ARTICLE 19

Brazil: Civil Rights Framework for the Internet

July 2012

Legal analysis

Executive summary

In July 2012, ARTICLE 19 analysed the Civil Rights Framework for the Internet in Brazil (the 'Marco Civil'). In particular, we examined the compatibility of the Marco Civil against international and comparative standards for the protection of freedom of expression.

ARTICLE 19 supports the adoption of the Marco Civil since our analysis shows that, on the whole, it is a progressive piece of legislation with generally satisfactory safeguards for the protection of freedom of expression and the right to privacy on the Internet. In particular, we welcome the fact that Internet Service Providers may only be held liable for failing to comply with a court order requiring them to takedown or block access to third-party content. Similarly, we are pleased that internet users may only be identified and their communications data disclosed following a court order and this for limited purposes, namely criminal investigations and criminal proceedings. Finally, if the bill is adopted, Brazil will be one of the first countries to guarantee net neutrality in South America, an important step in securing internet freedom in the continent as a whole.

ARTICLE 19 urges the Government of Brazil and all stakeholders, including civil society organisations, to rally around the Marco Civil and to promote broader public understanding of its provisions before and after it has been enacted.

At the same time, there are a number of ways in which the Marco Civil could still be improved to be more fully in line with international standards for the protection of freedom of expression. ARTICLE 19 makes a number of key recommendations on how this could be achieved and hopes these will be incorporated to the final version of the law.

Key Recommendations

- Article 7 (5) should make it clear that the communications data of internet users may only be disclosed following a court order and *where necessary and proportionate* for the protection of limited interests, such as the investigation of serious crimes;
- Article 9, sole paragraph should be amended in order to set out more clearly that internet filtering or monitoring is not allowed *except where necessary for technical reasons related to maintaining network integrity*. Article 9 mentions that there should be no discrimination in Internet traffic, except for technical reasons/network management. That's basically preserving the network neutrality principle. This does not necessarily cover internet filtering and monitoring which is addressed in Article 9, sole paragraph. It is therefore important to re-emphasise that internet filtering or monitoring is only permissible for technical purposes (at least in this particular context, filtering is perfectly acceptable, for example, when it's user-controlled), otherwise it would remain too open for interpretation ('except in the circumstances provided by law').
- Article 11 (2) should clearly provide at the outset that the extension of data retention periods may only be granted by a court and where necessary and proportionate for a very limited range of purposes, such as national security or the investigation of serious criminal offences. Similarly, access to communications data should only be granted to a limited number of public authorities. Finally, Article 11 should provide for a cut off period beyond which it is no longer permitted to retain and store communications data.
- Article 10 (3) should be amended to clearly lay down the penalties for failing to comply with data protection requirements;
- Chapter IV should be amended to provide for more specific measures to protect net neutrality in line with the recommendations of the special mandates for freedom of expression.

Table of Contents

About 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 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 June 2012, ARTICLE 19 analysed the Civil Rights Framework for the Internet in Brazil (the 'Marco Civil'). In particular, we examined the compatibility of the Marco Civil against international and comparative standards for the protection of freedom of expression and the right to privacy.

The Marco Civil is an initiative from the Brazilian Ministry of Justice, in partnership with the Center for Technology and Society of the Getulio Vargas Foundation, to develop a collaborative process in which all the actors from Brazilian society could identify together the rights and responsibilities that should guide the use of the Internet in Brazil. ARTICLE 19 notes that the process, which resulted in the text of the law, is an example of the importance and the great potential of multi-stakeholder involvement in policy-making. This analysis is ARTICLE 19's contribution to this process.

ARTICLE 19 has extensive experience of working on freedom of expression issues in Brazil. With our regional office for South America based in São Paulo, ARTICLE 19 has campaigned for the protection of online speech. For example, in January 2012, we commented on the draft Cybercrime Law of Brazil.[1] ARTICLE 19 has also analysed several ICT laws, such as the laws in Bolivia,[2] Venezuela,[3] Iran[4], Pakistan[5] and Tunisia.[6] Therefore, we believe that we are particularly well-placed to assess the Marco Civil which forms part of the legal framework governing freedom of expression on the Internet in Brazil.

Our analysis shows that the Marco Civil is on the whole a progressive piece of legislation with generally satisfactory safeguards for the protection of freedom of expression and the right to privacy on the Internet. In particular, we welcome the fact that Internet Service can only be held liable for third party content if they fail to comply with a court order requiring them to remove or block access to such content. Similarly, we are pleased that internet users may only be identified and their communications data disclosed following a court order and this only for limited purposes, namely criminal investigations and criminal proceedings. Finally, if the bill is adopted, Brazil will be one of the first countries to guarantee net neutrality in South America, an important step in securing internet freedom in the continent as a whole.

---

[1] ARTICLE 19, analysis of the Draft Cybercrime Law of Brazil, Januray 2012; available at http://www.article19.org/resources.php/resource/2946/en/brazil:-draft-cybercrimes-law.

[2] ARTICLE 19, analysis of the Law on Information and Communication Technologies of Bolivia, February 2012; available at http://www.article19.org/resources.php/resource/2950/en/bolivia:-law-on-telecommunications-and-information-and-communication-technologies.

[3] ARTICLE 19, analysis of the Law on Social Responsibilities on Radio, Television and Electronic Media of the Bolivarian Republic of Venezuela, December 2011; available at http://www.article19.org/resources.php/resource/2894/en/venezuela:-law-on-social-responsibility-of-radio,-television-and-electronic-media

[4] ARTICLE 19, analysis of teh Computer Crimes Law of the Islamic Republic of Iran, January 2012; available at http://www.article19.org/azad-resources.php/resource/2921/en/islamic-republic-of-iran:-computer-crimes-law.

[5] ARTICLE 19, analysis of Pakistan

Telecommunications (Re-organisation) Act, 1996, January 2012; available at http://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf

[6] ARTICLE 19, analysis of the state of internet freedoms in Tunisia, March 2012; available at http://www.article19.org/resources.php/resource/3014/en/tunisia:-internet-regulation

Nonetheless, there are a number of ways in which the Marco Civil could still be improved to be more fully in line with international standards for the protection of freedom of expression. In particular, some provisions of the Marco Civil concerning data retention are too vague and fail to reflect the requirements of necessity and proportionality under international human rights law. More specific measures for the protection of net neutrality and access to the Internet would also be desirable.

ARTICLES 19 urges the Government of Brazil and all stakeholders, including civil society organisations, to rally around the Marco Civil and promote broader public understanding of its provisions before and after it has been enacted

The legal analysis is divided into two sections. The first section lays down applicable international standards on the protection of freedom of expression online. The next section sets out the positive features of the Marco Civil against those standards. It also identifies the ways in which the text of the Marco Civil could be further improved and sets out our key recommendations on how to bring it more closely in line with international standards for the protection of freedom of expression.

International standards on Internet Freedom

The rights to freedom of expression and information are 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 these rights, in particular in relation to the regulation of online content, the liability of Internet Service Providers (ISPs), surveillance and access to the Internet. These standards form the basis of our recommendations on how best to protect freedom of expression on the Internet in Brazil, which are set out in Section III below.

The protection of freedom of expression under international law

Universal Declaration on Human Rights

Article 19 of the Universal Declaration of Human Rights (UDHR)[7] 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.[8]

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.[9] Brazil ratified 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.

In September 2011, the UN Human Rights Committee ('HRC'), as treaty monitoring body for the ICCPR, issued General Comment No 34 in relation to Article 19.[10] 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 clarification of international law related to freedom of expression and access to information.[11] It is particularly instructive on a number of issues relative to freedom of expression on the Internet.

---

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

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

[9] 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)

[10] See, CCPR/C/GC/3 available at http://www2.ohchr.org/english/bodies/hrc/comments.htm.

[11] ARTICLE 19 statement on UN Human Rights Committee Comment No.34:

Importantly, General Comment No 34 states that Article 19 ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[12] In other words, the protection of freedom of expression applies online in the same way as it applies offline.

At the same time, General Comment No 34 requires States party to the ICCPR to consider the extent to which developments in information technology, such as Internet and mobile based electronic information dissemination systems, have dramatically changed communication practices around the world.[13] In particular, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[14]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their Joint Declaration on Freedom of Expression and the Internet of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[15] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary.[16] They also promote the use of self-regulation as an effective tool in redressing harmful speech.[17]

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

The American Convention on Human Rights

At the regional level, freedom of expression is protected under Article 13 of the American Convention on Human Rights (ACHR), which in its relevant parts reads as follows:

> Article 13 - Freedom of Thought and 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.

---

http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression

[12] UN Human Righs Committee General Comment No.34, para. 12.

[13] *Ibid.*, para. 17.

[14] *Ibid.*, para. 39.

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

[16] *Ibid.*

[17] *Ibid.*

> 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…

Brazil ratified the ACHR on 7 September 1992. It is therefore equally bound to comply with the requirements of Article 13 as interpreted by the Inter-American Court of Human Rights and in line with the recommendations of the Special Rapporteur for Freedom of Expression for the Organisation of American States (OAS).

As early as 1999, the OAS Special Rapporteur for freedom of expression stated that the protection of freedom of expression under Article 13 of the ACHR extends to freedom of expression online:

> The community of American states has explicitly recognized the protecting of the right of freedom of expression in the American Declaration of the Rights and Duties of Man and the American Convention on Human Rights. These instruments allow a broad interpretation of the scope of freedom of expression. Internet content is covered by Article 13 of the American Convention on Human Rights. The Rapporteur urges the member states to refrain from implementing any sort of regulation that would violate the terms of the Convention.[18]

More recently, in January 2012, the OAS Special Rapporteur and the UN Special Rapporteur on Freedom of Opinion and Expression renewed their call for a strong protection of free speech on the Internet. In particular, they recalled that

> [L]egislation regulating the Internet should take into account the special characteristics of the Internet as a unique and transformative tool that enables billions of individuals to exercise their right to freedom of thought and expression as well as a range of other human rights.[19]

As a state party to the ACHR, Brazil is therefore bound to ensure that its laws regulating freedom of expression on the Internet comply with the requirements of Article 13 of the ACHR and take into account the special features of the Internet.

Limitations on the Right to Freedom of Expression

International Covenant on Civil and Political Rights

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;

[18] See OAS Special Rapporteur on Freedom of Expression, Annual Report, Vol 3 (1999), available at: http://www.cidh.oas.org/annualrep/99eng/Volume3c.htm

[19] http://www.oas.org/en/iachr/expression/showarticle.asp?artID=880&IID=1

> (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.[20]

- *Provided by law:* Article 19(3) of the ICCPR requires that restrictions on the right to freedom of expression must be provided by law. In particular, the law must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[21] Ambiguous or overly broad restrictions on freedom of expression are therefore impermissible under Article 19(3).

- *Legitimate aim:* Interferences with the right to freedom of expression must pursue a legitimate 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.[22]. Similarly, a restriction on freedom of expression 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.

- *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 means that if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.

The same principles apply to electronic forms of communication or expression disseminated over the Internet. In particular, the UN Human Rights Committee has said in its General Comment No 34 that:

> 43. Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.[23]

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

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

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

[23] Concluding observations on the Syrian Arab Republic (CCPR/CO/84/SYR).

These principles echo the findings of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in a recent report dated 16 May 2011.[24]

American Convention on Human Rights

Under Article 13 of the ACHR, any restriction on the right to freedom of expression must meet the same three-part test as under the ICCPR, namely: (i) the restriction must be provided by law; (ii) the restriction must pursue a legitimate aim recognised under Article 13; and (iii) the restriction must be proportionate to the aim pursued.

In particular, it is worth noting that the OAS Special Rapporteur recently declared that:

> In considering both domestic legislation and international treaties such as the Anti-Counterfeiting Trade Agreement, States should recall that while freedom of expression may be limited in the pursuit of legitimate objectives such as the prevention of crime or the protection of the rights of others, such limitations should be narrowly tailored and interfere to the least extent possible with the right to freedom of expression. Any measure that affects speech on the Internet should be specifically designed to preserve the Internet's unique capacity to promote freedom of expression by facilitating the free exchange of information and ideas instantaneously and inexpensively regardless of frontiers.[25]

Role of Internet intermediaries and intermediary liability

Intermediaries, such as Internet Service Providers (ISPs), search engines, social media platforms and web hosts, play a crucial role in relation to access to the Internet and transmission of third party content. They have come to be seen as the gatekeepers of the Internet. For Internet activists, they are key enablers of the meaningful exercise of the right to freedom of expression, facilitating the free flow of information and ideas worldwide, while law enforcement agencies view them as central to any strategy to combat online criminal activity.

Given the huge amount of information that is available on the Internet, and that could potentially be unlawful, e.g. copyright law, defamation laws, hate speech laws, criminal laws for the protection of children against child pornography, Internet intermediaries have had a strong interest in seeking immunity from liability on the Internet.

In many western countries, Internet intermediaries have been granted immunity for third-party content.[26] They have also been exempted from monitoring content.[27] However, they have been

[24] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[25] See 2012 Joint Declaration with the UN Special Rapporteur on Freedom of Opinion and Expression, cited above at n 21.

[26] See for example, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the 'E-commerce directive' in the EU. See also the Communications Decency Act 1996 in the US, and in Singapore, the Electronic Transaction Act 2010 which gives strong protection to innocent providers.

[27] See Article 15 of the E-commerce directive. In the recent case of *SABAM v. Scarlet Extended SA,* the Court of Justice of the European Union (CJEU) considered that an injunction requiring an ISP to install a filtering system to make it absolutely impossible for its customers to send or receive files containing musical works using peer-to-peer software without the permission of the rights holders would oblige it to actively monitor all the data relating to each of its customers, which would be in breach of the right to privacy and the right to freedom to receive or impart information. The court noted that such an injunction could potentially undermine freedom of information since the

made subject to **'notice and take-down' procedures**, which require them to remove content once they are put on notice by private parties or law enforcement agencies that a particular content is unlawful. This system can be found for example in the E-commerce directive in the EU and the Digital Copyright Millennium Act 1998 (the so-called 'safe harbours') in the US.

A number of problems have been identified in relation to such 'notice and take-down' procedures. First, **they often lack a clear legal basis.** For example, a recent OSCE report on Freedom of Expression on the Internet highlights that:[28]

> Liability provisions for service providers are not always clear and complex notice and takedown provisions exist for content removal from the Internet within a number of participating States. Approximately 30 participating States have laws based on the EU E-Commerce Directive. However, the EU Directive provisions rather than aligning state level policies, created differences in interpretation during the national implementation process. These differences emerged once the provisions were applied by the national courts. Aware of such issues, the European Commission launched a consultation during 2010 on the interpretation of the intermediary liability provisions. A review report is expected during 2011.

Moreover, **these procedures lack fairness**: rather than obtain a court order requiring the ISP to remove unlawful material (which, in principle at least, would involve an independent judicial determination that the material is indeed unlawful), ISPs are required to act merely on the say-so of a private party or public body. This is problematic because intermediaries tend to err on the side of caution and take-down material which may be perfectly legitimate and lawful. As the UN Special Rapporteur on freedom of expression recently noted:[29]

> 42. [W]hile a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially illegal content. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences.

Accordingly, the four special rapporteurs on freedom of expression recommended in their 2011 Joint Declaration on Freedom of Expression and the Internet that:

> (i) No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information; [30]

---

suggested filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

[28] OSCE report, Freedom of Expression and the Internet, July 2011, p 30.

[29] See UN Special Rapporteur on Freedom of Expression report, cited above at n 26, para. 42.

[30] *Supra note* 17.

(ii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;[31]

(iii) ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[32]

Similarly, the UN Special Rapporteur on freedom of expression has stated that

> [C]ensorship measures should never be delegated to a private entity, and that no one should be held liable for content on the Internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf.[33]

He has further recommended that in order to avoid infringing the right to freedom of expression and the right to privacy, intermediaries should:[34]

> [O]nly implement restrictions to these rights after judicial intervention; be transparent to the user involved about measures taken, and where applicable to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and minimize the impact of restrictions strictly to the content involved.

Finally, the Special Rapporteur has emphasised the need for effective remedies for affected users, including the possibility of appeal through the procedures provided by the intermediary and by a competent judicial authority.[35]

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.

The right of private communications is strongly protected in international law through Article 17 of the ICCPR, which states that:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

In General Comment no. 16 on the right to privacy, the UN Human Rights Committee clarified that:

> 3. The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis

[31] *Ibid.*

[32] *Ibid.*

[33] See UN Special Rapporteur on FOE report, cited above at n 26, para. 43.

[34] *Ibi*d. para 47.

[35] *Ibid.*

> of law, which itself must comply with the provisions, aims and objectives of the Covenant.

The Committee went on to explain that:

> 4. The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

The Committee further stated that:

> 8. Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test: [36]

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

The Special Rapporteur further defined the scope of legitimate restrictions on the right to privacy as follows: [37]

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

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. In his report of 16 May 2011, the UN Special Rapporteur on Freedom of Opinion and Expression expressed his concerns that:

> 53. [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and, by undermining people's

[36] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.

[37] *Ibid.*, para. 21

> confidence and security on the Internet, impede the free flow of information and ideas online.

The UN Special Rapporteur on Freedom of Expression further noted that:

> 59. [T]he right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.

In particular, the Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[38]

Access to the Internet and network neutrality

Access to the Internet

The Internet has become a basic requirement for the exercise of freedom of expression. It is also necessary for the meaningful exercise of other rights and freedoms, such as freedom of assembly. States are therefore under a positive obligation to promote and facilitate access to the Internet. The UN Special Rapporteur on Freedom of Expression, Frank La Rue, thus recently stated:[39]

> Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States.

The Special Rapporteur recommended that States should draw up concrete policies involving all stakeholders with a view to ensuring universal access, i.e. make the Internet widely available, accessible and affordable to all segments of the population. In particular, he suggested that States should work in partnership with the private sector to ensure Internet connectivity in all inhabited localities, including in remote rural areas. He further noted that States could subsidise Internet services and low-cost hardware.

Similarly, the four special mandates on freedom of expression have articulated a number of principles in relation to access to the Internet in their 2011 Joint Declaration on Freedom of Expression and the Internet, which reads as follows:

> 6. Access to the Internet
> a. Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to

[38] *Ibid.*, para 84.

[39] See UN Special Rapporteur on Freedom of Expression report of 10 August 2011, available here: http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf

promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.

b. Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.

c. Denying individuals the right to access the Internet as a punishment is an extreme measure, which could be justified only where less restrictive measures are not available and where ordered by a court, taking into account the impact of this measure on the enjoyment of human rights.

d. Other measures which limit access to the Internet, such as imposing registration or other requirements on service providers, are not legitimate unless they conform to the test for restrictions on freedom of expression under international law.

e. States are under a positive obligation to facilitate universal access to the Internet. At a minimum, States should:

i. Put in place regulatory mechanisms – which could include pricing regimes, universal service requirements and licensing agreements – that foster greater access to the Internet, including for the poor and in 'last mile' rural areas.
ii. Provide direct support to facilitate access, including by establishing community-based ICT centres and other public access points.
iii. Promote adequate awareness about both how to use the Internet and the benefits it can bring, especially among the poor, children and the elderly, and isolated rural populations.
iv. Put in place special measures to ensure equitable access to the Internet for the disabled and for disadvantaged persons.

f. To implement the above, States should adopt detailed multi-year action plans for increasing access to the Internet which include clear and specific targets, as well as standards of transparency, public reporting and monitoring systems.

From a comparative perspective, it should also be noted that some western countries have expressly recognised a right of access to the Internet in their national legislation or otherwise. For example, the French Conseil constitutional declared that Internet access was a fundamental right in 2009. In Finland, a decree was passed in 2009 which provides that every Internet connection needs to have a speed of at least one Megabit per second. Access to the Internet has also recognised as a basic human right in Estonia since 2000.

Network neutrality

An important component of the right of access to the Internet is the principle of 'network neutrality' or 'net neutrality'. It protects the right of consumers to access the content, applications, services and hardware of their choice without restrictions by Internet Service Providers (ISPs) or governments.

The principle of net neutrality requires that all Internet traffic should be treated equally, i.e. without discrimination based on content, device, author, origin or destination of the content, service or application. This means that Internet Service Providers (ISPs) or governments should not be allowed to use their control over the infrastructure of the Internet or their market power to block content, or prioritise, or slow down access to certain applications or services, such as peer-to-peer transmission.

In other words, net neutrality is essential to preserve the infrastructure and the openness of the Internet. It is also essential for the sharing of information and ideas on the Internet as protected under international human rights law. For this reason, the four special rapporteurs on freedom of expression adopted a set of principles in relation to network neutrality in their 2011 Joint Declaration on Freedom of Expression and the Internet. In particular, they declared the following:[40]

> Network Neutrality
> a. There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application.
> b. Internet intermediaries should be required to be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.

The adoption of any net neutrality rules at domestic level should reflect these standards. In this regard, the recent Chilean law on network neutrality offers a positive example in that it provides fairly comprehensive safeguards against discriminatory practices by ISPs. [41]

In particular, it is important to ensure that there are sufficient safeguards against discrimination between different types of Internet services, such as fixed and mobile broadband. For example, ARTICLE 19 criticised the rules adopted by the US Federal Communications Commission in December 2010, as they failed to provide sufficient safeguards in that respect.[42] The European Union is currently considering the adoption of net neutrality rules.

[40] See 2011 Joint Declaration cited above at note 17.

[41] See http://www.subtel.gob.cl/prontus_subtel/site/artic/20100826/pags/20100826145847.html

[42] To read more about ARTICLE 19's concerns with the FCC rules, please go to: http://www.article19.org/resources.php/resource/2824/en/net-neutrality:-stronger-rules-needed-in-us-and-eu

Analysis of the Marco Civil

Positive aspects of the Marco Civil

ARTICLE 19 welcomes a number of positive features of the Marco Civil from the perspective of international standards for the protection of freedom of expression online. In particular, the Marco Civil contains positive measures in the area of intermediary liability, data protection and net neutrality.

General comments
At the outset, ARTICLE 19 welcomes the general manner in which the Marco Civil has been drafted, especially its first Chapter which contains the basic principles and values governing the use of the Internet in Brazil. In particular, we are pleased to see the following:

- human rights, pluralism, diversity and openness are clearly set out as the basic values underpinning the use of the Internet in Brazil (Article 2, Chapter 1);

- the guiding principles for the regulation of the Internet in Brazil include the right to freedom of expression as guaranteed by the Constitution, the right to privacy and net neutrality (Chapter 1, Article 3);

- the bill seeks to promote access to the Internet and access to information (Chapter 1, Article 4).

We also find it heartening that the rights of Internet users are put at the forefront of this bill. This is apparent from the fact that Chapter 2 reiterates that freedom of expression and the right to privacy are essential for the enjoyment by users of the right of access to the Internet (Article 8, Chapter 2).

Network neutrality – Chapter III, section 1
ARTICLE 19 welcomes section 1 of Chapter 3, which essentially guarantees the principle of net neutrality in Brazil. If the bill is adopted, Brazil will become the second country in Latin America to fully recognise this principle which is fundamental to safeguard the open Internet.

Right to privacy and data protection – Chapter III, section 2 and 4
ARTICLE 19 generally supports sections 2 and 4 of Chapter 3, which seek to protect the communications data and the information allowing the identification of internet users. In our view, section 4 provides a satisfactory procedure to protect the right to privacy of internet users, since communications data may only be disclosed following a court order and this for the protection of limited interests, namely criminal investigations and criminal proceedings. Moreover, under section 4, the onus is on the requesting party to provide evidence that unlawful activity has taken place and to prove that disclosure of the data is useful for the purposes of the investigation.

In addition, we note with approval that the retention of communications data for more than a year may only be authorised by a judge on application by law enforcement agencies, which is in line with the requirements of judicial oversight under Article 17 of the ICCPR and Article 11 of the ACHR.

Intermediary liability – Chapter III, section 3
ARTICLE 19 welcomes the fact that under section 3 of Chapter 3, Internet Service Providers (ISPs) are not liable for third-party content. Moreover, they are only required to take down or block access to third-party material following a court order. In other words, extrajudicial notice-and-takedown procedures are not required by law. Section 3 further requires that any such order should be content-specific. Section 3 is therefore in line with the recommendations of the special mandates on freedom of expression outlined in Section I of this report.

Access to the Internet – Chapter IV
In the main, ARTICLE 19 favours the measures which government authorities are required to promote under Chapter IV of the bill, in particular: the promotion of the interoperability of communications systems, the development of infrastructures that respect net neutrality and the openness of the Internet, digital skills training and greater access to the Internet, including in remote areas.

Proposal for improvements of the Marco Civil

ARTICLE 19 believes that the Marco Civil could be brought more closely in line with international and comparative law standards on the protection of freedom of expression and the right to privacy if the following recommendations were incorporated to its final version .

General Comments
ARTICLE 19 notes that Chapter III of the Marco Civil is concerned with "internet connection and applications" and contains four sections. Section 1 is entitled "data traffic" and essentially deals with net neutrality. Section 2 addresses data retention, while section 4 sets out the procedure for the disclosure of communications data. Section 3 deals with intermediary liability with third party content.

We query whether the structure and title of Chapter III, as well as the title of some of the sections in that chapter, are appropriate. In our view, the current structure and titles are confusing and would be best organised as follows:

- *First*, section 1 should be renamed 'network neutrality' as it would more firmly establish the recognition of this important principle. Moreover, it should form part of a separate chapter (e.g. Chapter III), bearing the same name, that would also include the measures contained in Article 19, Chapter IV which are closely connected with net neutrality.

- *Secondly*, sections 2 and 4 should be brought together under a separate chapter (e.g. Chapter 4) entitled 'data retention' that would cover the retention of communications data and applicable procedure for disclosure.

- *Thirdly*, section 3 which deals with intermediary liability should form part of a separate chapter (e.g. Chapter 5) as it concerns an issue that is substantially different from data retention.

Recommendations:
- Chapter III should be re-organised and renamed to reflect the different issues it seeks to address, including network neutrality, data retention and intermediary liability.

Users' rights and guarantees – Chapter II

As already noted, ARTICLE 19 generally welcomes the fact that users rights and guarantees have been put at the heart of the Marco Civil. We also welcome the fact that under Article 7 (5) of the Bill, consumers' internet communications may only be disclosed following a court order for limited purposes, namely criminal investigations and criminal procedures. However, in our view, this provision could be improved by using the language of Article 17 of the ICCPR (right to privacy), in particular the proportionality test. We believe that the right to privacy would be better protected if Article 7 (5) expressly stated that internet communications data must not be disclosed to third parties, except where authorised by a court and *in circumstances where it is necessary and proportionate* for the protection of limited interests, such as the investigation of serious crime. We note, however, that some of our concerns may be alleviated by the data protection bill, which is currently pending before Parliament.

We have two further minor comments. First, we believe that Article 8 which sets out the general rights and principles should precede Article 7 which sets out more specific rights connected with the right of access to the internet. Secondly, Article 7 provides that access to the Internet is essential to citizenship. While this may well be true, access to the Internet goes well beyond that. In particular, the UN Special Rapporteur recently highlighted that:[43]

> [A]ccess to the Internet is not only essential to enjoy the right to freedom of expression, but also other rights, such as the right to education, the right to freedom of association and assembly, the right to full participation in social, cultural and political life and the right to social and economic development.

We believe, therefore, that Article 7 should be amended to reflect the broader implications of access to the Internet for the exercise of other rights. In particular, the language of the UN Special Rapporteur cited above could be used.

Recommendation:

- Article 7 (5) should be amended to the effect that internet communications data must not be disclosed to third parties, except where authorised by a court and *in circumstances where it is necessary and proportionate* for the protection of limited interests, such as national security or the investigation of serious crimes.

Data retention – Chapter III

As the UN Special Rapporteur recently said "*The right to privacy is essential for individuals to express themselves freely*".[44] It is therefore vital that the provisions on the retention and access to communications data comply with the requirements of international human rights law.

ARTICLE 19 has three main concerns about the retention provisions in Chapter III of the Marco Civil. We note, however, that as with Chapter 2 above, some of those concerns may already be addressed in the Data Protection Bill currently pending before Parliament. We haven't had the benefit of analysing that Bill but it is clear to us that it should also reflect the principles which we have outlined in the first section of this analysis and avoid the flaws which we have identified in the Marco Civil as follows:

[43] *Supra note* 41, para. 61.

[44] *Supra note* 26, at para. 53.

- *First,* Article 9, sole paragraph, provides that the filtering and monitoring of the content of internet communications is not allowed "*except according to the provisions of the applicable legislation."* In our view, this is too vague and fails to comply with the requirement under Article 17 of the ICCPR that any restriction on the right to privacy must be provided by law. For example, Article 15 of the E-commerce directive clearly states that Internet Service Providers do not have a general obligation to monitor the information that goes through their networks with no exceptions. We understand, however, that the use of deep-packet-inspection may be necessary in certain circumstances for purely technical reasons related to maintaining network integrity, for instance. Therefore, we would recommend that Article 9, sole paragraph should be amended in order to set out more clearly the very limited circumstances in which such interference may be necessary.

- *Secondly,* we note that under Article 10 (3), providers may be subject to civil, criminal and administrative penalties for failure to comply with the requirement of non-disclosure of the communications data of their customers. While we welcome vigorous data protection laws, we are concerned that in this instance, the sanctions, which may be criminal, are not defined in the law in breach of the requirement of legal certainty under Article 17 of the ICCPR.

- *Thirdly,* Article 11 (2) allows law enforcement agencies or public authorities to apply for an extension of the data retention period, which under Article 11 (1) is '*at least one year'.* Article 11 (3) clarifies that the extension may only be authorised by a court. Article 13 (2) further appears to suggest that extension orders may only be granted in connection with 'specific facts' that relate to a 'given period'. ARTICLE 19 believes that Article 11 (2) should clarify at the outset that the extension of data retention periods may only be granted by a court. Furthermore, it should make clear that such order may only be granted where necessary and proportionate for a limited range of purposes, such as national security or the investigation of serious crime. Similarly, we believe that only a limited number of public authorities should be permitted to request access to communications data. In the UK, for example, there was a public outcry following the discovery that a local authority had used their communications data powers to spy on a family which had allegedly sent their children out-of-zone.[45] Finally, we believe that Article 11 should provide for a cut off date beyond which it is no longer permissible to retain communications data.

ARTICLE 19 has one further minor comment. Article 10 (2) places an obligation on providers to provide complete information about safety and non-disclosure measures. However, it is not clear to us whom this provision is intended to benefit. It appears that consumers would be the primary beneficiaries. In any event, it would be helpful if this could be more clearly spelled out in Article 10 (2).

Recommendations:

- Article 9, sole paragraph should be amended in order to set out more clearly that internet filtering or monitoring is not allowed *except where necessary for technical reasons related to maintaining network integrity*. Article 9 mentions that there should be no discrimination in Internet traffic, except for technical reasons/network management. That's basically preserving the network neutrality principle. This does not necessarily cover internet filtering and monitoring which is addressed in Article 9, sole paragraph. It is therefore important to re-emphasise that internet filtering or monitoring is only permissible for technical purposes (at least in this particular context, filtering is perfectly

[45] See JUSTICE, *Freedom from Suspicion,* September 2011, at 174.

acceptable, for example, when it's user-controlled), otherwise it would remain too open for interpretation ('except in the circumstances provided by law').

- The criminal, civil and administrative sanctions for failing to comply with the requirement of non-disclosure of communications data should be clearly spelled out;

- Article 11 (2) should make it clear at the outset that the extension of data retention periods may only be granted by a court and where necessary and proportionate for a limited range of purposes, such as national security or the investigation of serious crime. Similarly, access to communications data should only be granted to a limited number of public authorities. Finally, Article 11 should provide for a cut off period beyond which it is no longer permissible to retain communications data.

Action on the part of the authorities – Chapter IV

We have already noted above that Article 19 of Chapter IV would be better placed under a separate Chapter dealing with net neutrality. More generally, we find the title of Chapter IV unclear. If our recommendation about Article 19 is followed, we would respectfully suggest that Chapter IV should be renamed 'Universal access to the internet and digital literacy'.

In addition, we draw attention to the 2011 Joint Declaration on Freedom of Expression and the Internet, in which the four special mandates on freedom of expression outlined the types of measures required giving substance to the right of access to the Internet. In particular, they recommended:

> e. States are under a positive obligation to facilitate universal access to the Internet. At a minimum, States should:
>
> i. Put in place regulatory mechanisms – which could include pricing regimes, universal service requirements and licensing agreements – that foster greater access to the Internet, including for the poor and in 'last mile' rural areas.
>
> ii. Provide direct support to facilitate access, including by establishing community-based ICT centres and other public access points.
>
> iii. Promote adequate awareness about both how to use the Internet and the benefits it can bring, especially among the poor, children and the elderly, and isolated rural populations.
>
> iv. Put in place special measures to ensure equitable access to the Internet for the disabled and for disadvantaged persons.
>
> f. To implement the above, States should adopt detailed multi-year action plans for increasing access to the Internet which include clear and specific targets, as well as standards of transparency, public reporting and monitoring systems.

In this regard, we note that Article 22 of the Marco Civil could be further improved by providing for more detailed measures, such as pricing regimes or state subsidies for the development of the required infrastructure in rural areas. We recognise, however, that this may addressed in separate legislation dealing with the telecommunications or ICT sector.

Recommendation:

- Chapter IV should be renamed, for example, 'Universal access to the internet and digital literacy';
- The measures contained in Chapter IV could be more specific and include, for example, pricing regimes, universal service requirements.

Annex: Draft Marco Civil

BILL

Sets forth the principles, guarantees, rights and duties for the use of the Internet in Brazil

The NATIONAL CONGRESS hereby decrees:

"CHAPTER I

PRELIMINARY PROVISIONS

Art. No. 1 This Law establishes the principles, guarantees, rights and duties for the use of the Internet in Brazil and sets forth the directives for action to be taken by the Federal Government, the States, the Federal District and the Cities with regard to this issue.

Art. No. 2 The guidelines for the use of the Internet in Brazil have, as their underpinnings:

I - the recognition of the world-wide scale of the web;
II - human rights and citizenship on digital media;
III - pluralism and diversity;
IV - openness and cooperation; and
V - free enterprise, free competition and consumers' rights.

Art. No. 3 The regulations for the use of the Internet in Brazil are set forth according to the following principles:

I - guaranteed freedom of expression, communication and the right to speak one's mind, as enshrined in the Constitution.
II - protection of one's privacy;
III - protection of personal data, as set forth in the applicable legislation;
IV - ensuring and safeguarding the net's neutrality, according to the regulation in place;
V - safeguarding the web's stability, security and functionality through the use of technical resources in keeping with international standards, and by encouraging to the use of good practices.
VI - accountability on the part of the agents, according to their activities, according to the relevant legislation; and
VII - safeguarding the net's participatory nature.

Sole Paragraph: The principles herein set forth shall not exclude other principles called for in the nation's legal framework in connection with this issue, or in the international treaties in which the Federative Republic of Brazil is a signatory.

Art. No. 4 The regulations for the use of the Internet in Brazil have the following purposes:

I - to promote all of its citizens' right to access the Internet;
II - to promote access to information, knowledge and participation in the nation's cultural life in the handling of public-interest issues.
III - to promote innovation and encourage widespread application of new technologies and utilization and access modes; and

IV - to promote compliance with open technological standards that enable communication, accessibility and the interoperability among applications and databases.

Art. No. 5 For the purposes hereof, the following definitions shall apply:

I - Internet - the system comprising a set of logical protocols, structured in world-wide scale for public and unrestricted use, in order to make data communication available between terminals by means of a number of distinct nets;

II - Terminal - computer or any device that may be connected to the Internet;

III - Self-Contained System Administrator - natural person or legal entity that manages specific IP - Internet Protocol address blocks and the relevant self-contained switching system, propertly registered in the nation-wide entity in charge of entering and distributing IP addresses that are geographically associated to the Country;

IV - IP address - a code assigned to a net's terminal in order to allow its identification, established according to international parameters;

V - Internet connection - the enabling of a terminal to send and receive data packages through the Internet, by means of the assignment or the authentication of an IP address;

VI - connection record - a set of data associated to the date and time at which an Internet connection starts and ends, its duration and the IP address used by the terminal to send and receive the data packages;

VII - Internet applications - a set of functionalities that may be accessed by means of a terminal connected to the Internet; and

VIII - Internet application access records - a set of information associated to the date and time at which a given Internet application was used from a given IP address.

Art. No. 6 As far as this Law is concerned, the following issues will be taken into consideration, in addition to the Internet's underpinnings, principles and expected goals: its nature, the specific uses and customs, as well as its relevance for the enhancement of promotion of human, economic, social and cultural development.

"CHAPTER II
USERS' RIGHTS AND GUARANTEES

Art. No. 7 Access to the Internet is essential to citizenship. The user shall be entitled to the following rights:

I - Unassailability and secrecy of his/her communications through the Internet, except in case a warrant is issued, under the assumptions and in compliance with the procedures set forth by the legislation in place to meet the requirements of a criminal inquiry or criminal procedural ruling;

II - continuous internet connection except in case of debt in connection with its use;

III - maintenance of the quality agreed upon in terms of the Internet connection, in compliance with Article 9;

IV - clear and full information in services contracts, with specific agreement with regard to the protection of his/her personal data, connection records and

Internet application access records, as well as the net management practices that can affect the quality of the services offered; and
V - full commitment not to provide, to third parties, his/her internet connection records, except in case permission is granted or under the assumptions provided for in the applicable legislation.

Art. No. 8 The guarantee of the right to privacy and freedom of expression in communications is essential for the user to enjoy the right to access the internet to the full extent.

CHAPTER III
CONNECTION AND INTERNET APPLICATIONS PROVISION

Section I
Data Traffic

Art. No. 9 The individual in charge of transmission, routing or switching shall treat all data packages in the same manner, without distinction with regard to content, origin and destination, service, terminal or applicatory. No discrimination or degradation in traffic shall be allowed unless it is associated with the technical requirements for proper performance or the services, as per the applicable regulation.

Sole Paragraph: While providing Internet connection, free of charge or otherwise, no filtering, analyzing or monitoring of the data packages content is allowed, except according to the provisions of the applicable legislation.

Section II
Record-Keeping

Art. No. 10. The safekeeping and release of internet connection and internet application access records, in compliance herewith, shall be performed so as to protect the intimacy, private life, honor and image of whatever parties are directly or indirectly involved.

§ 1 The access provider in charge of such record-keeping shall only be required to release the data that allow the user's identification when a warrant is issued, in accordance with Section IV of this Chapter.
§ 2 The internet service provider shall provide full information on the safety and non-disclosure measures, in compliance with the standards set forth in the relevant regulations.
§ 3 Failure to comply with the non-disclosure requirement set forth in the header shall result in civil, criminal and administrative penalties according to the legislation in force.

Sub-Section I
Connection Record-Keeping

Art. No. 11. While providing internet service, the relevant self-contained system's administrator shall be required to keep connection records as a secret, in controlled and safe environment, for at least one year, in compliance with the regulation in force.

§ 1 The responsibility for connection record keeping shall not be assigned to third parties.

§ 2 The law enforcement agency or administrative authority may request, as a provisional remedy, the internet service record keeping for a length of time in excess to that set forth in the header.
§ 3 In the case mentioned in § 2, the requesting authority shall have a sixty-day timeframe, as of the the day of the request, to file for a warrant covering the access to the records described in the header.
§ 4 The internet service provider in charge of the record-keeping shall have a non-disclosure commitment with regard to the requirement called for in § 2, which shall no longer remain in force if the request for a warrant is not granted or if such request has not been filed within the timeframe set forth in § 3.

Sub-Section II
Record-Keeping With Regard to Internet Applications Access

Art. No. 12. Internet service providers, whether they operate free of charge or otherwise, are barred from keeping records regarding internet application access.

Art. No. 13 Internet service providers are allowed to keep records with regard to users' access, as long as the provisions in Article No. 7 are complied with.

§ 1 If the internet service provider chooses not to keep records on Internet applications access, this shall not entail any accountability with regard to damages resulting from the use of such services by third parties.
§ 2 A warrant may result in the obligation, on the part of the internet service provider, to keep, for a given timeframe, records on Internet application access, provided such records are in connection with specific facts in a given period. The disclosure of information shall take place in compliance with the provisions of Section IV hereof.
§ 3 Pursuant to the provisions of § 2, the relevant law-enforcement agency or administrative authority may require the record-keeping with regard to Internet applications, provided the procedure and the timeframes set forth in §§ 3 and 4 of Article No. 11 are complied with

Section III
Liability for Damages Resulting from Content Generated by Third Parties

Art. No. 14 The internet service provider shall not be liable for damages resulting from content generated by third parties.

Art. No. 15. Except for a legal provision stating otherwise, the Internet service provider may only be liable for damages resulting from content generated by third parties if, after having been served a specific warrant, it fails to take the steps required to render the content regarded as infringing unavailable, within the scope of its services and within the timeframe set forth.
Sole Paragraph: The warrant referred to in the header shall provide a clear and specific indication of the content regarded as infringing, so as to allow the unambiguous location of the material. Failure to comply with this requirement shall render the warrant null and void.

Art. No. 16. Whenever the internet applications provider has contact information regarding the user who is directly directly responsible for the content referred to in Article No. 15, the provider shall inform such user of the warrant's execution.

Section IV
Warrant for the Disclosure of Records

Art. No. 17. The plaintiff may, in order to acquire evidence in a civil or criminal action, in an incidental or autonomous capacity, request that the judge order the party in charge of the safekeeping to provide the connection records or the Internet application access records.

Sole Paragraph: Without prejudice to the remaining legal requirements, the request shall incorporate the following items. Failure to comply with this requirement may render it unacceptable.

I - evidence that the illegal action has taken place;
II - proof, based on reasonable cause, of the usefulness of the records requested, for the purpose of investigation and submission of evidence; and
III - timeframe to which the records are related.

Art. No. 18 The judge shall take the necessary steps in order to ensure the non-disclosure of the data received, as well as the preservation of the user's intimacy, private life, honor and image. He or she may determine that the case be held in camera. Such requirement may encompass the requests for the safekeeping of records.

CHAPTER IV
ACTION ON THE PART OF THE AUTHORITIES

Art. No. 19. the following items comprise the guidelines for the actions to be taken by the authorities, on the Federal, State, Federal District and Municipality level, for the Internet's development in Brazil:

I - establishment of transparent, cooperative and democratic stewardship procedures, with the participation of society, represented by all of its segments;
II - promotion of the rationalization and the technological interoperability of the government-related electronic services amongst the various branches and levels of government, in order to allow to the exchange of information and to ensure procedures are carried out swiftly;
III - promotion of the interoperability amongst a number of systems and terminals; this shall encompass the various levels of government and all segments of society;
IV - preferred use of open and free standard technologies and formats;
V - open and structured advertising and release of public data and information;
VI - net infrastructure enhancement, promoting technical quality, innovation and the release of Internet applications, causing no harm to their openness, neutrality and participatory character;
VII - development of action and programs of qualification for use of the Internet;
VIII - culture and citizenship promotion; and
IX - provision of public services to the citizenry in an integrated, efficient, simplified manner through a multitude of access channels. .

Art. No. 20. The Public Sector agencies' websites and gateways shall seek:

I - compatibility of the government-related electronic services with a number of terminals, operational systems and applications, for access;
II - accessibility to all interested individuals, regardless of their motor or physical, cognitive, cultural and social capabilities, taking into account the non-disclosure requirements and the legal and managerial constraints;
III - compatibility with both human reading and automated processing of information;
IV - user-friendly government-related electronic services; and
V - enhanced participation of society in public policy.

Art. No. 21. The discharge of the State's duties, enshrined in the Constitution, in providing education at all levels includes capacity building, integrated to other educational practical, for safe, thoughtful and responsible use of the Internet as tool to enhance citizenship, and to promote culture and technological development.

Art. No. 22. The public initiatives to enhance digital culture and promote the Internet as social tool must:

I - seek to do away with the digital divide;
II - seek to reduce inequality, especially between the Country's regions, with regard to access to information and communication technologies and their use; and
III - encourage production and disclosure of local content.

Art. No. 23. The State must, periodically, formulate and encourage studies and establish targets, strategies, plans and timeframes with regard to the use and development of the Internet in the Country.

CHAPTER V
FINAL PROVISIONS

Art. No. 24. The defense of the interests and rights established in this Law may be carried out in court, jointly or severally, according to the applicable legislation.

Art. No. 25. This Law shall come into force sixty days after the date of its publication.

Brasília: