the same standards to Deputy Teixeira's alternative Bill and makes recommendations for strengthening its human rights protection.

ARTICLE 19 welcomes the spirit and intent of the Bill to limit the application of the criminal law to computer-related activities. It is also positive that the drafters of the Bill recommend that any new laws should only be enacted *after* the adoption of the Civil Rights Framework for the Internet in Brazil (also previously analysed by ARTICLE 19). We are also pleased that intention is an ingredient of the index offence. However, there are various shortcomings in the Bill that need to be addressed in order to make it compliant with international standards on freedom of expression and information.

In particular, ARTICLE 19 is concerned that the Bill fails to provide definitions of key legal and technical elements of the offences. The Bill does not require the proof of any harm as an element of the offence of obtaining or using 'secret information': nor does it provide for a public interest defence in relation this offence, which, in our view, is a major weakness of the Bill. Furthermore, ARTICLE 19 considers that increased penalties for offences committed against public officials are wholly unjustified. ARTICLE 19 urges the drafters of the Bill and the Brazilian legislature to revise the Bill in order to comply with international standards on freedom of expression and information.

Recommendations

1. Key legal and technical terms of the offence must be defined, either expressly in the Bill or by reference to other laws, in particular terms such as "data,"' "security mechanisms" and "computer systems."
2. The Bill should require proof of harm arising out of the criminal activity, particularly in relation to offences involving the obtainment or dissemination of "secret information."
3. The Bill should provide for a public interest defence in relation to the "obtainment of secret information."
4. Penalties for offences should be clarified and should not include minimum mandatory sentences, which unduly constrain the judge at the sentencing stage.
5. There should be no inequity in the penalties for offences committed against public officials as opposed to "ordinary" citizens.

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 and 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 this analysis, please contact Gabrielle Guillemin, Legal Officer of ARTICLE 19 at gabrielle@article19.org or +44 20 7324 2500.

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, Freedom of Expression Officer at laura@article19.org or +55 11 3057 0071.

Introduction

In January 2012, ARTICLE 19 analysed the Brazilian Senate's Substitute Act to the House Bill No. 89 of 2003 ("the Cybercrime Bill"),[1] which proposed new provisions relating to the prevention, detection and punishment of offences committed with the use of the internet. ARTICLE 19 made a number of recommendations to amend the Cybercrime Bill to make it compliant with international standards regarding freedom of expression and information.[2]

This subsequent analysis follows on from the January report and, applying the same international standards, analyses provisions of Bill PLC35/2012 ('the Draft Bill'). The Draft Bill has been promoted by six congressmen as an alternative to provisions of the Cybercrime Bill, which were widely criticised for, *inter alia,* their potentially disproportionate criminalization of "everyday" internet use and requiring internet intermediaries to monitor and report on alleged criminality online.

ARTICLE 19 generally welcomes the spirit and intent of the Draft Bill, which according to the explanatory notes ("notes") to the Bill,[3] is to limit the application of the criminal law, refine the legal definitions used, clarify the motivational element of the criminal offences and make the penalties more commensurate to the crime.

ARTICLE 19 further considers that, in general, the Bill is an improvement to the comparable provisions proposed in the Cybercrime Bill. In particular, it is much narrower in scope, dealing principally with one index offence of invading a computing device. "e are also pleased that the Bill includes a mental element of intention in the offence and reduced prison sentences, in line with our recommendations regarding the Cybercrime Bill. It is also very positive that the Bill recommends that any new criminal provisions should be enacted *after* the adoption of the Civil Rights Framework for the Internet in Brazil ("the Marco Civil da Internet"), which currently remains under consultation.[4]

However, despite these improvements, ARTICLE 19 remains concerned that the Bill fails to meet international standards regarding the right to freedom of expression and information in a number of respects. Key legal and technical elements of the offences are not defined. The offence of obtaining 'secret information' fails to identify the nature of the threat to national security and fails to require proof of harm or the likelihood of harm to national security interests. This offence also lacks a general defence of public interest in the information obtained or subsequently passed on to others. Finally, the proposal in the Bill for increased

---

[1] For ARTICLE 19's analysis of the Draft Cyber Crime Bill, January 2012, see http://www.article19.org/resources.php/resource/2946/en/brazil:-draft-cybercrimes-law.

[2] The Cybercrimes Bill was hugely controversial and received trenchant criticisms from civil society. See for example Giswatch report 2011 about Internet Rights in Brazil; available at http://giswatch.org/en/country-report/internet-rights/brazil

[3] Translated as "justification" in the narrative translation provided to ARTICLE 19.

[4] The Civil Rights Framework for the Internet in Brazil; available in English at http://direitorio.fgv.br/sites/direitorio.fgv.br/files/Marco%20Civil%20-%20English%20Version%20sept2011.pdf. For ARTICLE 19's analysis of the Civil Rights Framework for the Internet in Brazil, see http://www.article19.org/data/files/medialibrary/3389/12-07-26-LA-brazil.pdf.

penalties for an offence committed against designated public officials is wholly unjustified under international law.

ARTICLE 19 urges the drafters of the Bill and the committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of the Bill with international standards of freedom of expression.

Analysis of the Draft Bill

The Index Offence of "invasion of a computing device"

The Draft Bill proposes the introduction of Article 154-A into the Brazilian Criminal Code. This article provides for an offence of

> Invading a computing device belonging to another, connected to a computer network or otherwise, through undue violation of security mechanisms and with the intention of obtaining, adulterating or destroying data or information without the express or tacit authorization of the owner of the device, installing vulnerabilities or obtaining and illicit advantage.

Lack of definitions

Given the potential breadth of the offence, ARTICLE 19 is concerned that key technical and legal elements are not properly or adequately defined within the Draft Bill so as to provide the level of precision required under international human rights law.[5]

- Technical terms
  Despite ARTICLE 19's previous comments on the Cybercrime Bill, we are disappointed that key technical terms in the Draft Bill, such as "computer system", "data" or "security mechanisms" remain undefined.[6] We note, for example, that equivalent provisions in a variety of international and national laws - including the Council of Europe Convention on Cybercrime,[7] the UK Computer Misuse Act 1990[8] and the Australian Criminal Code 1995 - provide definitions of these terms.

- "Obtaining an illicit advantage"
  One means of committing the index offence is obtaining an "illicit advantage" through the 'invasion of a computing device belonging to another'. The term "illicit advantage" is not defined in the Draft Bill and is equivocal. For example, an 'illicit advantage' could be interpreted as an economic benefit obtained with fraudulent intent, or as a commercial benefit obtained through exploiting information, or as a non-economic advantage of some kind. It is also not clear whether the term 'illicit advantage' applies to natural and/or legal persons as it is a term that may be more relevant to business operations or activities in the commercial sector.

[5] This also includes the Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, para 25.

[6] The same criticism applies to the term 'propagating' within Article 154-A(1), which should be defined so that it can be distinguished from the other terms of 'producing, offering, distributing...[and]...selling'

[7] For example, in the COE Convention on Cybercrime, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (Article 1(a))

[8] See section 17 of this Act, which specifically provides for interpretation of terms

ARTICLE 19 would therefore recommend that the term "illicit advantage" is either removed or further defined along the lines of the definition provided for comparable offences in countries such as the United States.

For example, the US Computer Fraud and Abuse Act provides for a crime of "accessing a computer to defraud and obtain value"[9], which is an offence distinct from that of "accessing a computer and obtaining information."[10] Particular elements of the former offence require accessing a computer with intent to defraud and, by accessing the computer, furthering the fraud and obtaining anything of value by doing so.[11] The "advantage" gained by the fraud must have some quantifiable value. For example, the offence would apply if a defendant alters or deletes computer records and receives something of value from the person who relied on those altered or deleted records; or if a defendant obtains information from a computer and uses that information to later commit a fraud.[12] Moreover, the use of the computer itself must be linked to the fraud and the obtainment of value or the 'economic advantage'. Punishment for this offence is a fine and up to five years imprisonment, whereas the lesser offence of accessing a computer and obtaining information is punishable with a fine or a term of up to one year in prison.[13]

Recommendations:

- The Draft Bill should include a definition of "computer system," "data" and 'security mechanisms."
- Article 154-A of the Draft Bill should be amended by either the removal of the term "illicit advantage" or the inclusion of a clear definition of this term, its scope and application.
- The offence in Article 154-A of the Draft Bill should require the obtainment of an "illicit advantage" (as defined) rather than merely the intention to obtain such an advantage.

Proof of harm

ARTICLE 19 recognises that the offence under Article 154-A of the Draft Bill pursues the legitimate aims of preventing crime and of respecting the privacy rights of others (Article 19(3)(a) ICCPR), the latter being protected by Article 17 ICCPR. However, it is of concern that the offence does not require the proof of any harm to a complainant. We note that the Convention on Cybercrime[14] requires that the offence of "data interference" requires the damaging, deletion, deterioration, alteration or suppression of computer data without right.

[9] Computer Fraud and Abuse Act 18 USC §1030 (a) (4)

[10] Computer Fraud and Abuse Act 18 USC §1030 (a) (2)

[11] Unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any one year period

[12] In *United States v. Butler*, 16 Fed. Appx. 99 (4th Cir. 2001) (unpublished), the defendant altered a credit reporting agency's records to improve the credit ratings of his co-conspirators, who then used their improved credit ratings to make purchases. In *United States v. Sadolsky*, 234 F.3d 938 (6th Cir. 2000), the defendant used his employer's computer to credit amounts for returned merchandise to his personal credit card

[13] Unless other aggravating factors exist.

[14] The Convention on Cybercrime is mentioned for a comparative perspective. It was adopted in Budapest on 23 November 2001; available at http://conventions.coe.int/Treaty/en/Treaties/html/185.

The Convention also provides that a State Party may reserve the right to require that such conduct amounting to data interference results in "serious harm" to establish the offence.[15]

In the Draft Bill, by contrast, a violation of "security mechanism" by someone with an intention of 'obtaining' data without the owner's consent can give rise to criminal sanctions even if no data is obtained or destroyed, no vulnerability is installed and no illicit advantage is actually obtained. Even though Article 154-B states that an offence pursuant to Article 154-A is only to be proceeded with if a complaint or 'representation' is made, this does not equate to proof of harm. It is foreseeable that a complaint could be made even if no harm had been occasioned.

Recommendations:

- Article 154-A of the Draft Law should provide that proof of harm is a constituent element of the offence.

Penalties

The penalty for commission of the index offence in Article 154-A of the Draft Bill is detention from three months to one year and a fine.

ARTICLE 19 believes that this penalty is in breach of both the legality and proportionality requirements under Article 19(3) ICCPR. ARTICLE 19 notes that the level or range of the fine is not defined nor is it made clear whether the fine is in addition - or an alternative - to imprisonment. Furthermore, ARTICLE 19 is concerned that the sentencing Judge is unduly constrained by the minimum, mandatory custodial sentence. Neither the USA[16] nor the UK[17] provide for minimum mandatory sentences for offences similar to those provided for in the Bill. This is despite these countries providing for maximum terms of imprisonment well in excess of those suggested in the Bill.[18]

Recommendations:

- Sentencing provisions should establish the level of the fine applicable, either explicitly within Article 154-A of the Draft Bill or by reference to other criminal provisions.
- Sentencing provisions should make it clear whether a fine is in addition – or an alternative – to imprisonment.
- Mandatory minimum sentences should be removed.

Article 154-A – paragraph 1

Paragraph 1 of Article 154-A of the Draft Bill criminalises the "producing, offering, distributing, selling or propagating [of] computer programmes with the intention of enabling the ... conduct defined [in the index offence]."

---

[15] *Ibid.*, Article 4(1) and (2).

[16] Computer Fraud and Abuse Act, Fn 11 above, §1030(a)(1-4).

[17] Computer Misuse Act 1990, sections 1-3A.

[18] For certain offences, 10 or 20 year maximum terms of imprisonment.

ARTICLE 19 is concerned that this provision may be used to prosecute individuals or companies producing, distributing, selling or otherwise circulating software used to break Digital Management Rights systems.

We note that the index offence criminalises the invasion of a computing device belonging to another through an 'undue' violation of "security mechanisms." In our view, the term "undue violation" is itself inherently vague, i.e. it is wholly unclear how an 'undue' violation differs from an ordinary violation.

Furthermore, as noted above, the term "security system" is undefined and is sufficiently vague so as to include Digital Rights Management Systems. DRM systems are a type of technology principally used by hardware manufacturers, publishers and copyright holders to control how digital content may be used after sale. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising in perpetuity absolute control over the sharing of information is strongly contested. For example, DRM systems prevent individuals from engaging in trivial and non-commercial acts of copyright infringement such as transferring data between their own electronic devices; they can also prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use."[19]

The explanatory notes indicate that the Bill seeks to avoid the criminalization of day-to-day conduct practised by a large part of the population. They also state that the offence does not include "the legitimate violation of security mechanisms, such as the elimination of technical protection measures that impede legitimate access... to a protected CD or DVD, for example." While Article 154-A may achieve this purpose by not criminalising the circumvention of DRMs itself, i.e. someone intentionally breaking a security system on his *own* device, ARTICLE 19 believes that Article 154-A and Article 154-A paragraph 1, read conjunctively, may be used to prosecute those who sell or otherwise distribute software that enables such conduct. The fact that the "intention" of enabling such conduct would have to be proven does not change this analysis since individuals and companies selling or distributing that kind of software would still be liable to prosecution. In the absence of any explicit definition of "security mechanisms", the natural and ordinary meaning of this term would appear to include DRM systems.

Recommendations:

- The term "undue" before "violation of security mechanisms" should be dropped from Article 154 A.
- The Draft Bill should not criminalise the circumvention of DRM systems or the production, distribution of software that may enable such conduct;
- The drafters of the Bill should be careful not to use broad language that may be construed as criminalising the circumvention of DRMs or enabling such conduct.

The offence of obtaining "secret information"

Paragraph 3 of Article 154-A of the Draft Bill reads as follows:

[19] For example, for educational purposes

> If the invasion [of a computing device] results in the obtainment of the content of private electronic communications, business and industrial secrets, secret information, as defined in the law, or unauthorized remote control of the invaded device ... penalty – imprisonment from six months to two years and [a] fine.

Paragraph 4 of Article 154-A further provides:

> In the case of paragraph 3, the penalty is increased by two thirds if there is publication, commercialization or transmission to any kind of third party of the data or information obtained, if the fact does not constitute a more serious offence.

Lack of definition of "secret information"

In ARTICLE 19's view, paragraphs 3 and 4 of Article 154-A of the Draft Bill clearly interfere with the freedom to obtain and exchange information that may be in the public interest. In order to be justified, therefore, they must meet the three-part test under international law. In particular, they must be 'provided by law', i.e. they must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.

ARTICLE 19 notes however that "secret information", is a term that is neither defined in the Bill itself, nor by reference to any other *specific* legislative provision.[20] Secret information may include both public (state) and private information. It may include information held by private individuals, who have no contractual relationship with the public sector regarding such information. Furthermore, secret information is usually divided into categories of "top secret", "confidential", "restricted" etc. - depending on the information's perceived national security importance. However, the Bill entirely fails to account for these distinctions, and, in particular, the various classifications of "secret information."

Recommendations:

- Article 154-A(3) of the Draft Bill should provide a definition of the term "secret information." In particular, it should distinguish between the various categories of classified information.

The protection of national security interests

While ARTICLE 19 recognises that the restriction in relation to 'secret information' pursues the legitimate aim of protecting national security, as is provided for in Article 19(3)(b) ICCPR, we believe that it must also be compatible with the Johannesburg Principles of Freedom of Expression and National Security.[21] According to these Principles, any restriction on freedom of expression or information that a government seeks to justify on grounds of national security must have the *genuine* purpose and demonstrable effect of protecting a legitimate national

[20] Paragraph 3 does make a vague reference to secret information 'as defined in the law', despite the fact that Article 4 of the Access to Information law gives a more specific definition of 'classified information' and 'personal information'.

[21] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1996, available at http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf

security interest.[22] For example, a legitimate national security interest does not include protecting a government from embarrassment or the exposure of wrongdoing.[23]

Furthermore, the Johannesburg Principles provide that no person may 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.[24] Finally, a person or organization may not be subject to such sanctions, restraints or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime.[25]

ARTICLE 19 is concerned that paragraphs 3 and 4 of Article 154-A of the Draft Bill fail short of meeting the Johannesburg Principles. In particular, the Draft Bill does not identify the precise nature of the threat (perceived or actual) from the obtainment or onward transmission of secret information, however this term is defined. Furthermore, the Draft Bill does not establish a direct and immediate connection between the onward expression and the threat, as required by international legal standards.[26] Information obtainment and/or disclosure[27] must be shown to harm or to be likely to harm national security interests if such obtainment or disclosure is to be met with criminal sanctions. The Draft Bill fails to expressly deal with the requirement for harm arising from either the "obtainment" or "publication ... transmission ... commercialization" of "secret information" (Article 154-A(4).

This analysis is also consistent with the UN Human Rights Committee's interpretation of Article 19 of the ICCPR. In its General Comment No. 34, the Committee said that

> [I]t is not compatible with [Article 19(3) ICCPR] to invoke...laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information."[28]

ARTICLE 19's analysis is also confirmed by reference to comparative legislation. For example, the US Computer Fraud and Abuse Act creates a separate offence of 'obtaining national security information.'[29] This offence punishes the act of obtaining national security information without, or in excess of, authorization and then wilfully providing or attempting to provide the information to an unauthorized recipient, or wilfully retaining the information. The offence defines national security information as

---

[22] Principle 1.2.

[23] Principle 2.b.

[24] Principle 15.

[25] Principle 24.

[26] Human Rights Committee, General Comment No. 34, para 35.

[27] I.e, the publication, commercialization or transmission to a third party (Article 154-A(4) of the Bill).

[28] General Comment No. 34, *supra note* 5, para 30.

[29] 18 USC §1030 (a) (1)

> [I]nformation that has been determined by the ... Government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defence or foreign relations...

The offence is punishable with a fine, up to ten years imprisonment, or both. The US offence thus defines the 'information' relevant to the section, explains what executive order is required to deem information to be in the "national security interestm" requires the use or retention of the information and commensurately increases the penalty for the offence. The offence also requires that the defendant has reason to believe that the national security information could be used to the injury of the United States or to the advantage of any foreign nation. Therefore, there is an additional element of knowledge factored into this offence, which better satisfies the need for a direct and immediate connection between the threat to national security and the retention or transmission of the information.

Recommendations:

- Article 154-A(3) and (4) of the Draft Bill should provide for proof of harm or the likelihood of harm as a constituent element of the offences

The lack of a public interest defence

ARTICLE 19 is concerned that the Draft Bill also fails to expressly include a public interest defence regarding the obtainment, publication or transmission of 'secret information.' In our view, this is a major weakness of the Bill. It is critical to the proper functioning of government that the broader public interest in the disclosure of information is considered. This public interest override is lacking in the Draft Bill, which is a necessary minimum human rights standard as enumerated in The Johannesburg Principles.

Recommendations:

- Article 154-A(3) and (4) should include an express public interest defence.

Penalties

The punishment for the offence in Article 154-A(3) of the Draft Bill is a minimum term of six months – and up to two years – imprisonment and a fine. It is not clear if these sanctions are to be read disjunctively, conjunctively or with the potential for both such interpretations.

Of more concern is that the minimum term of imprisonment and the level of the custodial sentences are disproportionate to the seriousness of the actual or potential harm caused by the obtainment or transmission of 'secret information'. A judge will be restricted at the sentencing stage in including a proper consideration of actual harm, likely harm, loss or other relevant mitigating circumstances.

Recommendations:

- Sentencing provisions in Article 154-A(3) and (4) of the Draft Bill should make it clear whether a fine is in addition – or an alternative – to imprisonment.
- Mandatory minimum sentences should be removed from Articles 154-A(3) and (4) of the Draft Bill.

Crimes against public officials

Paragraph 5 of Article 154-A of the Draft Bill provides that penalties are increased by one third up to one half if the offence (in any of its manifestations) is practised against public officials including the President, the President of the Federal Supreme Court and other senior managers of the direct and indirect federal, state, municipal or Federal District administration.

ARTICLE 19 notes, however, that the Human Rights Committee stated that laws

> [S]hould not provide for more severe penalties solely on the basis of the identity of the person that may have been impugned.[30]

Public figures, including those exercising the highest political authority, are legitimately subject of criticism and political opposition. It is foreseeable that the access to innocuous 'private electronic communications' of one of the identified public officials may result in similar harm to access to similar communications of a private individual. However, in the case of the public official, the same access would result in a much harsher criminal penalty. In ARTICLE 19's view, paragraph 5 of the Bill is therefore clearly incompatible with international standards on freedom of expression.

Recommendations:

- Delete Article 154-A(5) of the Draft Bill so that the law equally applies to all individuals.

The need for a complaint

Article 154-B provides as follows:

> The crimes defined in Article 154-A are only to be proceeded with [sic] using representation, unless the crime is committed against the direct or indirect public administration of any of the Powers of the Union, States, Federal District or Municipalities or against public service companies.

ARTICLE 19 welcomes the requirement in Article 154-B of the Draft Bill for a 'representation' or complaint to be made as a prerequisite for prosecution. However, the fact that this requirement is obsolete if the 'crime is committed against the direct or indirect public administration....' is unjustified. ARTICLE 19 repeats the analysis above regarding the need for proof of harm. The need for a complaint goes some way towards addressing this lacuna in the Bill (but not far enough) but there is no objective necessity to permit prosecution under different terms and circumstances for offences allegedly involving public officials.

Recommendation

- Article 154-B of the Draft Bill should include a requirement of a complaint or representation (in addition to proof of harm) in all cases of prosecution.

[30] *Ibid.*, para 38.