NOTAS ACERCA DO DIREITO À PRIVACIDADE NA INTERNET: A PERSPECTIVA COMPARATIVA

Carlos Alberto Rohrmann*

INTRODUÇÃO

A. *O atual estágio da Internet e do comércio eletrônico: proteção aos dados e à privacidade do usuário.*
B. *Múltiplas propostas de proteção à privacidade online e a legislação brasileira pertinente*

PARTE UM – OS ESTADOS UNIDOS E A EUROPA

I – REVISÃO DO DIREITO NORTE-AMERICANO

A. *Definição de privacidade e da expectativa de privacidade*
B. *A proposta de solução legislativa: o COPA, o COPPA e as demais propostas de leis*
C. *O papel das entidades administrativas: DOC, FTC, FCC e SEC*

II – O MODELO EUROPEU E A PROPOSTA CANADENSE

A. *A diretiva da União Européia para proteção da privacidade online*
B. *A Proposta Canadense: utilização de assinaturas eletrônicas*
C. *O código dos programas é a lei da Internet? Criptografia e as demais soluções técnicas para a proteção da privacidade online*

PARTE DOIS – PRIVACIDADE *ONLINE* NO BRASIL

I – ANÁLISE DA REALIDADE DA INTERNET E DA PRIVACIDADE *ONLINE* NO BRASIL

A. *Realidade da Internet e do comércio eletrônico no Brasil: os aspectos técnicos e sociais*
B. *A proteção constitucional à privacidade e a Lei 9.296/96*

---

* Professor da Faculdade de Direito Milton Campos. **Bolsista da CAPES-Brasília Brasil** durante o Doutorado em Direito na Universidade da Califórnia em Berkeley. Master of Laws (UCLA). Mestre em Direito Comercial (UFMG). Bacharel em Direito (FDMC). Bacharel em Ciência da Computação (UFMG). Membro professor da *Computer Law Association*. Advogado. Meus sinceros agradecimentos aos seguintes professores: Prof. Laurent Mayali, grande incentivador deste trabalho, por sua leitura de uma versão incial deste artigo, Prof. Dr. Arthur José Almeida Diniz, Prof. Dr. Luiz Otávio Linhares Renault, Prof. Dr. Osmar Brina Corrêa-Lima, Prof. Dr. Wille Duarte Costa. Rendo meus agradecimentos a João Bosco Miquelão por sua valiosa ajuda durante o trabalho de pesquisa e redação deste artigo. Este artigo encontra-se disponível em formato "pdf" no *web site* do *Instituto Online para Direito e Informática*, em http://www.home.earthlink.net/~lcgems/Privacidade.pdf, julho de 2000.

C. *Projetos de lei no Congresso Brasileiro e demais perspectivas*

II – UM MODELO DE LEGISLAÇÃO PARA O BRASIL

A. *Qual a melhor solução: uma lei nova ou a auto-regulamentação?*
B. *Sugestão de Lei de Proteção à Privacidade Online*

CONCLUSÃO

INTRODUÇÃO

A. *O atual estágio da Internet e do comércio eletrônico: proteção aos dados e à privacidade do usuário na Internet*

O desenvolvimento da Internet ao longo da década de noventa causou muita especulação no meio jurídico quanto à aplicação das normas jurídicas existentes no "mundo físico" com vistas à efetiva regulamentação da rede. Os primeiros estudos datam da primeira metade da década de noventa e foram dominados pela tese de que a Internet seria "ingovernável."[1] Trata-se de uma corrente doutrinária que defendia a tese de que a Internet criaria uma jurisdição própria, separada. Ao longo daquela década, outras propostas teóricas surgiram nos Estados Unidos. Pode-se classificar as propostas de regulamentação da Internet em quatro grandes grupos: adoção de tratados internacionais, aplicação de leis nacionais, utilização de mecanismos meramente técnicos para o controle da Internet e a criação da Internet como uma jurisdição à parte (como se fora um Estado soberano). Este artigo filia-se à corrente que entende ser o direito de cada Estado o mais adequado para regular as relações humanas no meio virtual.

O surgimento do comércio eletrônico foi um ponto da maior relevância no sentido de se exigir uma maior e efetiva regulamentação da Internet. Dentre os inúmeros fatores

[1] Os professores David Post e David Johnson publicaram inúmeras obras defendendo a teoria de que a Internet faria surgir um novo direito "descentralizado". Maiores referências: POST, David, JOHNSON, David R. Law and Borders--The Rise of Law in Cyberspace. *48 Stan. L. Rev. 1367* (1996); POST, David, JOHNSON, David R. "Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems. *73 Chi.-Kent L. Rev. 1055* (1998) e POST, David, JOHNSON, David R. *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized Emergent Law, in Coordinating The Internet*. Brian Kahin & James H. Keller eds., 1997. Acerca do tópico específico da Internet como uma entidade soberana: WU, Timothy S. Cyberspace Sovereignty? – The Internet and the International System. *10 Harv. J.L. & Tech. 647* (1997).

que impulsionam o comércio eletrônico, a privacidade dos usuários e dos consumidores é um elemento crucial. Pesquisas apontam que, dentre as principais resistências apresentadas pelos consumidores que não utilizam o comércio eletrônico, o temor quanto à falta de privacidade é um dos mais sérios.[2]

No Brasil, a Internet terminou o ano de 1999 com quatro milhões e meio de pessoas ligadas à rede. Um total de 28% da população brasileira tem acesso ao computador, seja em casa, ou no trabalho e, deste total, 53% têm acesso à Internet. Das residências brasileiras, 7,4% têm computador e acesso à Internet via linha telefônica; todavia, da população que utiliza a Internet, 84% ainda não faziam compras pela rede.[3]

Entendemos que as preocupações com as fraudes e com a privacidade *online* são dois fatores que dificultam o desenvolvimento do comércio eletrônico no Brasil e que devem ser solucionados pelo direito brasileiro. Por privacidade *online*, entende-se a proteção dos dados pessoais que são disponibilizados *online*. Esses dados podem ser coletados do usuário através de perguntas realizadas por um determinado *site*, ou pior, podem ser coletados diretamente do computador do usuário, sem a sua autorização (e, muitas vezes, sem o seu menor conhecimento). Uma vez coletados, os dados podem ser utilizados por empresas privadas ou mesmo pelo governo, sem o devido conhecimento e autorização do usuário.

---

[2] Uma pesquisa realizada pela revista *Business Week* em março de 1998, aponta a privacidade das informações pessoais como o principal fator que mantém consumidores que não fazem uso do comércio eletrônico fora da Internet, conforme: Business Week/Harris Poll: Online Insecurity. *Business Week*, 16 de março de 1998, página 102.

[3] Estes dados foram retirados da sexta pesquisa IBOPE sobre a Internet. A pesquisa foi parcialmente divulgada pela imprensa (dados genéricos) como, por exemplo, pelo jornal Estado de Minas em seu *site* na Internet (http://www.estaminas.com.br/agora/20000330182508060876071.html) visitado em 30 de março de 2000. Tivemos acesso à totalidade da pesquisa que nos foi gentilmente remetida pelo IBOPE para fins exclusivamente acadêmicos e de pesquisa.

B. Múltiplas propostas de proteção à privacidade online e a legislação brasileira pertinente

O Brasil não dispõe hoje de legislação específica protetiva da privacidade *online* como a que este artigo trata. Todavia, não se pode deslembrar da Lei n. 9.296, de 1996, que trata da interceptação das comunicações telefônicas e de dados. Cuida-se de lei que protege a privacidade dos dados quando de sua transmissão, mas que, todavia, não regulamenta a coleta espontânea de dados de consumidores e sua posterior utilização. Assim sendo, em face da Lei 9.296/96, a análise do uso de dados pelo governo para fins de investigação criminal e instrução processual penal está fora do escopo de estudo deste artigo. O artigo da referida lei[4] que criminaliza a interceptação de dados será objeto de análise deste trabalho, na Parte 2, item IIB.

O presente trabalho realiza um estudo comparativo da legislação referente à proteção da privacidade *online* com vistas à elaboração de uma proposta de legislação adequada à realidade técnica, econômica e cultural do Brasil. Na primeira parte, o artigo analisa as propostas legislativas, administrativas e técnicas nos Estados Unidos, Europa e Canadá. A parte dois cuida do Brasil: uma retrospectiva da realidade da Internet no Brasil e uma proposta de lei que trata do tema em estudo.

Este artigo conclui que é possível aprender da experiência estrangeira (no caso, da proposta européia) quando da elaboração de uma lei que preencha a lacuna ora existente no Brasil no campo da privacidade *online*. Outra conclusão é que, por se tratar de um ambiente internacional, é desejável a uniformização dos princípios de privacidade *online*.

[4] Cuida-se do artigo 10 da Lei 9296/96, disponível, *online*, em <http://home.earthlink.net/~lcgems/Projetos2.htm>.

PARTE UM – OS ESTADOS UNIDOS E A EUROPA

I – REVISÃO DO DIREITO NORTE-AMERICANO

A. Definição de privacidade e da expectativa de privacidade

A Internet terminou a década de noventa como um dos maiores fenômenos da chamada "nova economia" nos Estados Unidos[5] e a privacidade na rede é tema intimamente ligado ao desenvolvimento do comércio eletrônico naquele país. A doutrina norte-americana é rica no que tange ao tema em análise. Durante mais de cinco anos, professores debateram o tema e inúmeras propostas acadêmicas foram apresentadas.[6]

---

[5] Quando da redação deste artigo, havia uma enorme dúvida quanto ao futuro da "nova economia". O índice NASDAQ despencara, caindo mais de 9% no dia 14 de abril de 2000, e acumulando perdas de mais de 25% no ano. Se o NASDAQ continuar caindo ao ritmo que vem apresentando, talvez o tema discutido no presente artigo fique precluso...

[6] Conforme: AGRE, Philip E., ROTENBERG, Marc. *Technology and Privacy: The New Landscape*. MIT Press, 1997; ATKINS, Bruce T. Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet? *1996 U. Ill. L. Rev. 1151*, 1996; BRODER, Elena N. (Net)workers' Rights: The NLRA and Employee Electronic Communications. *105 Yale L.J. 1639*, 1996; CARTER, Patricia I. Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"? *25 Wm. Mitchell L. Rev. 223*, 1999; CLARKE, Roger. Information Privacy on the Internet. *48 Telecommunication Journal of Australia 2*, Maio/Junho 1998 (Austrália); DECEW, Judith W. *Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, 1997; DREYER, Anthony. When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence. *64 Fordham L. Rev. 2285*, 1996; EFFROSS, Walter A. Piracy, Privacy, and Privatization: Fictional and Legal Approaches to the Elctronic Future of Cash. *46 Am. U. L. Rev. 961*, 1997; FREIWALD, Susan. Uncertain Privacy: Communication Attributes After the Digital Telephony Act. *69 S. Cal. L. Rev. 949*, 1996; GANTT, Larry O. Natt II. An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector. *8 Harv. J. Law and Tec. 345*, 1995; GARFINKEL, Simson. *Pretty Good Privacy*. O'Reilly and Associates, 1995; GURAK, Laura. *Persuasion and Privacy in Cyberspace: The Online Protests Over Lotus Marketplace and the Clipper Chip*. Yale University Press, 1997; HASH, Paul E., IBRAHIM, Christina M. E-Mail, Electronic Monitoring, and Employee Privacy. *37 S. Tex. L. Rev. 893*, 1996; KANG, Jerry. Information Privacy in Cyberspace Transactions. *50 Stanford L. Rev. 1193*, 1998 (o Professor Jerry Kang tem ampla experiência na área, por ter trabalhado diretamente com o tema para o governo dos Estados Unidos. Atualmente o Professor Kang leciona na Faculdade de Direito da Universidade da Califórnia em Los Angeles); MELL, Patricia. Seeking Shade in the Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness. *11 High Tech. Law J. 1*, 1996; RACKETT, Christina A. Telemedicine Today and Tomorrow: Why "Virtual" Privacy Is Not Enough. *25 Fordham Urb. L.J. 167*, 1997; ROTHFEDER, Jeffrey. *Privacy for Sale: How Computerization Has Made Everyone's*

O direito à privacidade é assunto da maior relevância para o público americano e pode ser definido como o "direito de ser deixado a sós", ou o "direito de permanecer anônimo."[7] Pode-se identificar as raízes do direito à privacidade na Quarta Emenda à Constituição norte-americana[8] que cuida de buscas para fins criminais, embora a própria Suprema Corte norte-americana já tenha afirmado que a referida Emenda não trata exclusivamente de um direito absoluto à privacidade.[9] A proteção à privacidade nos Estados Unidos depende da expectativa de privacidade que a pessoa tem em um determinado momento. Assim, por exemplo, quando a pessoa encontra-se em sua casa, a sua expectativa de privacidade é alta, ao passo que, quando se encontra no carro, essa expectativa é menor. Ocorre que a sociedade americana, baseada na doutrina do individualismo, tem uma grande expectativa de privacidade. Basicamente, o entendimento é que, se uma pessoa está na rua e não está fazendo nada suspeito, ela não é obrigada a identificar-se. O uso da Internet nos Estados Unidos reflete, claramente, como o consumidor norte-americano alimenta essa grande expectativa de proteção à privacidade.[10]

Private Life an Open Secret. Simon and Schuster, 1992; SCHWARTZ, Paul M., REIDENBERG, Joel R. *Data Privacy Law: A Study of U.S. Data Protection*. Michie Publishing, 1996; SKATOFF-GEE, Michelle. Changing Technologies and the Expectation of Privacy: A Modern Dilemma. *28 Loy. U. Chi. L.J. 189*, 1996; WELLBERY, Barbara S. On-Line Liability: Privacy Protection on the Information Superhighway. *11 St. John's J.L. Comm. 659*, 1996.

[7] Uma importante conferência *online* sobre o tema que contou com a participação de Daniel Weitzner, dentre outros, foi realizada pelo MIT e ainda se encontra disponível na Internet, trata-se de MIT, *Anonymity: Should the Lcs Anonymous Remailer be Shut Down?* (http://www.lcs.mit.edu/anniv/speakers/presentation?id=041399-15), página visitada em 14 de abril de 2000.

[8] Quarta Emenda: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

[9] *Charles Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507: "Fourth Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all."

[10] Uma vez que o americano sai à rua sem temer que a polícia pergunte se está levando consigo o seu documento de identidade, presume-se que ele também saia com um escudo psicológico de privacidade.

A Suprema Corte entendeu, ainda, em 1973, que o direito à privacidade abrange o direito de a pessoa fazer escolhas significativas para sua vida sem a interferência de terceiros (inclusive o direito de a mulher decidir se vai fazer aborto ou não).[11] Como corolário dessa decisão, a pessoa tem o direito de decidir o fluxo a ser tomado por seus dados pessoais[12] (e, conseqüentemente, por suas informações[13]). É exatamente neste momento que a Internet começa a trazer problemas: como impedir que dados sejam coletados sem a autorização do usuário ou, ainda, como evitar o abuso da boa-fé do usuário, que descortina os seus dados em um determinado negócio virtual (no seu cadastro como cliente *online*, por exemplo), na ilusão de que eles não serão usados pelo dono do *site* em aplicações futuras não relacionadas com aquela determinada operação comercial?

B. *A proposta de solução legislativa: o COPA, COPPA e as demais propostas de leis*

Não se preocupa, por exemplo, em estar vestido dessa ou daquela forma (ao contrário de nós mineiros, sempre tão preocupados com a chamada "roupa de missa" dos domingos) ao sair do seu âmbito privado para o público. Esse comportamento está muito presente na Internet. O americano pode fazer compras nas lojas virtuais, sem sair de casa, usando seu pijama. Obviamente, a expectativa de privacidade é cada vez maior: pode-se comprar um carro em casa, à noite, antes de ir dormir.

[11] *Roe v. Wade*, 410 U.S. 113, 93 S.Ct. 705: "Right of personal privacy or a guarantee of certain areas or zones of privacy does exist under Constitution, and only personal rights that can be deemed fundamental or implicit in the concept of ordered liberty are included in this guarantee of personal privacy; the right has some extension to activities relating to marriage." Esse caso reconheceu a legalidade do aborto nos Estados Unidos: "Constitutional right of privacy is broad enough to encompass woman's decision whether or not to terminate her pregnancy."

[12] Conforme magistério do Prof. KANG, obra citada, *supra*, nota 3: "Finally, the third cluster of privacy concerns the flow of personal information. More precisely, information privacy concerns an individual's control over the processing--i.e., the acquisition, disclosure, and use--of personal information. In this third cluster, the paradigmatic privacy violation does not occur, for instance, when the state places an undue burden on some significant decision. Rather, this strand of privacy is invaded when, for example, someone obtains sensitive medical data by rifling through confidential files without permission."

[13] É muito interessante ressaltar que a questão aqui em foco tem implicações multifacetadas, abrangendo até mesmo a privacidade genética. Trata-se de tema que foge ao escopo deste artigo mas que é objeto de importantes pesquisas no campo jurídico: GREELY, Henry T. et al. Respecting Genetic Privacy. *40 Jurimetrics 153*, Winter 2000.

A primeira manifestação legislativa nos Estados Unidos que protegeu a privacidade *online* preocupou-se com a coleta de dados de crianças que, inocentemente, navegam pela rede. Trata-se do *Child Online Protection Act*[14] (COPA) que determina que dados coletados por *sites* do comércio eletrônico de material danoso para menores não podem ser divulgados para terceiros.[15] Uma vez que o COPA tratava, basicamente, de evitar o acesso de menores de 17 anos a conteúdo indecente na rede, e tal disposição legal acabava por impedir o acesso de adultos a material de conteúdo pornográfico, uma liminar foi concedida reconhecendo a inconstitucionalidade dessa barreira jurídica.[16]

Dentro do COPA encontra-se o *Children's Online Privacy Protection Act of 1998* (COPPA)[17]. Basicamente o COPPA torna ilegal a coleta de dados de menores de 13 anos sem a devida autorização do pai (ou do maior responsável).[18]

Temos, ainda, nos Estados Unidos, o *Electronic Communications Privacy Act* de 1986 (ECPA)[19] que proíbe a interceptação e divulgação de dados armazenados durante comunicação de dados. Trata-se de lei análoga à nossa lei brasileira de número 9.296 de 1996.

---

[14] Trata-se do 47 U.S.C. 231, que entrou em vigor em 29 de novembro de 1998. Esta lei foi aprovada pelo Congresso Norte-Americano como resposta à decisão da Suprema Corte que julgou inconstitucional o *Communications Decency Act* de 1996 que tentava varrer a indecência para fora da Internet.

[15] Conforme a seção 231 do COPA: "(d) Privacy Protection Requirements.-- (1) Disclosure of information limited.--A person making a communication described in subsection (a)-- (A) shall not disclose any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older without the prior written or electronic consent of-- (i) the individual concerned, if the individual is an adult; or (ii) the individual's parent or guardian, if the individual is under 17 years of age."

[16] Trata-se da decisão interlocutória proferida em 1º de fevereiro de 1999, na ação ACLU v. Reno, *civil action number 98-5591, in the United States district court for the Eastern District of Pennsylvania.*

[17] "Children's Online Privacy Protection Act of 1998": H.R. 4328 - Omnibus Appropriations Bill - Title XIII--Children's Online Privacy Protection, seção 1301, diponível *online* em <http://www.gseis.ucla.edu/iclp/coppa.htm>, visitado em 21 de abril de 2000.

[18] Id., seção 1303.

[19] Codificado como 18 U.S.C. §§ 2510-2522.

Em face da iniciativa européia que será objeto de análise deste artigo, os Estados Unidos estão também à busca de um estatuto legal protetivo dos dados pessoais na rede. Alguns projetos de lei tramitam no Congresso dos Estados Unidos[20], destacando-se, dentre eles, o *Online Privacy Protection Act*[21] que torna ilegal para um operador de *web site* coletar dados pessoais sem observar determinados preceitos, dentre os quais: apresentar notícia de que dados serão coletados; colher, de forma simples e sem maiores complicações, a aprovação do usuário quanto à coleta de seus dados; manutenção de procedimentos que protejam a integridade e o sigilo dos dados coletados.[22] Pode-se

---

[20] Os projetos de lei podem ser pesquisados e encontrados *online* em <http://thomas.loc.gov/cgi-bin/query> visitado em 14 de abril de 2000, dentre os projetos pertinentes ao tema, pode-se elencar o seguinte grupo como relevante: *Online Privacy Protection Act of 1999* (apresentado no Senado)[S.809.IS]; *Electronic Privacy Bill of Rights Act of 1999* (apresentado na Câmara)[H.R.3321.IH]; *Electronic Rights for the 21st Century Act* (apresentado no Senado)[S.854.IS]; *Secure Online Communication Enforcement Act of 2000* (apresentado na Câmara)[H.R.3770.IH]; *Secure Online Communication Enforcement Act of 2000* (apresentado no Senado)[S.2063.IS] e o *Collections of Information Antipiracy Act* (apresentado na Câmara)[H.R.354.RH].

[21] Trata-se do *Online Privacy Protection Act of 2000* (Apresentado na Câmara)[H.R.3560.IH].

[22] Conforme a seção 2 do *Online Privacy Protection Act*:

SEC. 2. REGULATION OF UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN CONNECTION WITH THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION.

(a) Acts Prohibited–

(1) IN GENERAL– It is unlawful for an operator of a Web site or online service to collect, use or disclose personal information in a manner that violates the regulations prescribed under subsection (b).

(2) DISCLOSURE– Notwithstanding paragraph (1), neither an operator of a Web site or online service nor the operator's agent shall be held to be liable under this Act for any disclosure made in good faith and following reasonable procedures in responding to a request under subsection (b)(1)(B) by an individual for disclosure of personal information pertaining to such individual.

(b) Regulations–

(1) IN GENERAL– Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate under section 553 of title 5, United States Code, regulations that—

(A) require the operator of any Web site or online service—

(i) to provide notice on its Web site, in a clear and conspicuous manner, of the identity of the operator, what personal information is collected by the operator, how the operator uses such information, and what information may be shared with other companies; and

(ii) to provide a meaningful and simple online process for individuals to consent to or limit the disclosure of personal information for purposes unrelated to those for which such information was obtained or described in the notice under clause (i);

(B) require the operator to provide, upon request of an individual under this subparagraph who has provided personal information to that Web site or online service, upon proper identification—

(i) a description of the specific types of personal information collected by that operator that was sold or transferred to an external company; and

(ii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the individual to obtain the personal information described in paragraph (i) from such individual; and

concluir que essas medidas são importantes e devem ser observadas quando da nossa elaboração de um proposta de regulamentação para o Brasil.

C. *O papel das entidades administrativas: DOC, FTC, FCC e SEC*

Enquanto uma lei não regulamenta de forma mais clara a proteção à privacidade dos usuários da Internet nos Estados Unidos, algumas entidades administrativas estão desempenhando tal papel. Dentre elas, destacam-se a *Federal Trade Comission* (FTC), *Securities Exchange Comission*[23] (SEC), a *Federal Comunnications Commission* (FCC) e o Departamento de Comércio (DOC). Destas quatro, sem dúvida, a FTC, não só por ser a mais ativa, mas também por ser a que lida diretamente com a proteção do consumidor nos Estados Unidos, é a que merece especial atenção deste trabalho.

Um princípio básico – notícia - orienta a atuação da FTC na proteção da privacidade *online*, ou seja, o usuário deve ser amplamente informado pelo *site* acerca de quais dados seus serão coletados. A atuação da FTC tornou-se mais agressiva a partir de junho de 1998, quando a FTC publicou um relatório sobre a privacidade *online* para o Congresso Norte-Americano.[24] Segundo esse documento, 92% dos *web sites* coletam dados pessoais e 86% deles não deixam claro que estão coletando tais dados.[25] Mantendo a política segundo a qual o consumidor estaria sendo lesado quando *web sites* coletassem

---

(C) require the operator of such Web site or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information it collects (...)

[23] Maiores referências específicas são escontradas *online* em <http://www.sec.gov/enforce/intrela.htm>, visitada em 02 de abril de 2000.

[24] FEDERAL TRADE COMMISSION, *Privacy Online: A Report to Congress*, junho de 1998, documento elaborado por Martha K. Landesberg, Toby Milgrom Levin, Caroline G. Curtin e Ori Lev. Posteriormente, a FTC ainda publicou o *Children's Online Privacy Protection Rule*, disponível *online* em <http://www.ftc.gov/os/1999/9907/childprivacyfrn.htm>.

[25] Id., páginas 23 e 24.

dados sem sua autorização, o FTC ajuizou, em 1999, sua primeira ação referente à privacidade na Internet. O provedor norte-americano, *Geo-Cities*, era o réu na ação e as partes chegaram a um acordo em que o provedor-réu comprometia-se a publicar, claramente, em suas páginas na Internet, quais informações pessoais seriam coletadas e para que propósitos.[26]

Ainda em 1999, o Departamento de Comércio dos Estados Unidos publicou o documento *International Safe Harbor Privacy Principles*, apresentando um conjunto de sete princípios como sendo aqueles que deviam ser observados quando da proteção internacional da privacidade *online*. São eles: notícia (de que o *site* vai coletar dados); escolha (o usuário é quem decide se vai ou não permitir a coleta de dados); transferência autorizada (o *web site* que coleta os dados só pode repassá-los a terceiros com a devida autorização do usuário); segurança (precauções razoáveis para prevenir a perda de dados de terceiros); integridade (evitar que os dados sejam adulterados); acesso (o usuário deve ter pleno acesso aos seus dados) e o estabelecimento de mecanismos que permitam a efetiva fiscalização e o cumprimento dos seis princípios pelos diversos *sites*.[27]

É interessante ressaltar que a União Européia aceitou os sete princípios acima como compatíveis com sua "Diretiva de Privacidade de Dados" a ser estudada por este

---

[26] Conforme o acordo publicado em: *40. Geocities, Docket No. C-3849 (final consent Feb. 12, 1999):* "GeoCities, one of the most popular sites on the World Wide Web, agreed to settle Federal Trade Commission charges that it misrepresented the purposes for which it was collecting personal identifying information from children and adults, in the first FTC case involving Internet privacy. Under the settlement, GeoCities has agreed to post on its site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, GeoCities also will have to obtain parental consent before collecting information from children 12 and under." Disponível em <http://www.ftc.gov/opa/1998/9808/geocitie.htm> e <http://www.ftc.gov/opa/1999/9902/petapp4.99.htm>, visitados em 15 de março de 2000.

[27] Trata-se do *International Safe Harbor Privacy Principles*, publicado pelo *Department of Commerce* dos Estados Unidos. Há uma versão disponível no Internet em: <http://www.ita.doc.gov/ecom/shprin.html>, visitada em 25 de outubro de 1999.

artigo a seguir.[28] Nota-se uma convergência de princípios na comunidade internacional que podem ser observados pelo Brasil quando da elaboração de sua legislação.

II – O MODELO EUROPEU E A PROPOSTA CANADENSE

A. *A diretiva da União Européia para proteção da privacidade online*

Apesar de a Europa não apresentar o mesmo volume de utilização da Internet encontrado nos Estados Unidos[29], é inegável que a União Européia teve a melhor iniciativa referente à proteção da privacidade na Internet, tanto que forçou os Estados Unidos a agirem no sentido de compatibilizarem a sua posição legal com ela. Embora os sete princípios básicos já tenham sido apresentados no item anterior, quando da análise do *International Safe Harbor Privacy Principles*, é interessante analisar o documento europeu, dada não só a sua importância histórica, como também a sua aplicabilidade prática quando, por exemplo, um determinado *site* brasileiro atua voltado para os clientes eletrônicos europeus.

---

[28] Conforme INTERNET LAW. *EC Approves U.S. Safe Harbor Principles as Consistent with EU Data Privacy Rule*: "The European Commission gave formal approval March 29 to a set of U.S. "Safe Harbor Principles" as an adequate, if not equivalent, form of personal data protection that meets the requirements of Directive 95/46/EC, the European Union's Data Protection Directive." Disponível *online* em <http://internetlaw.pf.com/subscribers/html/Recent.asp?target=NEWS0430>, visitado em 14 de abril de 2000.

[29] No dia 12 de abril de 2000, o primeiro ministro britânico Tony Blair lançou um programa visando tornar a Inglaterra o centro do comércio eletrônico mundial. É difícil saber se ele terá sucesso pois, até aquele dia, o Vale do Silício, ao sul de São Francisco na Califórnia, continuava sendo o líder mundial em concentração de empresas de informática e de comércio eletrônico.

A extensa diretiva européia "95/46/EC"[30], datada de 24 de outubro de 1998, começa com uma definição clara: o direito à privacidade relativo ao processamento de dados pessoais é um direito fundamental da pessoa natural que deve ser protegido pelos Estados europeus.[31] Duas outras importantes definições dizem respeito aos conceitos de "dados pessoais" e "processamento de dados pessoais", respectivamente definidos pela diretiva européia: "dados pessoais significam qualquer informação relacionada a uma pessoa natural identificada ou identificável" e "processamento de dados pessoais significa qualquer operação ou conjunto de operações que são realizados, utilizando dados pessoais".[32]

Uma diferença importante entre os modelos europeu e americano reside na proibição encontrada na diretiva européia no tocante ao processamento de dados que revelam origens étnicas ou raciais, opiniões políticas, convicções religiosas ou filosóficas, vida sexual ou saúde das pessoas.[33] A diretiva somente permite tal processamento quando há o consentimento específico, e no caso de o Estado europeu não proibir consentimentos para aquele tipo especial de processamento de dados (como

[30] European Union and the Council of the European Union Directive 95/46/EC, disponível *online* em <http://internetlaw.pf.com/subscribers/html/Recent.asp?target=NEWS0430>, visitada em 15 de abril de 2000.

[31] Id., capítulo I, artigo 1° - Objetivo da Diretiva: "*In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*"

[32] Id., capítulo I, artigo 2, letra (a): "Article 2- Definitions - For the purposes of this Directive: (a) 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); (b) 'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data (...)"

[33] Id., seção III, artigo 8° (1): "*SECTION III - SPECIAL CATEGORIES OF PROCESSING - Article 8 - The processing of special categories of data 1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.*"

ocorre, por exemplo, na Alemanha, que proíbe manifestações políticas referentes ao nazismo).[34]

Esta última característica do modelo europeu dificilmente seria validada nos Estados Unidos, dada a Primeira Emenda à Constituição Norte-Americana[35] que garante a liberdade de expressão e que tem sido interpretada pela Suprema Corte como norma que confere elevado grau de proteção ao discurso de cunho político.[36] Neste tema, o Brasil alinha-se com o pensamento europeu, uma vez que temos legislação restritiva da expressão tanto referente à discriminação racial quanto no tocante ao discurso político de cunho nazista, criminalizado pela Lei 9.459 de 13 de maio de 1997 (e que é plenamente aplicável à veiculação de símbolos nazistas em páginas da Internet).[37] Não há, pois, impedimento jurídico para o Brasil adotar tal modelo quando da elaboração de sua legislação referente à privacidade *online*.

B. A Proposta Canadense: utilização de assinaturas eletrônicas

---

[34] Id., seção III, artigo 8° (2): "*2. Paragraph 1 shall not apply where: (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or (...)*"

[35] Constituição dos Estados Unidos da América, Primeira Emenda: *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

[36] Conforme várias decisões da Suprema Corte dos Estados Unidos, dentre elas: *Terminiello v. City of Chicago*, 337 U.S. 1, 69 S.Ct. 894 (1949).

[37] A Lei 9.459/97 deu a seguinte redação ao artigo 20 da Lei 7.716 de 1989:
Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
Pena: reclusão de um a três anos e multa.
§ 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.
Pena: reclusão de dois a cinco anos e multa.

Merece breve referência a proposta canadense de aliar a solução técnica à proposta jurídica com vista à efetiva proteção da privacidade *online*. Trata-se do projeto de lei *Bill C-54* de 1° de outubro de 1998, originalmente apresentado no parlamento canadense. Essa proposta foi apresentada novamente em 1999, agora sob o título de *The Information Protection and Electronic Documents Act*.[38] Além desse projeto de lei contemplar as proteções que refletem os princípios como notícia, pleno conhecimento e autorização por parte dos usuários, a iniciativa vai além e incentiva o uso de assinaturas eletrônicas[39] em transações que envolvem o governo canadense.

O uso de assinaturas eletrônicas corresponde ao emprego de uma ferramenta técnica (um programa de computador, um *software*) que ajuda a manter a integridade dos dados quando de seu tráfego pela rede.[40] O único ponto polêmico do projeto (e que não deve ser copiado pelo modelo brasileiro) é uma proposta de emenda que busca permitir às agências governamentais acessar os dados pessoais quando da necessidade de se obter informação referente a pessoas (para fins juridicamente determinados) sem a obrigatoriedade de mandados judiciais.[41]

O ponto mais interessante desse projeto é o que faz referência à solução técnica. Em outras palavras, parte da solução reside em um programa de computador, em um "código." Há uma corrente doutrinária crescente nos Estados Unidos advogando a

---

[38] O projeto de lei foi apresentado em 1999 como *Bill C-6*.

[39] Por assinaturas eletrônicas, neste projeto de lei especificamente, entende-se tanto o uso de senhas que identificam o usuário, como o de assinaturas digitais que fazem uso de recursos de criptografia assimétrica forte. Para maiores referências quanto às assinaturas digitais: ROHRMANN, Carlos. O Direito Comercial Virtual - A Assinatura Digital, *Revista da Faculdade de Direito Milton Campos*, Vol. 4, 1997.

[40] Conforme - News From Around the World. *The Bereau of National Affairs World Internet Law Report*. Vol. 1, Fascículo 3, Novembro de 1999, página 3: "Legislation on Personal Privacy Reintroduced in Canada - The legislation also calls for the use of electronic signatures and electronic documents in federal government transactions and the delivery of government services."

[41] Id.: "The privacy legislation has been the subject of considerable controversy, particularly over an amendment proposed by Industry Minister Manley to exempt law enforcement agencies from a requirement to seek a warrant to obtain personal information."

proposta de que o código é a lei da Internet. Em outras palavras, neste caso, não haveria como legalmente manter o direito à privacidade na rede sem o controle direto do código (dos programas) usado para implementar a Internet.[42] Essa proposta doutrinária incorre em grave erro ao confundir o instrumento computacional (o programa de computador) com o direito. Dado o crescimento dessa corrente doutrinária equivocada dentro do estudo do Direito da Internet nos Estados Unidos, dedicamos um capítulo à sua análise.

C. *O código dos programas é a lei da Internet? Criptografia e as demais soluções técnicas para a proteção da privacidade online*

A corrente doutrinária responsável pela super valorização do código como lei da Internet pode ser encontrada na recente obra *Code and Other Laws of Cyberspace,*[43] que reúne argumentos de vários artigos anteriormente publicados pelo professor Lessig.[44] Outros professores norte-americanos também endossam a teoria, embora de forma menos intensa, apregoando que o código é a lei[45] da Internet em certos casos como, por

---

[42] O professor Larry Lessig, da Universidade de Harvard, é o principal expoente desta corrente. Autor de vários artigos publicados ao longo da década de 90 acerca do tema, Lessig defende a teoria que o governo deverá ter controle sobre o código dos programas para fazer valer o direito no meio virtual.

[43] LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. New York, Basic Books, 1999.

[44] Dentre tais artigos de autoria do professor Larry Lessig, podemos citar: Zoning Speech on the Internet: A Legal and Technical Model, *98 Mich. L. Rev. 395 Michigan Law Review November, 1999*; The Limits in Open Code: Regulatory Standards and the Future of the Net, *14 Berkeley Tech. L.J. 759 Berkeley Technology Law Journal Spring 1999*; Keynote Address: Commons and Code, *9 Fordham Intell. Prop. Media & Ent. L.J. 405 Fordham Intellectual Property, Media and Entertainment Law Journal Winter Symposium 1999*; Open Code and Open Societies: Values of Internet Governance, *74 Chi.-Kent L. Rev. 1405 Chicago-Kent Law Review 1999*; What Things Regulate Speech: CDA 2.0 vs. Filtering, *38 Jurimetrics J. 629 Jurimetrics Journal Summer, 1998*; Constitution and Code, *27 Cumb. L. Rev. 1 Cumberland Law Review 1996-1997*; Reading the Constitution in Cyberspace, *45 Emory L.J. 869 Emory Law Journal Summer 1996*; Intellectual Property and Code, *11 St. John's J. Legal Comment. 635 Saint John's Journal of Legal Commentary Summer 1996*; The Zones of Cyberspace, *48 Stan. L. Rev. 1403 Stanford Law Review May, 1996*.

[45] Aqui ficamos com um problema de tradução. A língua inglesa faz uso do termo "Law" para "Direito". Todavia, há momentos nos quais "law" pode ser traduzido como "lei", sem prejuízo do termo "statute", usado nos Estados Unidos para "lei".

exemplo, quando da utilização de programas de filtragem[46] de conteúdo pelos pais para evitar que os filhos tenham acesso à pornografia *online*.[47] No exemplo analisado a seguir, segundo a corrente acima elencada, o programa de filtragem seria a "lei da Internet", para o filho, quando do seu acesso à rede.[48]

O motivo de nossa discordância reside na definição de "Law", ou "direito", ou "lei no sentido amplo." Entendemos que o direito tem algumas propriedades fundamentais que o código, como ferramenta, não tem. O direito é aplicável de forma universal, ao passo que o código só é aplicado àqueles que optam por sua utilização (em nosso exemplo, pelo pai que resolveu comprar um programa de bloqueio aos *sites* indecentes). O direito, por seu turno, é aplicado pelo poder público de ofício ou mediante provocação. Neste exemplo, não há como o pai pedir ao poder público que aplique sanções à filha por eventual a não-utilização do programa de filtragem.[49] Finalmente, o direito é redigido com vista ao bem público, característica que não se encontra no código, escrito para beneficiar o fabricante do programa e não a população em geral (mesmo porque alguns pais hão de achar o programa de filtragem desaconselhável, por entenderem que "nenhuma leitura deve ser dirigida, ou censurada").

---

[46] Os programas de filtragem da rede fazem uso de classificações dos *web sites* de forma a bloquear o acesso a certos *sites* como os de conteúdo indecente. Um bom exemplo dessa família de programas é o *Cyberpatrol*. Maiores referências são encontradas *online* em <http://www.cyberpatrol.com/dyn_hm.htm>, visitado em 21 de abril de 2000.

[47] Dentre eles, pode-se citar o professor Stuart Biegel com sua obra a ser publicada em 2001: *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Chapter 7, MIT Press (forthcoming - 2000/2001).

[48] Este exemplo foi trazido pelo professor Stuart Biegel para justificar a sua tese de que, em certos casos, o código é a lei da Internet. Os artigos do professor Biegel podem ser encontrados *online* em sua página mantida na Universidade da Califórnia em Los Angeles - UCLA <http://www.gseis.ucla.edu/iclp/hp.html>, visitada em 21 de abril de 2000.

[49] Os programas de filtragem podem ser desativados por usuários mais qualificados. Ou mais, eles podem ainda ser ignorados pelo sistema através da utilização de recursos computacionais mais avançados. Para quem tiver curiosidade em como desativar tais programas de filtragem, nós sugerimos: *How to disable Cyber Patrol*, <http://www.peacefire.org/bypass/Cyber_Patrol/>, página visitada em 21 de novembro de 1999.

Trazendo a análise para o campo da privacidade, os autores retro-mencionados defendem a utilização, por exemplo, de programas de criptografia como solução para garantir a privacidade *online*. Neste caso, continuam os autores, a "lei da privacidade da Internet" seria o *software* de criptografia.[50] Insistimos que não há nada de jurídico no uso da criptografia para proteger a privacidade, sendo ela apenas uma ferramenta técnica da computação, auxiliando o direito. Confundir o programa de computador usado no mundo *online* com o direito da Internet seria tão errado como confundir a polícia com a lei...[51]

PARTE DOIS – PRIVACIDADE *ONLINE* NO BRASIL

I – ANÁLISE DA REALIDADE DA INTERNET E DA PRIVACIDADE ONLINE NO BRASIL

A. *Realidade da Internet e do comércio eletrônico no Brasil: os aspectos técnicos e sociais*

Durante os primeiros meses do ano 2000, as empresas ligadas à Internet experimentaram grandes alterações de valor em todo o mundo, dada a enorme flutuação

[50] Maiores referências na nota 39, supra, e em páginas da Internet voltadas para a matéria, tais como RSA, <http://www.rsa.com>, visitada em 21 de abril de 2000; Electronic Privacy Information Center, *Cryptography and Liberty 1999: An International Survey of Encryption Policy*, <http://www.epic.org/reports/crypto1999.html>, visitada em 20 de novembro de 1999; e, ainda, o artigo do professor da Faculdade de Direito da Universidade de Miami, Michael Froomkin: FROOMKIN, A. Michael. It Came From Planet Clipper: The Battle Over Cyptographic Key 'Escrow'. *1996 U. Chi. L. Forum 15 (1996)*, <http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm>, visitada em 07 de outubro de 1999.

[51] Pode-se notar que a confusão é perigosa. Achar que o código dos programas é a lei só pode decorrer do fato de haver uma falta de noção da conceituação de "direito" por parte dos professores americanos que defendem tal teoria. As conseqüências seriam desastrosas: se o código fosse a lei, para que precisaríamos do legislador? Bastaria chamar o programador de plantão para "melhor" regulamentar o mundo *online*, algo como colocar um policial em frente a cada casa para evitar disputas entre vizinhos, sob a

das ações das empresas relacionadas à chamada "nova economia" e ao comércio eletrônico baseado no *Silicon Valley*.[52] A despeito de tal volatilidade, o comércio eletrônico ainda era responsável por importantes e valiosas aberturas de capital de empresas nas bolsas de valores internacionais. No Brasil, os números da Internet e do comércio eletrônico (como tivemos oportunidade de ver na Introdução deste artigo) ainda são modestos se comparados aos dos Estados Unidos.[53] Temos 7,4% dos domicílios brasileiros com acesso à Internet via linhas telefônicas.[54] Embora ainda tímido[55], as pesquisas apontam um enorme potencial de crescimento do comércio eletrônico no Brasil.[56]

Do ponto de vista técnico, as limitações ainda estão presentes. O Brasil tem poucas linhas de acesso à Internet via cabo e o acesso por telefone padece de alguns problemas. De um lado, temos, em certas localidades, centrais com linhas telefônicas ainda antigas e que não permitem grandes velocidades de comunicação de dados; do outro, o custo da ligação local no Brasil é relativamente alto. Nos Estados Unidos, os usuários residenciais não pagam impulsos telefônicos em ligações locais; assim, ficar

---

argumentação de que o policial é o mais capacitado por ser o que mais conhece o "código" da segurança pública.

[52] Uma excelente fonte de notícias sobre o que ocorre no coração da nova economia é o *San Jose Mercury*, disponível *online* em <http://www1.sjmercury.com/>, visitado em 02 de abril de 2000.

[53] Ver nota de rodapé número 3, supra.

[54] Id.

[55] Artigo publicado pelo jornal O GLOBO, *online* <http://www.oglobo.com.br> dá conta de uma estatística da ordem de 370 milhões de dólares de movimentação do e-commerce no Brasil em 2000: "Visa: e-commerce no Brasil movimentará US$ 370 milhões em 2000 (Jacqueline Breitinger) - Um estudo encomendado pela Visa ao Boston Consulting Group mostra que, este ano, as vendas na Internet brasileira poderão chegar a US$ 370 milhões, contra os US$ 130 milhões obtidos em 1999."

[56] Recente artigo publicado pela CNN dá conta de um crescimento considerável do comércio eletrônico no Brasil nos próximos anos: CNN, *Brasil vai liderar vendas on-line na América Latina em 2004, diz pesquisa*, <http://cnnemportugues.com/2000/economia/04/21/brasilonline.reut/index.html>, visitado em 22 de abril de 2000: "O comércio eletrônico alcançará 6,9 bilhões de dólares em 2004, com a região da América do Norte respondendo pela metade de todas as vendas on-line, e o Brasil com o maior número de transações feitas na América Latina, segundo informe da empresa de pesquisa Forrester Research. A empresa de pesquisa prevê que as vendas on-line no Brasil aumentem 165 por cento entre 2003 e 2004."

ligado à Internet 1 minuto ou 10 (ou mais) horas[57] seguidas custa exatamente o mesmo (no tocante à ligação telefônica, alguns provedores de acesso podem cobrar por hora conectada).

Outro ponto da maior importância, no campo social, é a facilitação de acesso das crianças brasileiras à rede. Precisamos criar incentivos governamentais para que o maior número de escolas públicas ofereçam acesso à Internet para que a maior parte possível da população ganhe familiaridade com essa notável ferramenta de pesquisa.[58] Trata-se de medidas que já foram tomadas nos Estados Unidos e que se mostraram de grande eficácia. Por outro lado, um fenômeno que começa a se alastrar pelo Brasil e que pode ser responsável por um considerável incremento do acesso dos brasileiros à Internet é o "acesso gratuito". Trata-se de provedores de acesso que não cobram de seus usuários, à espera de um aumento do número de pessoas que estão a visitar todos os dias um determinado *web-site*, o que, obviamente, aumenta o valor do provedor para fins de propaganda (publicidade) ou *links* para outras páginas da rede (e ajuda a incrementar o volume do comércio eletrônico no Brasil).[59]

B. *A proteção constitucional à privacidade e a Lei 9.296/96*

---

[57] Como no meu caso, durante vários momentos da redação deste artigo.

[58] O projeto de lei número 00794/2000, de autoria do deputado Paes Landim, "sugere ao poder executivo, por intermédio do Ministério das Comunicações, a instituição de incentivos para disseminação da Internet". Ementa disponível em: <http://home.earthlink.net/~lcgems/Projetos2.htm>, visitado em 27 de abril de 2000.

[59] Conforme artigo publicado pelo jornal "O Estado de São Paulo", *online*, <http://www.estadao.com.br>, visitado em 28 de fevereiro de 2000: "Internet cresce com acesso grátis: A comunidade de internautas no Brasil já cresceu entre 5% e 15% em decorrência do acesso gratuito, segundo dados do International Data Corporation (IDC), um dos maiores institutos de pesquisa do ramo. O gerente de Pesquisa do IDC Brasil, Gerd Souza, esclareceu que essa estimativa foi feita com base na expansão de computadores conectados à rede no País. Combinando esses dois fatores - Internet grátis e mais PCs - o IDC decidiu rever as projeções

A questão da privacidade dos dados foi objeto da primeira regulamentação aplicável à Internet em 1996, através da Lei 9.296 que regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.[60]

O artigo 10 da lei em análise criminaliza a "interceptação de comunicações telefônicas, de informática ou telemática, ou a quebra de segredo da justiça, sem autorização judicial ou com objetivos não autorizados em lei."[61] Nota-se que tal artigo dificilmente se aplica à coleta de dados diretamente do usuário, uma vez que não há "interceptação" de comunicação e uma analogia neste sentido seria inadmissível, por se tratar de analogia "in mala partem".

C. Projetos de lei no Congresso Brasileiro e demais perspectivas

Os inúmeros projetos de lei que tramitam no Congresso Nacional referentes à Internet cobrem matérias relativas ao comércio eletrônico[62], repressão à pornografia na

---

para o comércio eletrônico no País este ano. Segundo Souza, o comércio eletrônico brasileiro vai movimentar US$ 430 milhões este ano - 13% mais do que os US$ 380 milhões inicialmente previstos."

[60] Constituição da República, artigo 5° inciso XII – "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."

[61] Artigo 10 da Lei 9296/96: "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
Pena: reclusão, de dois a quatro anos, e multa."

[62] Dentre os projetos de lei referentes ao comércio eletrônico, temos: PL 1483/99, de autoria do deputado Dr. Hélio, que "institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico" e o PL 1589/99, de autoria do deputado Luciano Pizzatto que "dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital." Temos, ainda, o "Projeto de Regulamentação do Comércio Eletrônico", entregue pela OAB-SP ao deputado Michel Temer, disponível no *web site* da OAB-SP <http://www.oabsp.org/br/main3.asp?pg=3.2&pgv=a&id_noticias=335>, visitado em 13 de maio de 2000.

Internet e criação de incentivos ao desenvolvimento da rede no Brasil.[63] Em relação aos projetos de leis especificamente voltados para a privacidade *online*, boa parte dos projetos foram arquivados em face da Lei 9.296/96.

Uma vez que o próprio comércio eletrônico ainda não conta com lei regulamentadora no Brasil, é possível que, quando da edição de normas referentes à assinatura digital e aos demais temas referentes ao comércio eletrônico, a matéria "privacidade dos dados" seja novamente colocada em foco pelo legislador brasileiro.

Em face da ausência de legislação específica que trate, por exemplo, dos crimes cometidos por uso de computador, é ainda difícil a repressão jurídica às praticas computacionais nocivas aos usuários e à privacidade quando do uso da Internet (tais como a coleta indevida de dados, sem que os mesmos sejam apagados da memória do computador dos quais foram retirados).[64] Somos da posição de que a coleta indevida (sem a autorização inequívoca) de dados através da Internet deva ser tipificada no Brasil.[65]

É importante notar as primeiras manifestações no Brasil contrárias à presença de *sites* que propagam o "ódio" pela Internet (também conhecidos como *hate sites*). Os chamados "hate sites" são normalmente patrocinados por grupos norte-americanos[66] anti-

---

[63] O Senado Federal disponibiliza *online* uma ferramenta de pesquisa dos projetos de lei em tramitação: <http://www.senado.gov.br/sicon/mate.htm>, visitado em 04 de janeiro de 2000. Há uma relação de projetos referentes ao Direito da Informática em: <http://home.earthlink.net/~lcgems/>.

[64] Pratica que não poderia ser tipificada como crime de dano, uma vez que a integridade física do computador não é afetada. Neste exemplo, admite-se que não há a prática de estelionato relacionada com a coleta e utilização dos dados.

[65] Um dos mais importantes projetos de lei que tramitam no Congresso Brasileiro, e referentes a crimes cometidos na área de informática é o PL 00084, de 1999, de autoria do deputado Luiz Piauhylino. Outras informações acerca de sua tramitação são encontradas diretamente no sistema de informações do Senado Federal, nota 63, *supra*.

[66] Não só norte-americanos, há também inúmeros grupos neo-nazistas no Brasil publicando mensagens na rede.

semitas[67], anti-latinos, anti-negros, dentre outros, grupos que também se auto-identificam como "grupos de supremacia branca". Neste caso, a Internet oferece facilidades a tais iniciativas, em face da possibilidade de se manter um certo anonimato na rede.[68]

II – UM MODELO DE LEGISLAÇÃO PARA O BRASIL

A. *Qual a melhor solução: uma lei nova ou a auto-regulamentação?*

Neste momento, mais uma vez, voltamos à questão da utilização do código como lei da Internet. A despeito dos defensores da teoria supra citada, não acreditamos que a auto-regulamentação seja a mais indicada para a efetiva proteção da privacidade na Internet. Aqueles que defendem a auto-regulamentação argumentam que os próprios programas de computador podem ser utilizados pelos usuários para a efetiva proteção da privacidade *online*. Os motivos de nossa discordância são singelos. Primeiro, os usuários da Internet, em sua maioria, optam pela configuração-padrão dos programas de computador e, dificilmente, vão ter grandes preocupações em adquirir *software* específico de proteção de dados. Segundo, muitas vezes, o usuário é levado a descortinar os seus dados diretamente quando da utilização de um certo *site* que formula as perguntas independentemente de esse usuário estar usando um programa de proteção dos seus dados

[67] O que é crime no Brasil, V. nota 37, *supra*.

[68] Merece destaque a preocupação do deputado Marcos Rolim que, recentemente, anunciou a sua determinação no sentido de patrocinar uma proposta de lei que possa ajudar a coibir a "propagação do ódio" pela Internet, no Brasil: Deputados Atentos ao Rascismo na Internet - Marcos Rolim (PT-RS) propõe o fim de anonimato na criação de e-mails e páginas na rede. *Estado de São Paulo*. Publicado na Internet, em 11 de abril de 2000: " O presidente da Comissão de Direitos Humanos da Câmara, deputado Marcos Rolim (PT-RS), propôs a criação de um grupo informal de cerca de 10 deputados para elaborar um anteprojeto de lei prevendo a regulamentação do uso da rede mundial de computadores no País, de modo a

pessoais. Terceiro, os programas de proteção de dados poderiam ser evitados por programas de coleta de dados especialmente desenvolvidos para a finalidade de uma coleta de dados sem autorização, com nenhuma proteção jurídica ao titular dos dados.

Hoje, no Brasil, é grande a necessidade de novas leis regulamentadoras das relações humanas que ocorrem em meio virtual. Como já tivemos a oportunidade de ver, não só na área da privacidade *online*, como em outros aspectos do comércio eletrônico, o Brasil ainda carece de uma legislação específica.[69]

Assim, nossa proposta visa apresentar sugestão dos princípios que devem ser levados em consideração pelo legislador brasileiro quando da regulamentação da privacidade *online*, em face da experiência alienígena e em busca de uma uniformidade com os princípios consagrados na Europa e nos Estados Unidos.

B. *Sugestão de Lei de Proteção à Privacidade Online*

Lei n. (...), de (...) de 2000.

Cuida da proteção à privacidade e aos dados pessoais dos usuários de redes de computadores.

---

coibir a proliferação desse tipo de *sites*. A principal idéia defendida por Rolim e por Samuels é o fim do anonimato na criação de *e-mails* e páginas na Internet."

[69] Não se pode deslembrar, aqui, da Lei número 9.800/99 que trata da utilização da Internet para o envio de petições ao Poder Judiciário. Trata-se de uma iniciativa louvável e que deveria ser acompanhada de outras leis importantes que dêem suporte a uma segura utilização da Internet para fins públicos e privados (como, por exemplo, a regulamentação da assinatura digital e dos "cartórios virtuais"). Maiores referências: CORRÊA-LIMA, Osmar Brina. *Lei N. 9.800, de 1999*. Belo Horizonte, outubro de 1999, publicação disponível *online* em <http://www.home.earthlink.net/~lcgems/Lei9800BR.htm>, visitada em 22 de outubro de 1999.

Art. 1º. A coleta de dados pessoais de usuários de redes de computadores, por parte de entidades públicas ou privadas, através de *sites* comerciais ou não-comerciais observará o disposto nesta Lei.

Art. 2º. Dados pessoais são dados e demais informações relacionadas a uma pessoa natural civilmente identificável.

Art. 3º. É permitida a coleta de dados pessoais em sistemas de redes de computadores, desde que observados os seguintes princípios:

I - divulgação de forma clara e objetiva, por parte do *site* que visa coletar dados, de quais dados serão coletados e com quais finalidades;

II - autorização prévia e inequívoca da coleta por parte do titular dos dados pessoais;

III - adoção, pelo coletor, de mecanismos técnicos de segurança para a proteção dos dados pessoais coletados contra perdas, alterações, adulterações e cópias não autorizadas;

IV - manutenção de mecanismos de acesso do titular aos seus dados coletados e mantidos em computadores ou nas demais dependências da entidade coletora;

V - opção, mediante comunicação escrita, por parte do titular dos dados pessoais, da revogação da autorização de coleta, manutenção ou transferência de dados pessoais, o que acarreta em imediata retirada dos seus dados anteriormente coletados dos computadores ou demais dependências da entidade coletora.

Art. 4º. Constitui crime coletar dados pessoais em redes de computadores, manter, alterar, adulterar ou transferir a terceiros dados pessoais já coletados, sem o prévio conhecimento e a devida autorização prévia do titular dos dados pessoais.

Pena: reclusão, de dois a quatro anos, e multa.

Parágrafo único. Quando o crime for cometido contra titular de dados pessoais menor de 18 anos.

Pena: reclusão, de quatro a oito anos, e multa.

Art. 5º. Independentemente do procedimento criminal, o titular dos dados pessoais poderá intentar ação para proibir ao infrator a prática do ato incriminado, com cominação de pena pecuniária para o caso de transgressão do preceito.

§ 1º. A ação de abstenção de prática de ato poderá ser cumulada com a de perdas e danos pelos prejuízos decorrentes de infração.

§ 2º. Independentemente de ação cautelar preparatória, o juiz poderá conceder medida liminar proibindo ao infrator a prática do ato incriminado, nos termos deste artigo.

Art. 6º. Esta Lei entra em vigor seis meses após a sua publicação.

Art. 7º. Revogam-se as disposições em contrário.

Brasília, (...) de (...) de 2000, 179º da Independência e 112º da República.

CONCLUSÃO

O estudo do Direito Comparado mostra-se, mais uma vez, de grande importância para a comunidade jurídica brasileira. Da mesma forma que, quando da elaboração do Código Civil Brasileiro, institutos foram inspirados no direito estrangeiro, mais uma vez, agora no campo do Direito Virtual, a observação da experiência jurídica alienígena é de grande valia. Dado o enorme crescimento econômico experimentado pelos Estados

Unidos nos últimos cem anos, a complexidade das relações comerciais naquele país atingiu níveis muitos altos, levando ao maior desenvolvimento do direito comercial norte-americano. O estudo do direito societário brasileiro e sua relação com o direito norte-americano (principalmente no que tange à sociedade anônima) exemplificam bem tal questão. Pode-se apontar os Estados Unidos como o país de maior desenvolvimento do Direito Virtual neste momento, sendo pois a principal fonte de estudo quando da perspectiva comparativa da regulamentação da Internet e do direito comercial eletrônico, todavia, não se pode deixar de acompanhar o que ocorre em outros países, como tivemos oportunidade de demonstrar no caso do modelo europeu. Cabe concluir que o estudo do Direito Comparado não deve ser visto como um simples método de importação do direito estrangeiro, mas como uma ciência que visa estudar os diversos institutos jurídicos sob a ótica dos mais variados sistemas jurídicos.

Apesar de o comércio eletrônico ainda estar começando a expandir-se no Brasil, algumas questões são da maior importância para o uso efetivo e seguro da Internet pelos brasileiros. A falta de legislação específica voltada para a regulamentação da Internet no Brasil gera insegurança quando do uso da rede pelas pessoas não acostumadas com os desafios trazidos pelo mundo *online*. Algumas características do mundo *online*, tais como: ninguém estar "fisicamente presente" no espaço virtual; facilidade de coleta, duplicação e alteração de dados na Internet e a possibilidade de automação cada vez maior das tarefas realizadas pelos computadores, dificultam a aplicação de legislações antigas quando da regulamentação das relações humanas que ocorrem no meio virtual. Urge elaborar um conjunto de leis voltadas para a regulamentação da Internet no Brasil, o

que, indiscutivelmente, acarretará um crescimento do uso juridicamente seguro da rede pelos brasileiros.