

# PINHEIRO NETO ADVOGADOS

## SENATE BILL NO. 279/03: DETAILED RECORDS ON E-MAIL ACCOUNTS

### WRITTEN BY

Francisco Werneck Maranhão

associate in the corporate area coordinated by partner MVM at the Rio de Janeiro office of Pinheiro Neto Advogados

### OFFICES

R. Boa Vista, 254/280  
São Paulo SP  
01014-907 Brasil  
Tel. (55-11) 3247-8400  
Fax (55-11) 3247-8600

Av. Nilo Peçanha, 11  
Rio de Janeiro RJ  
20020-100 Brasil  
Tel. (55-21) 2506-1600  
Fax (55-21) 2506-1660

SCS, Quadra 1, Bloco I  
Brasília DF  
70304-900 Brasil  
Tel. (55-61) 312-9400  
Fax (55-61) 312-9444

www.pinheironeto.com.br  
pna@pinheironeto.com.br

This article was prepared as a source of information and debates only, and should not be construed as a legal opinion on any specific transaction or business.

© 2004. Pinheiro Neto Advogados. All rights reserved.

1. - In the wake of the torrid discussions over Internet governance recently held in Tunis at the World Summit on the Information Society, and amid the voting of the Data Retention Directive<sup>1</sup> by the European Parliament, a legislative bill proposed by the Brazilian Senate back in 2003 has attracted renewed media attention and divided the opinions of local experts.

2. - With the alleged objective of ‘avoiding the use of e-mail technology for criminal purposes’, Senate Bill No. 279 requires ‘e-mail service providers’ to keep a detailed record of the holders of e-mail accounts, which should include, in relation to individuals, their complete name, residential address, identity card number (along with date of issuance and issuing body) and the number of their enrollment with the Federal Revenue Office. Records of legal entities holding e-mail accounts shall include their complete name, complete address and number of enrollment with the Federal Revenue Office. The Bill sets forth a 90-day term within which all e-mail accounts have to be ‘regularized’ by the e-mail service providers, which are required to promptly cancel any e-mail accounts that remain irregular after this period.

3. - Under the proposed statute, e-mail service providers shall have an obligation to present to the competent authority, whenever so requested, the records on electronic communications carried-out by a given e-mail account within a given time-frame, which may retroact up to 10 years from the moment the records are requested. Records shall be sufficient to inform: (i) the addressee or recipient of the messages; (ii) the date and time the message was sent or received; and (iii) the identification of the computer that accessed the e-mail account

4. - It is further proposed in the Bill that e-mail service providers shall be liable for the veracity of the information contained in their records and that such service providers shall be subject to a fine of at least R\$10.000,00 in case they fail to comply with the provisions proposed

<sup>1</sup> *Directive on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services.*

in the Bill. Finally, the Bill sets forth that the National Telecommunications Agency – ANATEL, the local state regulator of telecommunications, shall be in charge of giving effect to its provisions.

5. - There are a number of aspects of Senate Bill No. 279 which in our view may be vulnerable to challenges. The 90-day period for regularization of e-mail accounts may be construed as too short given the amount of effort that internet service providers (ISPs) will have to devote to the mammoth task of updating or creating extended records in connection with all their e-mail accounts, and considering the immense loss of revenues they will be subject to in the event they are unable to successfully complete such task. By contrast, ten years may be deemed as a far too long period for a legal obligation applicable to an environment where technology is subject to dramatic changes within a very short period of time, specially when compared to the 2-year period for data retention as per the proposed European Parliament Data Retention Directive.

6. - Any liability for the veracity of the information they receive from e-mail account holders will no doubt be overly burdensome to ISPs, who would be exposed to a risk of difficult quantification and would thus be required to put in place strict and expensive procedures for the opening of new e-mail accounts (and regularization of old ones) so that they could check the veracity of the information they receive. In addition, it seems that the participation of ANATEL as the body in charge for giving effect to the provisions of Bill No. 279 would deserve a more profound debate on the role of ANATEL in an environment of converging technologies, considering that ISPs are currently not subject to regulation by ANATEL<sup>2</sup>.

7. - However, what appears to be of greater interest to the debate over Senate Bill No. 279 and a more pressing issue is the question of whether or not the proposed statute is conceived with the minimum elements that could allow it to fulfill its declared aim of avoiding the use of e-mail technology and the Internet for criminal purposes. In order to assess this issue, one has to review the different ways in which individuals may have access to e-mail and other forms of electronic communication.

8. - Registering with an ISP based in Brazil and thus subject to the laws enacted in this country is most certainly not the only way in which a Brazilian citizen (or a foreign citizen located in Brazilian territory for that matter) may have access to e-mail or other forms of electronic communications. At least two other alternatives exist and are available even to those ill-versed in information technology: (i) one may register with a foreign-based ISP and still have access to this ISP's e-mail account out of Brazil; or (ii) one may simply obtain an e-mail account from a foreign-based ISP that does not require registration and access such e-mail account through a 'webmail' service (e.g. Hotmail or Gmail). There are also a number of ways to ensure anonymity even if registration is required, such as the use of anonymous remailer services, in which original e-mails messages are retransmitted by ISPs through anonymous e-mail accounts for privacy purposes.

9. - The architecture of the Internet allows no necessary connection to be made between an e-mail address and a person and this potential for anonymity is indeed a problem for regulators and law enforcement. But the creation of a mandatory registration and record keeping system, the effects of

---

<sup>2</sup> *The provision of access to the Internet is deemed as a valued added service which falls outside the scope of authority of ANATEL, in accordance with Article 61 of Law No. 9,472 of July 16, 1997 – the General Telecommunications Law.*

which are irremediably limited to a given physical jurisdiction, is insufficient to tackle such anonymity problem to the extent that, in practice, such a system would not prevent individuals from having access to e-mail accounts without first being registered with an ISP based in the jurisdiction where such mandatory scheme is in force.

10. - In this regard, a parallel may be drawn between the registration and recording keeping scheme proposed under Senate Bill No. 279 and the restriction to strong encryption currently in force in the US. The opponents to the restriction to strong encryption argue that criminals will not comply with such restriction. On the contrary, they will take all available measures to secure their own communications (including illegal measures), while, thanks to the legal limitations on encryption, they will more easily prey on law-abiding individuals and business<sup>3</sup>.

11. - The same may be said of the scheme proposed under Senate Bill No. 279. It is clear that only well-intentioned individuals would voluntarily abide by the rules and limit their communications to registered and thus traceable e-mails. Criminals would almost certainly resort to measures (available to anyone with a degree of computer literacy) that can ensure that it would be virtually impossible for law enforcement agencies in the physical world, either in Brazil or elsewhere, to track them down and prosecute<sup>4</sup>. To be effective to combat crime in cyberspace, the measures advanced by the Bill would have to be supplemented by draconian measures such as (i) the mandatory identification not only of e-mail account holders but of all those who communicate, by requiring identification cards at cyber-café, public telephone booths, wireless spots and other forms of access to pre-paid services; and (ii) the banning of use of international communications services such as webmail (e.g. Hotmail and Gmail) and blocking the use of foreign-based Internet services providers.

12. - The proponents of Bill No. 279 argue that they propose the taking of a precautionary measure, one that would avoid the recurring situation where a 'lock is put in the door only after criminals have already broken into the house'. In our view, this statement shows not a virtue but a flaw of the proposed legal statute to the extent that it shows that the Bill seeks a solution for a problem that has not yet been properly identified. In these circumstances, it is possible that the costs of regulation (i.e. the increased costs of operation of ISPs which will be passed on to consumers) will exceed its benefits, given the clear limitations of the suggested registration and record-keeping scheme.

São Paulo, December 15, 2005

**PINHEIRO NETO ADVOGADOS**

---

<sup>3</sup> *'Any restriction on the use of cryptographic programs will be unenforceable in practice, since the basic mathematical and algorithmic methods for strong encryption are widely published and can easily be implemented in software by any person skilled in the art.'* In Strossen, N (2000) *'Cybercrimes v. Cyberliberties'* *International Review of Law Computers & Technology* 14(1):11-24.

<sup>4</sup> Murray, A and Scott, C (2002) *'Controlling the New Media: Hybrid Responses to New forms of Power'* *The Modern Law Review* 65(4):491-516.