KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS ON BRAZIL'S PROPOSED LAW 84/99

November 7, 2011

Proposed Law 84/99, currently under review in the House of Representatives, aims to update the law of Brazil to address various kinds of criminal activity on the Internet. However, as currently drafted, the proposed law contains vague or undefined terms that could criminalize many kinds of ordinary conduct by Internet users. Also, the draft could impose unjustified liability on the providers of Internet services, thus unintentionally stifling innovation and openness and threatening privacy online. An effective cyber-crime law would only cover intentional acts and would target the authors of "malicious code," not the intermediaries that transmit it or unknowingly host it. Moreover, before adopting a cyber-crime law, policymakers in Brazil should establish a civil regulatory framework that addresses the roles and responsibilities of users, companies, and other institutions that use or provide access to the network.

We are honored to provide these comments on Brazil's Proposed Law (PL) 84/99, also known as the Azeredo Bill.[1] Our observations have three major themes:

First, we share with the experts at the Fundação Getulio Vargas (FGV)[2] the view that the proposed law would criminalize many kinds of ordinary conduct of computer users. This problem results from vague language in the proposal. In particular, several of the crimes in the proposal are based on actions that violate an "express access restriction," which is a term so broad that it could include the "terms of service" of websites or other online services. Criminalizing such conduct could violate the basic principle of proportionality.

Second, several of the criminal offenses are not limited by the principle of intentionality. In the computer crime area, defining offenses without regard to intentionality can result in the criminalization of innocent or normal conduct.

Third, the draft could create legal consequences not only for the enactor of illegal conduct, but also intermediaries, such as ISPs, hosts, or platforms for user-generated content. The proposal would do this by making it a crime to "transfer" data without authorization of the legitimate holder of access, or to "disseminate"

---

[1] This analysis is based on the text of the law included in the report of the Comissão de Constituição e Justiça e de Cidadania (CCJC), dated October 6, 2010, available at http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028.

[2] "Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL n. 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania," Fundação Getulio Vargas (7 November 2010) http://biblioteca.universia.net/html_bura/ficha/params/title/comentarios-sugest%C3%B5es-substitutivo-do-projeto-lei-crimes-eletr%C3%B4nicos-pl-n/id/52183408.html.

"malicious code" without any reference to intent or knowledge. These provisions could lead intermediaries, seeking to avoid punishment, to overblock or remove more user-generated content than may be necessary, thus threatening freedom of expression and privacy. The proposed legal framework could also stifle innovation, as it might discourage the development of new, unique platforms for content-sharing.

We offer the following concrete recommendations on how to address these concerns.

I. Using the COE Convention As a Model – Risks and Benefits

Congressman Azeredo has said that "the inspiration" for PL 84/99 is the Council of Europe's (COE) Convention on Cybercrime, sometimes referred to as the Budapest Convention.[3] The Convention, while an important model, must be relied upon only with great caution, for it uses overbroad or undefined language that can result in the criminalization of innocent conduct or conduct that should be addressed only by means of the civil code.[4] Even the official Explanatory Report for the Convention[5] warns of the risk of criminalizing ordinary and trivial conduct, stating in paragraph 38 that "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized." (While noting the problem, the Explanatory Report does not adequately describe how to avoid it.)

Moreover, in several cases, the language used in PL 84/99 directly contradicts the COE Convention or fails to incorporate limitations recommended in the Convention. Most importantly, under the Convention, all computer-related offenses must be committed *with intention* in order for those offenses to be criminalized. We recommend revising the bill to reflect the concept of intentional harm. In addition, we note that several criminal provisions in PL 84/99 have no counterpart in the COE Convention and thus do not benefit from even the limited guidance of the Convention and related materials.

---

[3] Eduardo Azeredo, "Cybercrime legislation in Brazil," Octopus Interface Conference – Cooperation against Cybercrime, Council of Europe, Strasbourg, France (June 11, 2007) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

[4] Various experts have warned that the language in the COE Convention defining cybercrimes is too vague and overbroad. See, for example, Abraham D. Sofaer, "Toward an International Convention on Cyber Security," http://media.hoover.org/sites/default/files/documents/0817999825_221.pdf ("The COE effort to generalize makes the categories of offenses relatively easy to comprehend, but may have created coverage on some issues that is undesirably broad.").

[5] Council of Europe, "Convention on Cybercrime: Explanatory Report," http://conventions.coe.int/treaty/en/reports/html/185.htm.

II. Comments on Specific Crimes as Defined in PL 84/99

A. Article 2 - Unauthorized Access

Article 2 of PL 84/99 proposes amending Title VIII of the Special Part of the Penal Code by adding a new Article 285-A that would make it a crime to "access – through breach of security – a computer network, communication device or computing system, that is protected by an express access restriction."

The phrase "breach of security" might indicate that the offense requires the circumvention of a technical control, and that might be an important element of defining a suitably narrow offense. However, the phrase "an express access restriction" is unclear and could be interpreted very broadly. In particular, we are concerned that it could be interpreted as a reference to the terms of service set by an ICT service provider. For example, Facebook expressly states in its terms of service that no one shall create an account on the site unless they are at least 13 years old. A twelve-year old who opens a Facebook account has violated that site's terms of service. Is she "breaching the security" of a site protected by "an express access restriction?" The answer is unclear under the proposal as currently drafted, leaving too much discretion to prosecutors.[6] The problem of potential over-inclusiveness is compounded by the lack of an intentionality requirement.

We also note that the heading for Article 285-A reads, "Unauthorized access to a computer network, communication device, or computing system." The concept of "unauthorized access," which suggests that accessing a system without authorization of its owner, does not appear in the Article itself. This could generate further confusion regarding what kind of conduct is intended to be defined as a criminal offense.[7]

Article 285-A should be revised using language that is clear and direct and that includes intent. In a November 2010 analysis provided to Brazil's Commission on the

---

[6] When the COE Convention was being drafted, it was criticized for failing to distinguish adequately between conduct that should be criminalized and conduct that, while violating contract or other laws, should not be criminalized. See "Comments of the Center for Democracy and Technology on the Council of Europe Draft 'Convention on Cyber-crime' (Draft No. 25)" (February 6, 2001), http://old.cdt.org/international/cybercrime/010206cdt.shtml. The Explanatory Report addressed the problem but failed to resolve it. For example, when the Report states, "Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is 'with right,'" it does nothing to clarify whether a website or service that requires an email address to create an account and that includes restrictive terms of service "permits free and open access by the public."

[7] This is a problem that arises under the cybercrime laws of other nations, including the United States. Orin Kerr, a leading scholar of cyberlaw and a former official in the U.S. Department of Justice, has criticized the use of the undefined phrases "access" and "without authorization" in the U.S. statute. See Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," NYU Law Review, vol. 78, no. 5, pp 1596-1668 (November 2003) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740. In a recent article, Professor Kerr argued that the use of the phrase "without authorization" and the possibility that it can include terms of service makes the U.S. law unconstitutional under the principle that criminal statutes must clearly define the conduct they criminalize. Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," Minnesota Law Review (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187.

Constitution, Justice, and Citizenship, FGV scholars recommend that the Article be re-written as follows: "[b]reak into a computer network, communication device or system without authorization of the owner in order to obtain unfair advantage." An alternative approach would be to follow the suggestion of the COE treaty itself, which states, "A Party may require that the offence be committed by infringing security measures, … ." Combining this with the suggestion of FGV, Article 285-A could be revised to read as follows: "To access – through intentional breach of a technical security control – a computer network, communication device or computing system without authorization of the owner."[8]

B. Article 2 - Obtaining or Transferring Data

Article 2 also proposes amending the Penal Code to add a new Article 285-B that would prohibit a person from "obtain[ing] or transfer[ing] data or information contained within computer networks, communication devices or informatics systems that are protected legally and by express access restrictions, without or in breach of authorization by the legitimate holder of access."

The terms "express access restriction" and "without or in breach of authorization" could have a variety of interpretations, and their use in the statute could criminalize ordinary conduct by computer users. Broadly speaking, the act of transferring any file or data from one device to another could be at risk of criminal liability under this law, if the owner or operator of the website or service has placed any restrictions on use of the service. In one example, the experts at FGV note that the transfer of (legally downloaded) music from an iPod to another device or service could be considered criminal under Article 285-B, as it would constitute a transfer of data from one system to another without the authorization of Apple. Many websites and online services, including social networking services and other consumer-oriented sites, have access restrictions (if only user name and password) and place limits on how data on those sites can be used. While transfers might constitute a violation of copyright law or of the terms of a contract, it is probably not sound public policy to criminalize them under this law.

The proposed new Article 285-B is the first of several provisions in PL 84/99 that could have the effect (which is probably unintended) of also subjecting Internet intermediaries such as ISPs to criminal liability for the misconduct of others. The proposal makes it a crime to "transfer" data without authorization of the legitimate holder of access. An ISP transfers messages with no knowledge of the contents of those messages and no knowledge of whether the authors of those messages have authorization from the legitimate holder of access to the data contained in those messages. Yet, the language making it a crime to "transfer" data without authorization of the legitimate holder could cover the actions of ISPs. It is impossible for ISPs to know what they are transferring and impossible for them to determine the authority of the sender of each message. For this reason, the law of the European Union, the United States, and other countries makes it

[8] The phrase "without authorization of the owner" is not sufficient by itself to define the crime, but it is necessary to include it here in order to make it clear that security testing conducted with the permission of the system owner is not a crime. See COE Convention, Explanatory Report, paragraph 47.

clear that ISPs and other technological intermediaries cannot be held liable when they are acting as mere conduits.

The FGV analysis recommends that this Article be removed from the bill. It could be replaced with a provision focused on the subject of Article 3 of the COE Convention, the intentional "interception without right, made by technical means, of non-public transmissions of computer data," if such interception is not already covered under Brazilian law on the privacy of electronic communications.

C. Article 3 - Disclosure or Misuse of Personal Data

Article 3 proposes amending the Penal Code to add a new Article 154-A that would make it a crime to "[d]isclose, use, sell or make available data and personal or corporate information contained in a computing system with a purpose different from that which justified its registration, except in cases specified by law or by express permission of the person to which it refers, or his/her legal representative." There is no similar provision in the COE Convention.

The Article should be revised so that the act must be committed with "intent to harm" or "intent to gain unfair advantage" in order to constitute a criminal offense. In its current form, the Article could criminalize the act of re-using an email distribution list for a purpose similar to (but different from) that which justified its creation. If an environmental NGO had compiled the email addresses of people interested in protecting endangered animals, and then sent an email regarding deforestation to the same group of people, would the NGO be at risk of criminal liability under this law? We recommend incorporating a stipulation of "intent to gain unfair advantage" into the article. It could also be stipulated that the act must bring harm to the victim(s).

D. Article 4 - Damage to Data

Article 4 of PL 84/99 proposes making it a crime to damage or destroy electronic data, by amending Penal Code Article 163 as follows (new wording in italics): "[t]o destroy, render useless or degrade things *or electronic data* of others." Under this Article, a person who accidentally deletes an electronic file or unintentionally passes on a virus that destroys data belonging to another person could be convicted of a criminal offense. At a minimum, the Article should be revised so that the act must be committed with intent or "intent to harm" in order to constitute a criminal offense. This is what is recommended under Article 4 of the COE Convention.

E. Article 5 - Insertion or Dissemination of Malicious Code

Article 5 proposes amending the Penal Code by adding a new Article 163-A, which would make it a crime to "insert or disseminate malicious code in a communication device, computer network, or informatics system." Under this Article, a person who unknowingly forwards an email containing a virus would receive the same penalty as a

person who did so with the intention of harming the computer or system to which the message was sent. In addition, the provision could apply to any ISP that "disseminated" malicious code without knowledge or intent. The Article should be revised so that the act must be committed with intent or "intent to harm" in order to constitute a criminal offense.

Article 12 suffers from a similar flaw, when it makes it a crime, without reference to knowledge or intent, to disseminate malicious code when the act threatens military administration. Finally, the meaning of "malicious code" is unclear. The only definition of the term appears in Article 16. The language used here is vague and could conceivably apply to innocent or normal conduct.

F. Article 6 - Fraud

Article 6 proposes amending Penal Code Article 171 to criminalize the "disseminat[ion], by any means, of malicious code in order to devastate, copy, alter, destroy, facilitate or allow unauthorized access to a computer network, communication device or computer system, in order to gain unfair economic advantage to the detriment of others."

Article 6 reflects greater linguistic clarity than some of the previous articles; while there is no explicit reference to "intent," the Article describes the agent as disseminating "malicious" code "in order to facilitate undue access to a computer network." If a person engages in an act "in order to" accomplish something, it could be argued that he or she engages in that act "with intent." Moreover, under the provision, a crime arises only if the conduct is undertaken "in order to gain unfair economic advantage to the detriment of others." This is a more limited provision; it may serve the same purpose as the proposed amendment to Article 163 and may make the amendment to Article 163 unnecessary.

G. Forgery of Electronic Documents

Articles 8 and 9 propose amending Penal Code Articles 297 and 298 to prohibit (new wording in italics): "forgery of public document *or electronic data*" and "forgery of private document *or electronic data*" respectively. The vague language used in these Articles could criminalize many ordinary uses of electronic data, including the citation or alteration of documents owned or issued by public universities or cultural centers.

We join the experts at FGV in recommending that these Articles be eliminated from the bill. Forgery is criminalized in Brazil's Penal Code; forgery of electronic documents should be penalized in equal fashion to forgery of non-electronic documents.

H. Article 19 - Child Pornography

Article 19 proposes amending the heading of Article 241 of Law nº 8069 (13 July 1990), which criminalizes child pornography, to read as follows:

> "To present, produce, sell, receive, supply, disclose, publish or store, by any means of communication, including global computer network or Internet, photos, images with pornography or explicit sexual scenes involving child or adolescent"

The absence of any reference to "intent" is particularly problematic in this context. Under this law, the recipient of an unsolicited email containing a pornographic image of a child could be subject to criminal charges. Moreover, an Internet hosting service that stored child pornography with no knowledge could be held liable under this provision. The provision should be rewritten to include the requirements of knowledge and intent. The comparable article in the COE Convention includes an intent standard.

I. Article 20 - Data Retention

Article 20 of PL 84/99 is one of the most troublesome provisions of the proposed law. It has several elements, including:

- Data retention: It would require ISPs and other Internet access providers to retain traffic data regarding all communications for a period of three years.
- Data disclosure upon request: It would require the companies to disclose such data to the police and the public prosecutor "upon request."
- Data preservation: It would require ISPs and other access providers to preserve immediately, after judicial request, other information requested by the investigation.
- Data disclosure without request: It would require a service provider to disclose to the police "information in its possession or that it is capable of obtaining, that contains evidence of a crime" occurring within its network.

Data retention mandates have proven very controversial around the world.[9] The EU has a data retention mandate, although the maximum time period it permits countries to impose is 24 months, and it allows Member States to adopt data retention time periods of as little as 6 months.[10] In a May 2011 report, the European Data Protection Supervisor was highly critical of the Data Retention Directive, concluding that it does not meet the requirements imposed by the rights to privacy and data protection established in the European Convention on Human Rights and the EU Charter of Fundamental

[9] See Lilian Mitrou, Communications Data Retention: A Pandora's Box for Rights and Liberties?" (November 16, 2007) http://www.ittoday.info/Articles/Communications_Data_Retention.pdf.

[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:NOT.

Rights.[11] Constitutional courts of Romania and Germany have found that the implementation of the Directive locally violated national constitutions.[12] The United States has no data retention mandate, although legislation has been proposed in the lower chamber of Congress to establish such a requirement.[13]

In contrast, data preservation, also addressed under Article 20 of PL 84/99, is far less controversial. Data preservation laws require ISPs and other service providers to "freeze" data upon receipt of a government request, so that the data is preserved while the government prepares the necessary documentation and obtains the necessary approval for compulsory disclosure. The U.S. has a data preservation law, and data preservation has been proposed in Europe as an alternative to data retention. The COE Convention recommends data preservation, not data retention.

A critical question posed by any data retention (or data preservation) mandate is what should be the standard for government access to the data that is retained. In the European Union, 11 states accompany their data retention law with a requirement that the data can be disclosed to the government only with a judicial order.[14] In this regard, Article 20 is clearly inadequate, for it states that the data should be made available to the police or the public prosecutor "upon request." A critical question is whether other provisions of Brazilian law require a judicial order for the disclosure of communications traffic data. If not, consideration should be given to establishing clear judicial controls on police and prosecutorial access to this information before any retention or preservation mandate is adopted.

Data retention, data preservation, and the disclosure of communications data to government officials implicate the privacy rights provided under international human rights agreements. The Inter-American Court of Human Rights has expressly held that the right to privacy protected under Article 11 of the American Convention applies to the types of data associated with the communication process addressed by Article 20 of PL

---

[11] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) (May 31, 2011) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf.

[12] Analysis of European Digital Rights (Dec 3, 2010) http://www.edri.org/files/Data_Retention_Conference_031210final.pdf.

[13] See CDT Policy Post, Data Retention (February 2, 2011) http://www.cdt.org/policy/data-retention.

[14] Report from the Commission to the Council and the European Parliament, "Evaluation report on the Data Retention Directive (Directive 2006/24/EC)" (April 18, 2011) http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

84/99.[15] Accordingly, any measure concerning the storage and disclosure of such data must be "precise and indicate the corresponding clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorized to request it, to order it, and to carry it out, and the procedures to be followed."[16] All those required details are lacking from the proposal.

In sum, the measures proposed in Article 20 could risk infringement on the right to privacy, as defined by Article 21 of Brazil's Civil Code[17] and Article 11 of the American Convention on Human Rights. Furthermore, the data retention mandate outlined in Item 1 would prove costly for ISPs, and the burden of this cost would ultimately be born by their customers. There is evidence that a similar data retention mandate in Europe has discouraged use of Internet services, an effect that could impede Brazil's efforts to take full advantage of the information society to support economic and human development.[18]

III. Conclusion

On a broad scale, the passage of this law would represent an abrupt change in course for Brazil's digital policy environment, which has been highly regarded internationally as one that supports and encourages sharing, openness, privacy and innovation in the digital arena.

We share with the experts at FGV the view that it would be unwise for Congress to approve this or any law on cybercrime before establishing a civil regulatory framework that addresses the roles and responsibilities of users, companies, and other institutions that use or provide access to the network. This is the aim of the Marco Civil da Internet. If there is to be a specific criminal code regarding Internet use, it should be composed after a civil code has been put into force and should only address crimes that are not already punishable under criminal law.

---

[15] Case of Escher et al. v. Brazil, Judgment of July 6, 2009, http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf, paragraph 114. Likewise, the European Court of Human Rights has repeatedly stated that the "mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8" (the European counterpart to Article 11 of the American Convention). With regard to telephone data in particular, the European Court of Human Rights, to which the Inter-American Court looks for precedent, has stated that "release of that information to the police without the consent of the subscriber also amounts [...] to an interference with a right guaranteed by Article 8." See the Opinion of the European Data Protection Supervisor, note 11 above, at paragraph 7.

[16] Case of Escher at al v. Brazil, at paragraph 131.

[17] Código Civil Brasileiro, "Art. 21. *A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma*. [Article 21. The private life of a natural person is inviolable, and a judge, at an applicant's request, should take the necessary steps to prevent or stop action contrary to this standard.]" http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm.

[18] Analysis of European Digital Rights (Dec 3, 2010) http://www.edri.org/files/Data_Retention_Conference_031210final.pdf.

The Center for Democracy and Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. As a civil liberties group with expertise in law, technology, and policy, CDT works to enhance free expression and privacy in communications technologies by finding practical and innovative solutions to public policy challenges while protecting civil liberties. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media. CDT is based in Washington, D.C.

For more information, contact Cynthia Wong, Director of CDT's Project on Global Internet Freedom, Cynthia@cdt.org, or Ellery Biddle, Program Associate, Ellery@cdt.org.