GUARDA DOS REGISTROS DE CONEXÃO E DE APLICAÇÃO: ESTUDO SOBRE O CONFLITO PRIVACIDADE *VS*. SEGURANÇA JURÍDICA NA PROPOSTA DO PROJETO DE LEI N. 2.126/11

KEEPING OF CONNECTION AND IMPLEMENTATION RECORDS: STUDY ABOUT THE CONFLICT PRIVACY *VS*. LEGAL SECURITY AT THE LAW PROJECT N. 2.126/11 PROPOSAL

Bruna Pinotti Garcia[*]
Mário Furlaneto Neto[**]

RESUMO
Sob o enfoque da guarda dos registros de conexão e aplicação da *Internet*, tomando por referenciais teóricos os conceitos da Ciência da Computação, discute-se o PL n. 2.126/11, denominado de Marco Civil para a *Internet* no Brasil, atualmente em trâmite na Câmara dos Deputados, com a finalidade específica de debater o conflito entre a privacidade e a segurança jurídica. Assim, por meio de uma revisão bibliográfica, documental e jurisprudencial, busca-se enfrentar a necessidade de manutenção dos registros de conexão à *Internet*, bem como dos registros de acesso a aplicativos de *Internet*, enquanto formas de preservar a privacidade e a segurança jurídica diante de abusos do direito à liberdade praticados por usuários, inclusive considerando sobre o atual contexto destes armazenamentos. Conclui-se haver necessidade de ampla discussão sobre o teor do PL n. 2.126/11, notadamente no que tange à faculdade de armazenamento dos registros de acesso a aplicativos de *Internet* por parte do provedor de aplicações de *Internet*, sob pena de haver uma lacuna legislativa que inviabilizará a investigação de eventuais atos ilícitos praticados em abuso ao direito de liberdade de expressão.
PALAVRAS-CHAVE: Direito eletrônico; registros de conexão e de aplicação; Marco Civil para a *Internet*; conflito de princípios; ponderação.

ABSTRACT
Considering the focus of keeping of Internet connection and implementation records, taking as theoretical Computer Science concepts, it discuss the LP n. 2.126/11, named Landmark Civil to the Internet in Brazil, currently pending in the House, with the specific purpose of discussing the conflict between privacy and legal security. Thus, through a literature, document and case law review, it seeks to address the need for maintaining Internet connection records, such as Internet implementation records, as ways of preserving privacy and legal security before abuse of the right to freedom practiced by users, including considering about the current context of these stores. It concludes there is a need of extensive discussion about the content of the LP n. 2.126/11, especially regarding the faculty of storage of Internet connection and implementation records by the provider of Internet applications,

[*] Advogada. Mestranda em Direito do Centro Universitário Eurípides de Marília – UNIVEM, bolsista CAPES – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (modalidade 1). Aluna pesquisadora do "Núcleo de Estudos e Pesquisas em Direito e *Internet*". Endereço eletrônico: <brunapinotti@univem.edu.br>.
[**] Delegado de Polícia. Doutor em Ciência da Informação pela Universidade Estadual Paulista - UNESP. Docente do Programa de Mestrado em Direito do Centro Universitário Eurípides de Marília - UNIVEM. Coordenador do "Núcleo de Estudos e Pesquisas em Direito e Internet". Endereço eletrônico: <mariofur@univem.edu.br>.

lest there be a legislative gap thus disrupting the investigation of possible unlawful acts committed for abuse of the right of freedom of expression.
KEYWORDS: Electronic Law; connection and implementation records; Landmark Civil to the Internet; conflict of principles; weighing.

INTRODUÇÃO

As discussões do Projeto de Lei (PL) n. 2.126/11, denominado Marco Civil para a *Internet*, fez surgir defensores da tese de que a regulamentação quanto ao armazenamento de registros de acesso à *Internet* pode vir a ferir o direito à liberdade de expressão, a ponto de se tornar uma interferência estatal policialesca, com irrestrita invasão da privacidade alheia.

Ocorre que, atualmente, os provedores de *Internet* sediados no Brasil já guardam os registros de conexão e outros *logs*, sob o manto de recomendação do Comitê Gestor de *Internet* do Brasil (CGI), o que é corroborado pelo atual entendimento jurisprudencial. Além disso, essa prática já é regulamentada em outros países, em especial no eixo da Comunidade Europeia, com esteio em legislação que especifica critérios de tutela do sigilo de tais informações e estabelece as hipóteses específicas em que é passível a quebra do sigilo.

Na verdade, a ausência de regulamentação legal a respeito da guarda dos registros de conexão e de aplicação da *Internet* acaba por trazer insegurança jurídica e perda de privacidade ao próprio internauta, na medida em que nem ele sabe os limites de atuação dos servidores de *Internet*. De outro lado, também estes servidores não conhecem os seus deveres de guarda, posto que a diretiva do CGI não é coativa e a jurisprudência brasileira ainda não traz critérios bem delimitados, gerando insegurança jurídica também neste viés.

Assim, no presente artigo, parte-se da hipótese de que a falta de regulamentação sobre a guarda dos registros de conexão e aplicação tem gerado perda da privacidade e da segurança jurídica, posto que não há previsão de quais informações devem ser armazenadas e por quanto tempo, ficando o usuário a mercê da mantenedora/provedor da rede e vice-versa, sendo necessária a aprovação de uma legislação específica sobre a matéria que seja esclarecedora a respeito de prazos e conteúdos dos registros armazenados.

O estudo sobre a questão será realizado pelo método hipotético-dedutivo, com o teste da hipótese acima levantada, utilizando meios de pesquisa bibliográfica - referente à literatura de Ciência da Computação[1] e Direito - e documental - no que tange ao levantamento de projetos de lei brasileiros e da legislação estrangeira vigente. Em suma, propõe-se uma abordagem inicial a respeito dos conceitos de registros de conexão e aplicação, como esteio

[1] Estudo desenvolvido com o apoio do "Grupo de Pesquisa em Sistemas Computacionais Aplicados", liderado pelo Prof. Dr. Fabio Dacencio Pereira.

para uma posterior análise do contexto atual do armazenamento de registros no Brasil, com fundamento na diretiva estabelecida pelo Comitê Gestor de *Internet* e no posicionamento jurisprudencial majoritário, bem como no direito comparado, nomeadamente a diretiva europeia vigente, lançando base para enfrentar as propostas legislativas elaboradas, notadamente o PL n. 2.126/11, com a finalidade de produzir um referencial teórico para ponderar acerca do tratamento esperado dos dados do internauta sob o viés constitucional do conflito privacidade *vs*. segurança jurídica.

Com efeito, pretende-se fornecer um panorama geral a respeito dos conceitos técnicos envolvidos no armazenamento de registros do usuário da *Internet*, bem como do tocante às propostas legislativas elaboradas considerado o atual contexto do tratamento de dados, de modo a efetuar uma ponderação constitucional sobre as expectativas de tratamento da matéria no Estado Democrático de Direito brasileiro.

1 REGISTROS DE CONEXÃO E REGISTROS DE APLICAÇÃO: O SISTEMA DAS CAMADAS DE GUARDA

Paulatinamente, a tecnologia tem passado por intensos processos de mudanças visando atender às novas necessidades sociais, o que implica num aumento da complexidade em sua estruturação. O que começou com computadores gigantescos e caríssimos, hoje se encontra na palma da mão de boa parte das pessoas; a rede que a princípio deveria servir a fins somente militares foi incorporada à vida social, alterando substancialmente o modo de convivência entre os seres humanos.

Historicamente, remonta-se à *ARPAnet*, primeira rede de computadores criada, que antecedeu a *Internet*. Em 1972, a *ARPAnet* foi apresentada publicamente pela primeira vez por Robert Kahn, mesmo ano em que Ray Tomlison escreveu o primeiro programa de e-mail. A *ARPAnet* inicial era uma rede fechada e para se comunicar com uma máquina a ela conectada era preciso estar ligado a um outro IMP dessa rede. Do início a meados de 1970, surgiram novas redes de comutação de pacotes, como *ALOHAnet*, *Telenet*, *Cyclades*, *Tymnet* e *SNA*. Neste período, inúmeros estudos sobre as redes de conexão estavam em curso. Ao final da década de 1970, cerca de 200 máquinas estavam conectadas à *ARPAnet*; ao final da década de 1980, o número de máquinas ligadas à *Internet* pública, uma confederação de redes parecida com a *Internet* de hoje, alcançou cem mil. (KUROSE; ROSS, 2005, p. 40-43). No processo de crescimento da década de 1980, destaca-se a *NSFNET*, criada em 1986:

> A década de 1990 estreou com vários eventos que simbolizaram a evolução contínua e a comercialização iminente da *Internet*. A *ARPAnet*, a progenitora

> da Internet, deixou de existir. Durante a década de 1980, a *MILNET* e a *Defense Data network* (Rede de Dados de Defesa) cresceram e passaram a carregar a maior parte do tráfego do Departamento de Defesa dos Estados Unidos e a *NSFNET* começou a servir como uma rede de *backbone* conectando redes regionais nos Estados Unidos com nacionais no exterior. Em 1991, a *NSFNET* extinguiu a restrição que impunha a sua utilização com finalidades comerciais, mas, em 1995, perderia seu mandato quando o tráfego de *backbone* da *Internet* passou a ser carregado por provedores de serviços de *Internet*. O principal evento da década de 1990, no entanto, foi o surgimento da *World Wide Web*, que levou a *Internet* para os lares e empresas de milhões de pessoas no mundo inteiro. (KUROSE; ROSS, 2005, p. 43-44).

No final da década de 1990, a *Internet* continuava crescendo vertiginosamente, tornando algumas ferramentas bastante populares, como o e-mail, a *Web*, o serviço de mensagem instantânea e o compartilhamento P2P (KUROSE; ROSS, 2005, p. 44). Com efeito, no início nem se imaginava que a *Internet* se tornaria um dos principais meios de comunicação já criados, uma necessidade - ou ao menos um facilitador considerável - para atividades como trabalho, estudo e lazer. Entretanto, quanto mais os computadores e as redes de conexão começaram a fazer parte da vida das pessoas, mais elas buscavam neles novos recursos e finalidades. Neste sentido, afirma Castells (2006, p. 69) que a integração crescente entre mentes e máquinas está alterando de maneira fundamental o modo pelo qual o homem nasce, vive, aprende, trabalha, produz, consome, sonha, luta e morre.

Hoje, a rede mundial de computadores se faz presente em atividades cotidianas do Estado, numa intensificação constante da chamada governança eletrônica; das empresas privadas, tanto no trato do público quanto na potencialização de serviços internos; e, notadamente, das pessoas de variadas classes sociais, considerado o crescente processo de inclusão digital.

O uso dos recursos tecnológicos tem gerado um processo de inconsciência por parte das pessoas a respeito dos limites quanto à preservação da privacidade pessoal (FURLANETO NETO; GARCIA, 2011, p. 3530). Afinal, quanto melhores ficam os computadores, mais eficazes eles ficam em extrair dos *bits* da rede uma vasta gama de informações, algo que não é objeto de atenção pelos usuários. Ocorre que as pessoas se deixaram envolver pelo mundo conectado, aceitando a perda de privacidade em troca de eficiência e conveniência (ABELSON; LEDEEN; LEWIS, 2008, p. 02-10).

Cada vez é mais fácil organizar informações e armazená-las, mas os internautas parecem não se importar com isso, o que somente intensifica o processo de perda da privacidade. Afinal, diferentemente do que ocorre no dia-a-dia do mundo externo - onde são comuns avisos próximos a caixas eletrônicos e dentro de ônibus a respeito do uso de sistemas

de captação de imagens -, não se encontram espalhados pela *Internet* alertas de que cada postagem ou troca de informações está sendo gravada. Mais que gravada, está passando por um processo de armazenamento de dados, que não se encontra regulamentado na atualidade.

Nada do que se faz na rede mundial de computadores fica perdido, posto que por trás de um computador e de seu gráfico cheio de recursos acessíveis, que transparecem certa capacidade de esquecimento do que é transmitido com possibilidades como exclusão de arquivos e históricos, está um complexo sistema de interconexão de redes e máquinas. No decorrer deste processo, as informações de uma máquina são constantemente enviadas a outra para o estabelecimento de conexões, onde ficam registradas.

A fim de melhor compreender essa complexa estrutura computacional, necessário se torna entender onde ficam guardados e qual o conteúdo dos chamados registros de conexão e aplicação. Para tanto, inicialmente, vale apurar quais são os agentes e equipamentos envolvidos no processo de guarda de registros.

As ligações estabelecidas no processo de interconexão se dão entre os sistemas finais de *Internet*. Há alguns anos, somente alguns equipamentos podiam funcionar como sistemas finais de conexão, como PCs tradicionais de mesa, estações de trabalho com sistema Unix e os chamados servidores (que armazenam e transmitem informações). Hoje, podem funcionar como sistemas finais tanto os computadores de mesa quanto os vários aparelhos móveis com acesso, como agendas digitais (PDAs), TVs, computadores portáteis, telefones celulares, automóveis, equipamentos de sensoriamento ambiental, telas de fotos, sistemas domésticos elétricos e de segurança, câmeras *Web*, entre outros. (KUROSE; ROSS, 2005, p. 3-8).

Cada um destes equipamentos pode ser denominado hospedeiro ou sistema final, e todos acessam a *Internet* por meio de Provedores de Serviços de *Internet*, que gerenciam a sua rede ISP de forma independente. Os sistemas finais executam os protocolos que controlam o envio e o recebimento de informações, que são o TCP, controlador da transmissão, e o IP, registrador dela. Estes sistemas finais costumam receber designações diferentes, qual seja, cliente ou servidor. (KUROSE; ROSS, 2005, p. 3-8).

Os clientes são os internautas, pessoas físicas ou jurídicas, públicas ou privadas, que utilizam a rede mundial de computadores. Já os servidores são os chamados provedores de *Internet*, bem como todos os mantenedores de sítios na *Web* que conferem serviços variados como, por exemplo, troca de mensagem, publicação de informações e acesso a conteúdos. Nesta relação tríplice que usualmente se estabelece na *Internet*, geralmente, os registros de conexão ficam guardados pelo provedor, ao passo que os registros de aplicação ficam a cargo

da mantenedora do *site* na rede; já o usuário, por sua vez, tem a capacidade de guardar em sua máquina ambos os registros.

Compreendidos os agentes e equipamentos envolvidos no movimento de conexão da *Internet*, é preciso estudar como tal sistema se estrutura. A arquitetura da rede mundial de computadores é mais complexa do que aparenta, envolvendo inúmeras etapas que podem ser denominadas camadas. Cada um dos diversos protocolos pertencem a uma camada, podendo ser implementados num *hardware*, num *software* ou em ambos. (KUROSE; ROSS, 2005, p. 34-36). O sistema de camadas aceita dois possíveis modelos:

a) Modelo de referência OSI (*Open Systems Interconnection*), que é baseado numa proposta desenvolvida pela ISO (*Internacional Standards Organization*) como um primeiro passo na direção da padronização internacional de protocolos nas camadas, defendendo a existência de 7 camadas: física, enlace de dados, rede, transporte, sessão, apresentação e aplicação. Apenas informa o que cada camada deve fazer, sem dividir os protocolos entre elas. (TANENBAUM, 1997, p. 32-33). Soares, Lemos e Colcher (2004, p. 122-123) afirmam que o intercâmbio de informações entre computadores de fabricantes distintos com o passar dos tempos se tornou uma necessidade, isto é, passou a ser preciso definir uma arquitetura única e, para impedir que um fabricante levasse vantagem sobre o outro, esta arquitetura teria que ser aberta e pública, criando-se o modelo de referência OSI.

b) Modelo de referência TCP/IP, que é um modelo simplificado, no qual há apenas 5 camadas, quais sejam: aplicação, transporte, rede, enlace e física. Enquanto o TCP é um protocolo inerente à camada de transporte, destinando-se à camada de rede, o protocolo mais importante desta última é o IP. (KUROSE; ROSS, 2005, p. 36-37). "Os modelos de referência OSI e TCP/IP têm muito em comum. Os dois se baseiam no conceito de uma pilha de protocolos independentes. Além disso, as camadas têm praticamente as mesmas funções" (SOARES; LEMOS; COLCHER, 2004, p. 42). A arquitetura da *Internet*, explicam Soares, Lemos e Colcher (2004, p. 123), é uma das mais importantes estruturas que se baseia no modelo TCP/IP, o qual prima por possibilitar a coexistência de redes heterogêneas - locais, metropolitanas e de longa distância.

No que tange à utilização da *Internet*, as camadas que se mostram intrinsecamente ligadas à atividade de armazenamento de registros são a de rede, responsável pelos registros de conexão, e a de aplicação, em que guardam-se os registros de aplicação.

Na dinâmica da rede, o que geralmente se vê são os registros de aplicação, que se referem às variadas atividades por ela proporcionadas, como correio eletrônico, *Web*, mensagem instantânea, compartilhamento via P2P, transferência de arquivos, jogos

multiusuários em rede, vídeos armazenados, telefonia pela rede e videoconferência em tempo real (KUROSE; ROSS, 2005, p. 58). "A camada de aplicação é onde residem aplicações de rede e seus protocolos. Ela inclui muitos protocolos, tais como o protocolo HTTP (que provê requisição e transferência de documentos pela *Web*), o SMTP (que provê transferência de mensagens de correio eletrônico) e o FTP (que provê a transferência de arquivos entre dois sistemas finais)" (KUROSE; ROSS, 2005, p. 37).

Uma aplicação de rede se forma por pares de processos que enviam mensagens uns aos outros por meio de uma rede. Por exemplo, na aplicação *Web*, o processo cliente de um *browser* troca mensagens com o processo de um servidor *Web*; enquanto num sistema de compartilhamento de arquivos P2P, um arquivo é transferido de um processo que está em um par para outro que está em outro par, isto é, entre clientes. (KUROSE; ROSS, 2005, p. 61). Sobre o conteúdo das aplicações de rede, Kurose e Ross (2005, p. 57) explicaram:

> Aplicações de rede são a razão de ser de uma rede de computadores. Se não fosse possível inventar aplicações úteis, não haveria necessidade de projetar protocolos de rede para suportá-las. Nos últimos 35 anos, foram criadas numerosas aplicações de rede engenhosas e maravilhosas. entre elas estão as aplicações clássicas de texto, que se tornaram populares na década de 1980: correio eletrônico, acesso a computadores remotos, transferência de arquivo, grupos de discussão e bate-papo e também uma aplicação que alcançou estrondoso sucesso em meados da década de 1990: a *Web*. Há ainda muitas aplicações multimídia, como vídeo em tempo real, rádio e telefonia por *Internet* e videoconferência. Duas aplicações de enorme sucesso também surgiram no final do milênio - mensagem instantânea e compartilhamento não hierárquico de arquivos (*peer-to-peer* - P2P).

Assim, todas as principais atividades praticadas pelo internauta se dão na chamada camada de aplicação, ficando o registro em cada sistema final mantenedor de sítio na rede mundial de computadores, bem como no computador do usuário. No entanto, os registros de conexão são, também, de grande importância, pois eles que atribuem o IP utilizado pelo internauta na conexão feita - afinal, atualmente, em regra, os IPs são rotativos e, caso o horário de um provedor seja incompatível com o horário oficial, é possível que se gere controvérsia na prova.

Sobre a camada de rede, explicam Soares, Lemos e Colcher (2004, p. 134):

> O objetivo do nível de rede é fornecer ao nível de transporte uma independência quanto a considerações de chaveamento e roteamento associadas ao estabelecimento e operação de uma conexão de rede. [...] No serviço de circuito virtual (serviço orientado à conexão), é necessário que o transmissor primeiramente envie um pacote de estabelecimento de conexão. A cada estabelecimento é dado um número, correspondente ao circuito, para uso pelos pacotes subsequentes com o mesmo destino. Nesse método, os pacotes pertencentes a uma única conversação não são independentes.

A tarefa da camada de rede é entregar pacotes IP onde eles são necessários. O roteamento é uma questão de grande importância nessa camada, assim como evitar congestionamentos. (TANENBAUN, 1997, p. 40). O sistema de rotatividade de IPs, por sua vez, se mostra necessário devido ao número de sistemas finais superior ao de registros possíveis, ao menos na atual versão IPv4:

Cada endereço no modelo do IPv4 tem comprimento de 32 bits (equivalente a 4 bytes). Portanto, há um total de 2^{32} endereços IP possíveis. Aproximando 2^{10} por 10^3, retira-se o número de cerca de 4 bilhões de endereços IP possíveis. O endereço IP de um hospedeiro pode ser configurado de duas maneiras: manualmente e pelo Protocolo de Configuração Dinâmica de Hospedeiros (DHCP). O último é o mais popular, porque permite que o IP seja conferido automaticamente, assim, sempre que um hospedeiro conectar receberá seu endereço de IP automaticamente. Na teoria, cada vez que o hospedeiro se conectar deve receber o mesmo IP, contudo, como o número de IPs na versão IPv4 tem se mostrado insuficiente, tem-se adotado a atribuição de endereço IP temporário. (KUROSE; ROSS, 2005, p. 260-266).

> Para atender a essa necessidade de maior espaço para endereços IP, um novo protocolo IP, o IPv6, foi desenvolvido. Os projetistas do IPv6 também aproveitaram essa oportunidade para ajustar e ampliar outros aspectos do IPv4 com base na experiência operacional acumulada sobre esse protocolo. [...] O IPv6 aumenta o tamanho do endereço IP de 32 bits para 128 bits, isso garante que o mundo não ficará sem endereços IP. (KUROSE; ROSS, 2005, p. 270-271).

Enquanto não houver registro único de IP, é preciso um cuidado especial por parte dos provedores de acesso, que são os responsáveis pelo armazenamento de registros a respeito de data e hora de conexão de cada máquina com certo endereço de IP. Não é difícil imaginar uma possível controvérsia probatória, por exemplo, se o horário do provedor for incompatível com o do NTP[2], pois o internauta que de fato estava utilizando o endereço de IP naquele momento deixaria de ser responsabilizado, recaindo o fato investigado sobre um inocente.

2 CONTEXTO ATUAL DO ARMAZENAMENTO DE REGISTROS E A PROPOSTA DO MARCO CIVIL PARA A *INTERNET*

Após a análise dos aspectos técnicos que envolvem o armazenamento de registros, necessário se torna enfrentar a questão sob a ótica jurídica. Enquanto no direito comparado, principalmente o europeu, existem determinações cogentes, no Brasil há apenas diretivas facultativas estabelecidas pelo Comitê Gestor de *Internet*. Com efeito, o Legislativo tem

[2] Pelo Network Time Protocol - NTP é possível saber exatamente a hora legal brasileira, que é a única considerada válida para fins de investigações (BRASIL, 2012e).

promovido debates controversos a respeito da regulamentação da matéria, em especial diante da tramitação do PL n. 2.126/11, ao mesmo tempo em que o Judiciário forma jurisprudência a respeito da responsabilidade civil dos servidores (provedor e mantenedor de sítio na *Web*) pela ausência de armazenamento de registros, notadamente os de aplicação.

Quanto ao tratamento feito na Comunidade Europeia, percebe-se uma disciplina que exige o armazenamento dos dados de acesso na *Internet* por parte dos servidores e os Estados-membros em que estão alocados, tendo por finalidade o fornecimento de informações no caso de requisição policial e judiciária. Basicamente, são quatro os diplomas que trazem tal regulamentação:

> - Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 (a Diretiva sobre Proteção de Dados) - harmoniza as leis nacionais que exigem práticas de gestão de dados de alta qualidade por parte dos "responsáveis pelo tratamento de dados" e as garantias de diversos direitos para os cidadãos.
> - Diretiva 2002/58/CE relativa à privacidade e às comunicações eletrônicas, de 12 de Julho de 2002 - garante o tratamento de dados pessoais e a proteção da privacidade no sector das comunicações eletrônicas.
> - Regulamento 45/2001 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, de 18 de Dezembro de 2000 - regula o tratamento dos dados pessoais das pessoas singulares quando esse tratamento é executado por instituições e órgãos comunitários.
> - Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. (UE, 2012).

Nessa linha de raciocínio, a Comunidade Europeia busca preservar alguns direitos que tangenciam o tratamento de dados, tais como: ser o internauta informado de que seus dados pessoais serão tratados e armazenados ao acessar um sítio; possibilitar o acesso e o saneamento de incorreções a respeito dos dados guardados; oferecer fundamentos legítimos para obstar o tratamento; não se sujeitar a uma automática interligação de seus dados com seu desempenho no trabalho, solvibilidade ou conduta pessoal; receber compensação pela violação das diretrizes (UE, 2012).

Em contrapartida, os responsáveis pelo tratamento de dados, ora empresas e pessoas que mantém sítios na *Web*, têm o dever de: assegurar a observância dos direitos dos internautas, informando-lhes sobre o tratamento de dados; fazer com que os dados sejam recolhidos apenas para os fins previstos em lei; tratar de forma legítima os dados, mantendo-os confidenciais; notificar à autoridade competente quando necessário, dentre outros (UE, 2012).

Percebe-se que a União Europeia está ciente de que propõe uma política de tratamento de dados um tanto quanto restritiva garantindo, como forma de compensação, que o internauta seja expressamente informado a respeito do tratamento de seus dados. Evidentemente que o sistema adotado não está isento a críticas, pois não impede, na sua totalidade, a proteção dos dados contra ações criminosas.

Segundo alguns Tribunais europeus, a lei, em vigor desde 2008, não teria proporcionado uma maior solução dos crimes praticados, posto que os usuários passaram a usar técnicas para evitar o tratamento de dados, tais como o acesso via cibercafés, *Wi-Fi*, telefones púbicos e serviços para tornar o usuário anônimo, a exemplo das técnicas de redirecionamento de IP. Ademais, alguns Tribunais Alemães e Romenos têm declarado a inconstitucionalidade da Diretiva da União Europeia, caso não seja demonstrada a necessidade de armazenamento dos dados. (IDG NEWS SERVICE, 2011).

A União Europeia chegou a rever as diretrizes, contudo, avaliou ser útil e necessária a obrigação de empresas de telefonia e *Internet* na Europa armazenarem dados dos usuários. Porém, mesmo assim, muitos países não cumprem com rigor as diretrizes, a exemplo da Holanda, que não informa aos seus cidadãos que estão sendo vigiados (PAPÔT, 2011).

Apesar das críticas, não se pode descartar que na Europa houve uma preocupação específica em efetuar o tratamento dos dados pela legislação. No Brasil, tal preocupação também existe, mas esbarra nas discussões do Congresso Nacional, que enfrentam duas correntes: uma que apresenta uma postura mais liberal e outra que busca a maior preservação possível da segurança jurídica.

As correntes são delimitadas por dois projetos de lei: o PL n. 84/99 e o PL n. 2.126/11. Ambos abordam a regulamentação na rede mundial de computadores de forma diversa: o primeiro busca uma intensa criminalização de condutas e uma atuação policialesca dos próprios provedores de *Internet*, enquanto o segundo prioriza a liberdade e a autonomia do usuário.

Quanto à guarda dos *logs* de acesso, o PL 84/99, de cunho estritamente penal, busca estabelecer uma disciplina rígida, na qual o polêmico artigo 22, rejeitado pela Comissão de Ciência e Tecnologia, Comunicação e Informática, mas não pelas demais comissões envolvidas em sua tramitação, entre as quais a Comissão de Constituição e Justiça, estabelece: a) dever de guarda pelo prazo de 3 (três) anos; b) possibilidade de fornecimento destes dados para qualquer investigação mediante requisição judicial; c) obrigação de preservar todas as informações requisitadas; d) informação de todo indício de prática de crime à autoridade

competente; e) elaboração de um regulamento a respeito dos sujeitos envolvidos no armazenamento de registros; f) multa pesada pelo seu descumprimento (BRASIL, 2012a).

O dispositivo não delimita o conteúdo dos registros que devem ser armazenados, ficando claro que nem se buscou um conhecimento técnico específico a respeito do funcionamento da rede mundial de computadores. Aliás, se ele tivesse sido buscado, não seria preciso remeter a especificação dos sujeitos envolvidos a um regulamento, o que gera até mesmo insegurança jurídica.

Por sua vez, o PL n. 2.126/11 prevê o armazenamento dos registros de conexão pelo prazo de 1 ano (artigo 11) (BRASIL, 2012b) - lapso temporal que vai ao encontro das Diretrizes Europeias - vedando que a responsabilidade por essa manutenção seja transferida a terceiros, mas não estabelecendo um sistema sujeito a constantes fiscalizações por auditorias.

No capítulo dos direitos e garantias dos usuários, em específico no artigo 7º, II[3], prevê a inviolabilidade e o sigilo das comunicações pela *Internet*, salvo por ordem judicial, nas hipóteses em que a lei estabelecer para fins de investigação ou instrução criminal (BRASIL, 2012c). Vale frisar que o sigilo das comunicações é tutelado pelo artigo 5º, XII da Constituição Federal e cabe à lei infraconstitucional discipliná-la como, por exemplo, o faz atualmente a Lei n. 9.296/96, que é alvo de discussão em sede dos debates legislativos por conta da reforma do Código de Processo Penal.

O artigo 10, § 1º do PL 2126/2011[4] limita o provedor responsável pela guarda de registros a somente fornecer informações que identificam o usuário mediante ordem judicial (BRASIL, 2012c). O servidor detém não só os registros de conexão e/ou acesso (conteúdo), mas, também, os dados cadastrais do internauta que é seu cliente, sendo que ambas as informações podem auxiliar na identificação da pessoa indigitada. Eventualmente, os órgãos encarregados da persecução criminal já dispõem do conteúdo, como, por exemplo, no caso de um *e-mail* injurioso, bastando, apenas, obter informações sobre os dados cadastrais do cliente que fez uso do IP na data e horário especificados. O projeto evidencia que a intenção do legislador é a de vincular dados pessoais enquanto sigilosos, tanto quanto os dados de conexão.

---

[3] Tal temática era inicialmente tratada no inciso I, o qual foi renumerado por conta da apresentação de substitutivo pelo Deputado Alessandro Molon (BRASIL, 2012b).

[4] "O provedor responsável pela guarda somente será obrigado a disponibilizar as informações os registros mencionados no *caput*, de forma autônoma ou associados a outras informações que permitam possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo." (BRASIL, 2012b).

A análise do artigo 5º, XII da Constituição Federal[5] permite concluir que no ordenamento brasileiro se tutela a inviolabilidade dos meios de comunicação - em cujo contexto se insere a comunicação de dados ou, nos termos do artigo 1º, parágrafo único, da Lei n. 9.296/1996, o fluxo de comunicações em sistema de informática e telemática. Nessa linha de raciocínio, os dados cadastrais do cliente do provedor não estão na esfera de proteção constitucional.

Em que pese se reconhecer, atualmente, que informações como nome, números de RG e CPF, bem como o endereço do cliente do provedor de *Internet* (dados pessoais) não são dados sensíveis, isto é, não se tratam de conteúdo de comunicação de dados (pacotes) ou fluxo de comunicações em sistema de informática e telemática, torna-se claro que estes dados merecem alguma proteção mas, talvez, não tão abrangente quanto a que a Constituição prevê para as comunicações, em que se exige autorização judicial para a quebra do sigilo, sob pena de dificultar em excesso a apuração da autoria de possíveis ilícitos.

Afinal, sigilosas, perante a lei, são as informações pertinentes ao conteúdo acessado pelo usuário da rede, ou seja, quais sites acessou, por quanto tempo, a natureza das informações veiculadas pelos domínios acessados, o número do IP utilizado pelo internauta para o acesso, enfim, todos os *registros de conexão e aplicação* (!). Sobre estes registros, que são o cerne da temática do presente artigo, destacam-se os artigos 12 e 13 do PL n. 2.126/2.011:

> Subseção II
> Da Guarda de Registros de Acesso a Aplicações de *Internet*
> Art. 12. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de *Internet*.
> Art. 13. Na provisão de aplicações de *Internet* é facultada a guarda dos registros de acesso a estas, respeitado o disposto no art. 7°.
> § 1° A opção por não guardar os registros de acesso a aplicações de *Internet* não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.
> § 2° Ordem judicial poderá obrigar, por tempo certo, a guarda de registros de acesso a aplicações de *Internet*, desde que se tratem de registros relativos a fatos específicos em período determinado, ficando o fornecimento das informações submetido ao disposto na Seção IV deste Capítulo.
> § 3° Observado o disposto no § 2º, a autoridade policial ou administrativa poderá requerer cautelarmente que os registros de acesso a aplicações de *Internet* sejam guardados, observados o procedimento e os prazos previstos nos §§ 3° e 4° do art. 11. (BRASIL, 2012b).

[5] "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" (grifo nosso) (BRASIL, 2012c). Nota-se que todas as esferas de proteção referem-se a meios de comunicação, de forma que simples dados de identificação ou cadastrais não são protegidos, o que os retira da esfera de proteção constitucional.

Sistematizando o conteúdo dos artigos e considerando os aspectos técnicos enfrentados no primeiro tópico, pode-se afirmar que:

a) Provisão de conexão é a atividade de fornecer acesso à *Internet*, de maneira onerosa ou gratuita. O servidor responsável por esta provisão é conhecido como provedor. Caberá a eles guardar registros de conexão, inerentes à camada de rede, por exemplo, data e horário do acesso, incluindo fuso horário, além do endereço de IP utilizado. Com efeito, uma das principais responsabilidades do provedor é manter o registro dos horários de conexão alinhados perfeitamente ao horário oficial brasileiro (NTP), evitando controvérsias probatórias. Pelo artigo 12, estes não poderão guardar os registros de aplicação, que se referem ao conteúdo acessado na rede, ou seja, não poderão armazenar os conteúdos acessados pelo internauta que contrata o provedor para conseguir acessar a rede.

b) Isso não significa que os registros de aplicação não ficarão armazenados, pois embora os provedores estejam impedidos de guardá-los, os mantenedores de sítios na *Web* terão a faculdade de fazê-lo. Assim, o mantenedor poderá guardar todas as atividades praticadas pelos internautas no âmbito de seu endereço eletrônico - *e-mails*, conversas privadas, comentários publicados, páginas criadas e acessadas. Caso o mantenedor da aplicação opte por não guardar, não poderá ser responsabilizado. Somente em caso de prévia determinação judicial será possível condená-lo pelo não armazenamento. Por exemplo, havendo suspeitas da prática de um ilícito, será preciso pedir autorização do juiz para que a mantenedora de endereço na *Internet* passe a ter o dever de registrar os acessos de determinado internauta, a partir da determinação judicial.

Com efeito, o tratamento proposto pelo Marco Civil para a *Internet* no Brasil não é compatível, em alguns pontos, com o recomendado pelo Comitê Gestor de *Internet* e com o que tem sido decidido no Superior Tribunal de Justiça.

As Práticas de Segurança para Administradores de Redes *Internet*, do Comitê Gestor de *Internet* no Brasil, recomendam que:

> [...] os *logs* não podem ser mantidos on-line por tempo indeterminado, pois acabam por consumir muito espaço em disco. A melhor estratégia para resolver esta questão é transferir periodicamente os *logs* do disco para dispositivos de armazenamento off-line, tais como fita, CD-R ou DVD-R.
> É recomendável gerar um *checksum* criptográfico (tal como MD5 ou SHA-1) dos *logs* que são armazenados off-line. Esse *checksum* deve ser mantido separado dos *logs*, para que possa ser usado para verificar a integridade destes caso eles venham a ser necessários.
> Os *logs* armazenados *off-line* devem ser mantidos por um certo período de tempo, pois podem vir a ser necessários para ajudar na investigação de incidentes de segurança descobertos posteriormente. O Comitê Gestor da *Internet* no Brasil recomenda que *logs* de conexões de usuários de

> provedores de acesso estejam disponíveis por pelo menos 3 anos (vide http://www.cgi.br/acoes/desenvolvimento.htm). É aconselhável que os demais *logs* sejam mantidos no mínimo por 6 meses.
> É importante que os *logs* armazenados *on-line* sejam incluídos no procedimento de *backup* dos seus sistemas (backups são tratados na seção 4.9) (BRASIL, 2012d).

Logo, o CGI entende que os registros de conexão devem ser mantidos armazenados pelo prazo de 3 (três) anos, enquanto que os registros de aplicação precisam estar disponíveis por ao menos 6 (seis) meses. Por questões técnicas, recomenda-se a guarda de registros em discos como CDs e DVDs, evitando que o sistema se sobrecarregue de dados e fique passível de violações. De maneira geral, os servidores têm cumprido as recomendações do CGI, embora elas não sejam coativas. Com certeza, contribui para a adoção deste posicionamento o fato de o Judiciário constantemente decidir que o não fornecimento das informações requisitadas gera a responsabilidade civil do servidor.

É emblemático o seguinte julgado do Superior Tribunal de Justiça, do ano de 2010, sob o crivo da relatora Nancy Andrighi:

> [...] 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02. 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa *in omittendo*. 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na *Internet* (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de *Internet* (BRASIL, 2010).

Não havendo um meio suficiente de rastreamento do usuário que praticou um ato ilícito pela *Internet*, a responsabilidade ficará a cargo da mantenedora do *site* no qual o dano foi causado. De qualquer modo, o dano será ressarcido, somente se eximindo a empresa atuante na rede se trouxer dados suficientes para a identificação do autor do ilícito. Logo,

armazenar dados não é uma simples faculdade, pois pode gerar prejuízo para a mantenedora que será obrigada a responder pela reparação do dano.

Insta frisar, no entanto, que a responsabilização penal do autor da mensagem injuriosa fica inviabilizada em face da ausência dos registros de acesso, uma vez que, via de regra, não haverá possibilidade de identificar a autoria do delito. Afinal, mesmo que se identifique o IP da máquina de onde partiu o ato que gerou o dano, não se saberá ao certo quem a estava utilizando naquele momento.

Assim, sendo a recomendação do CGI um mandamento não imperativo, resta a faculdade de o servidor cumpri-la ou não, assumindo eventuais ônus por sua omissão, entre os quais se destaca a responsabilidade civil pela culpa *in omittendo*. Sob outro viés, percebe-se que não há nenhum impedimento em o provedor armazenar os dados de acesso à *Internet* por um prazo ainda maior do que o recomendado pelo CGI, o que gera uma insegurança para o internauta, que não sabe nada a respeito do tempo e do conteúdo dos seus dados guardados.

De um lado, tem-se um regramento não cogente, que tem sido cumprido de certo modo para evitar responsabilizações na esfera judiciária e que peca por não estabelecer exatamente os servidores responsáveis pela guarda dos tipos de registros (provedor ou mantenedor). Ademais, o prazo não cogente gera uma insegurança tanto por parte do servidor, que pode ser condenado na justiça mesmo tendo cumprido a diretiva do CGI, quanto por parte do usuário, que não sabe exatamente por quanto tempo e quem é efetivamente responsável pela guarda dos registros de acesso e aplicações de *Internet*, tampouco quais são as informações guardadas.

De outro lado, há uma proposta que limita os servidores envolvidos na guarda dos registros, inclusive efetuando alguma observação técnica do funcionamento da rede ao dividir as categorias de dados da camada de rede em relação aos da camada de aplicação, além de delimitar um prazo de guarda cogente. No entanto, diminui a esfera de proteção que tem se consolidado no Judiciário ao facultar a guarda dos registros de aplicação, eximindo de responsabilidade o mantenedor que não exercite esta faculdade.

3 DO CONFLITO ENTRE PRIVACIDADE E SEGURANÇA JURÍDICA: PONDERAÇÃO NO TRATAMENTO DOS REGISTROS DO INTERNAUTA

O conflito entre a privacidade e a segurança jurídica tem origem em um exercício abusivo da liberdade de expressão na *Internet*, uma vez que para se manter a privacidade resguardada se mostra necessário não armazenar qualquer espécie de registro das atividades na rede. Contudo, isso é prejudicial à segurança jurídica porque os usuários que excedem a

esfera de exercício da liberdade de expressão podem ofender direitos de outrem, que precisarão comprovar o ato ilícito por meio dos registros do que aconteceu na *Web*.

> O direito à privacidade ou direito ao resguardo tem como fundamento a defesa da personalidade humana contra injunções ou intromissões alheias. Esse direito vem assumindo, aos poucos, maior relevo, com a expansão das novas técnicas de comunicação, que colocam o homem numa exposição permanente (PAESANI, 2006, p. 49).

Se, por um lado, é preciso resguardar a privacidade do usuário, evitando intromissões alheias, por outro lado é necessário salvaguardar instrumentos que permitam a apuração de atos ilícitos originários de um exercício abusivo do direito de liberdade, muitas vezes ofendendo os direitos de privacidade e personalidade do usuário. A respeito dos limites da liberdade na rede, Daoun e Blum (2000, p. 118) comentam:

> Usando o abalo na credibilidade da rede e nos sistemas de comércio eletrônico, há quem defenda a opinião de que a *Internet* precisa de maior controle e regulamentação. Alguns sites de *hackers* chegam a dizer que os verdadeiros responsáveis pela ação são governos e setores conservadores, que buscam um motivo para limitar a liberdade dos usuários na rede. Para os que sustentam tal posição e que defendem insistentemente a chamada liberdade virtual, o direito específico e regulador das questões da criminalidade na rede será sempre encarado como uma "camisa de força" imposta pelos poderes estatais; afinal, segundo os mesmos, o ciberespaço deveria ser regido com base em um sistema que ultrapassa o liberalismo *latu sensu* e beira o anarquismo, onde toda a forma de interferência dos poderes constituídos revelar-se-ia no mínimo inaceitável e, por isso mesmo, ilegítima.

Impossível defender que o Estado deve se manter alheio aos acontecimentos na rede mundial de computadores, afinal, os atos ali praticados produzem relevantes reflexos no cenário jurídico. Contudo, a *Internet* naturalmente proporciona um exercício maximizado do direito de liberdade, o que acarreta uma menor proteção da esfera da privacidade, mas também propicia a criação de um espaço democrático para debates, cabendo ao Estado se adaptar a este novo contexto.

> O ocultismo proporcionado aos usuários cria a ilusão de um ambiente livre para a prática de todos os atos. Verifica-se que o usuário cria a expectativa de poder utilizar a ferramenta virtual da forma que melhor lhe convém, sem raciocinar sobre as consequências que seus atos podem causar. É neste quadro peculiar de dinamismo que se desenvolve o exercício da liberdade na *Internet*, o qual não prejudica, por sua vez, os modos de caracterização de atos ilícitos. As condutas praticadas no ambiente virtual, tanto quanto as cometidas fora dele, são plenamente tangíveis e, caso produzam danos, acarretarão punição. (GARCIA; LUCA, 2012, p. 153).

É preciso encontrar um ponto de equilíbrio entre o que é necessário para uma preservação adequada da privacidade, sem que se perca em segurança jurídica nem se

diminua as possibilidades da liberdade de expressão. Afinal, todos estes direitos são resguardados pelo artigo 5° da Constituição Federal:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à *liberdade*, à igualdade, à *segurança* e à propriedade, nos termos seguintes: [...] IV - é livre a manifestação do pensamento, sendo vedado o anonimato; [...] IX - é livre a *expressão* da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; X - são invioláveis a *intimidade*, a *vida privada*, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] (grifo nosso) (BRASIL, 2012c).

Bem se sabe que todos os direitos fundamentais assegurados no texto constitucional são relativos, no sentido de que nenhum prepondera sobre o outro, cabendo efetuar uma ponderação de interesses em caso de conflitos. Se princípios colidem, um deles deve ceder, embora não perca sua validade e nem exista fundamento em uma cláusula de exceção, ou seja, haverá razões suficientes para que em um juízo de sopesamento um princípio prevaleça (ALEXY, 2011, p. 91-94). Não só o intérprete, mas também o legislador, ao definir os casos infraconstitucionais de limitações aos princípios, efetua uma ponderação. Em suma, o critério para a escolha de uma limitação ou outra envolverá a ponderação e o sopesamento de princípios fundamentais, com base na proporcionalidade:

> Uma das aplicações mais proveitosas contidas potencialmente no princípio da proporcionalidade é aquela que o faz instrumento de interpretação toda vez que ocorre antagonismo entre direitos fundamentais e se busca desde aí solução conciliatória, para a qual o princípio é indubitavelmente apropriado. [...] Contudo, situações concretas onde bens jurídicos igualmente habilitados a uma proteção do ordenamento jurídico se acham em antinomia, têm revelado a importância do uso do princípio da proporcionalidade (BONAVIDES, 2011, p. 425).

Considerado o conflito entre privacidade e segurança jurídica, que se fundamenta na vedação do exercício irrestrito da liberdade de expressão, surge a necessidade de equilibrar os interesses envolvidos, não prevalecendo um sobre o outro. Um dos métodos é a simples ponderação efetuada pelo magistrado no caso concreto, cabível quando não existir uma regulamentação específica (assim, é o método que tem sido adotado para se decidir a respeito do armazenamento de registros); outro é a elaboração de uma lei específica pelo Poder Legislativo, escolhendo os limites ao exercício dos direitos fundamentais assegurados na Constituição Federal no que tange a determinada questão jurídica (aprovada proposta legislativa a respeito da guarda de *logs*, a ponderação de interesses terá ocorrido em abstrato, com delimitação do exercício de direitos e deveres do cliente e do servidor pelo legislador).

Na *Internet* percebem-se diversas particularidades que implicam, necessariamente, na necessidade de flexibilização normativa e de alta aceitação social (vislumbrada numa alta compatibilidade entre o direito posto e o agir ético esperado dos usuários, aproximando-se o Direito da Moral). Os principais elementos da rede que se enquadram nesta categoria são: desterritorialização, isto é, relativização dos conceitos de espaço e tempo; alto dinamismo, consistente num intenso e inesgotável fluxo de informações; e elevada autonomia de ação, considerados os recursos da rede que possibilitam uma interação ativa dos internautas.

Corrêa (2000, p. 08) explica que a *Internet* proporciona "[...] um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento". Ainda, explica Lévy (2003, p. 13) que as telecomunicações geram um dilúvio de informações porque possuem uma natureza exponencial, explosiva e caótica, de modo que cada vez mais aumentam os dados disponíveis, a densidade dos *links* e os contatos entre os indivíduos.

Como um Direito estático, com excessiva normatização, conseguirá atingir todas as situações de conflitos presentes na *Internet*? Afinal, diariamente, surgem novas relações jurídico-sociais, variados conflitos que serão levados ao Poder Judiciário. O legislador não conseguiria acompanhar o ritmo de evolução e crescimento da *Internet*, acabando o ordenamento jurídico por ficar constantemente desatualizado. Por outro lado, a flexibilização normativa consolida-se no uso intenso da Nova Hermenêutica Constitucional, aplicando-se sempre que necessária a força normativa dos princípios enquanto instrumento de solução de colisões. Não somente o Direito será mais dinâmico, atendendo de forma eficaz os litígios decorrentes da rede, como também se mostrará mais compatível com os padrões ético-sociais, o que implica numa maior aceitação das decisões impostas.

Embora a tendência pela flexibilização normativa deva prevalecer na *Internet*, existem casos em que os argumentos favoráveis à elaboração de uma legislação específica parece prevalecer, como no que tange à regulamentação do armazenamento de registros de conexão e de aplicação. Aliás, por ser esta uma questão relativamente definitiva, ou seja, o sistema de camadas sempre funcionará e a guarda de registros permanecerá como uma realidade, a legislação dificilmente se tornará desatualizada, isto é, não será ilidida pelo natural dinamismo das relações jurídico-sociais na *Internet*.

No mais, o que se mostra como um argumento principal, a ausência de lei específica a respeito da guarda de registros de conexão e aplicação tem possibilitado uma maior violação não só da segurança jurídica (FURLANETO NETO; SANTOS; GIMENES, 2012, p. 171-172), mas também da privacidade. A princípio, poderia se pensar que a falta de uma norma

regulamentadora ampliaria a privacidade: afinal, não seriam guardadas as informações dos internautas sem uma lei determinando que isso fosse feito. Contudo, o armazenamento se tornou uma realidade, encontrando algum fundamento legal nas diretivas do CGI e na jurisprudência, que, por não estabelecerem critérios coativos, permitem a formação de um contexto de guarda de registros sem critérios determinados.

Existe uma falta de esclarecimento a respeito do conteúdo, do tempo e do responsável pela tutela dos dados do cliente do provedor de acesso à *Internet*. Aliás, muitos internautas desconhecem que por trás da rede está um complexo processo de armazenamento e guarda de dados - como visto, o regramento da União Europeia determina a prévia informação a respeito desta guarda. Com efeito, o cliente perde em privacidade, porque o direito ao esquecimento na rede não fica assegurado, isto é, os servidores não estão impedidos de guardarem os dados pelo tempo que quiserem; de outro lado, o cliente vítima de um ato ilícito perde em segurança jurídica, pois, caso um servidor opte por não guardar os registros de conexão e aplicação, a autoria de um ato ilícito não será apurada, embora seja provável a condenação cível do servidor.

Por sua vez, considerando a posição do servidor, percebe-se um verdadeiro contexto de insegurança jurídica, porque ainda que este atenda as diretivas do CGI, poderá ser condenado judicialmente. A título de exemplo, supondo que um mantenedor de endereço eletrônico na rede guarde os registros de aplicação por 6 meses, conforme diretiva do CGI, caso seja proposta demanda judicial de responsabilidade civil, é possível que o magistrado entenda que o dever de guarda não se resume apenas a 6 meses, condenando o mantenedor. Se existisse um tratamento específico, o servidor teria segurança a respeito do tipo de informações e do prazo pelo qual deve mantê-las em arquivo.

Logo, no conflito privacidade *vs*. segurança jurídica, no que tange ao armazenamento de registros de conexão e de aplicação, a falta de tratamento legal apropriado tem gerado predominantemente prejuízos, e não uma ampliação da privacidade ou da segurança jurídica. Assim, se mostra necessária uma legislação específica, sendo que a proposta do Marco Civil para a *Internet* é a que mais se aproxima das perspectivas a respeito da tutela do armazenamento de registros, porém, está longe do ideal.

No que tange ao prazo de guarda, de 1 ano para os registros de conexão e de 06 meses para os registros de aplicação, a proposta do PL n. 2.126/2.011 parece atender às necessidades de preservação da privacidade (pois limita o tempo de armazenamento) e de segurança jurídica (conferindo lapso para que se postule ao Judiciário o fornecimento de informações e, eventualmente, se viabilize a condenação do autor do ilícito).

Da mesma forma, a limitação de sujeitos responsáveis é coerente, impedindo o jogo de empurra-empurra entre provedor e mantenedor. Assim, enquanto o provedor se responsabilizaria pela guarda dos registros de conexão, ao mantenedor caberia armazenar os registros de aplicação.

Cabe crítica, no entanto, à previsão de que a guarda de registros de aplicação pelo mantenedor de serviço na rede deve ser facultativa. Tal proposta vai na contramão do posicionamento jurisprudencial atual e tende a tornar inócuas todas as tentativas de pedido de informações. Não obstante, a proposta contraria princípios estabelecidos pelo próprio PL n. 2.126/11, nomeadamente no que tange à responsabilização dos agentes:

> Art. 3° A disciplina do uso da *Internet* no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição; II - proteção da privacidade; III - proteção aos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade da rede, conforme regulamentação; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; e VII - preservação da natureza participativa da rede. (BRASIL, 2012b).

Um diploma que prima pela preservação em equilíbrio da liberdade, da privacidade e da segurança jurídica não deve deixar brechas para que algum destes direitos seja exercido de uma forma abusiva. Nesta linha, embora a responsabilização de agentes seja uma regra, segundo o dispositivo acima, ela é excluída ao se estabelecer adiante a facultatividade de armazenamento por parte dos mantenedores de aplicações na rede.

Tem-se uma brecha legislativa que pode levar o Brasil ao patamar de uma ilha de impunidades. Levando em conta que o serviço de *netbanking* é uma aplicação de *Internet*, se tornaria muito difícil a apuração de um eventual crime de furto mediante fraude praticado por meio da rede mundial de computadores - em que o *cracker*, fazendo uso de um cavalo de troia, após ter capturado a senha e o número da conta corrente do cliente da instituição financeira, acessa o *netbanking* como se fosse o correntista e efetua transações fraudulentas (FURLANETO NETO; SANTOS, 2005, p. 611-612) -, uma vez que o PL n. 2.126/11 faculta o provedor de aplicações de *Internet* a guardar os registros de acesso, inviabilizando a investigação caso tais registros não tenham sido arquivados.

Em outra hipótese, em caso de portais que provêm aplicativos que permitem a interação com o internauta, por exemplo, com a possibilidade de o usuário inserir comentários diante de uma notícia ou de uma fotografia veiculada pelo portal, restará, casualmente,

inviável investigar eventual crime contra a honra por conta da possibilidade de o provedor de aplicações à *Internet* não ter guardado os registros de acesso respectivos.

Outra falha do projeto é a falta de esclarecimento quanto aos conceitos técnicos de registros de conexão e aplicação. A definição do artigo 5°, VI a VIII[6] parece ser muito sumária, não permitindo uma efetiva compreensão da técnica envolvida. E, como visto no primeiro tópico, referidos conceitos compreendem questões técnicas da Ciência da Computação que não estão ao alcance do operador do Direito, de forma que um maior aprofundamento seria importante.

Mais complexa, passando por um efetivo estudo de ponderação de interesses a ser transposto para a legislação positiva, é a questão das espécies de registros de aplicação que deveriam se sujeitar à guarda: conteúdos privados, conteúdos abertos ou ambos. Não seria razoável obrigar a guarda apenas dos registros de aplicação abertos ao público, exigindo quanto aos registros de aplicação privados prévia autorização judicial? Ou todos os registros merecem o mesmo tratamento? Trata-se de uma discussão importante, pois envolve questões afetas à redes corporativas ou mesmo *Intranet* e que não tem sido objeto de debates por parte dos legisladores, nem mesmo no âmbito dos debates do Projeto de Lei do Marco Civil para a *Internet*.

CONSIDERAÇÕES FINAIS

Conclui-se que o PL n. 2.126/11 tem o bônus de propor um tratamento razoável, em muitos aspectos, na questão do armazenamento de registros de conexão e de aplicação. Entretanto, é omisso em alguns pontos técnicos e apresenta uma redação eventualmente confusa, quando não controversa, com abordagem superficial em questões mais críticas que se referem ao conteúdo dos registros que devem ser guardados.

A definição quanto às responsabilidades de quem tem o dever de providenciar o arquivo de registros de conexão e de registros de aplicações de *Internet*, assim como o prazo previsto para que os provedores mantenham os arquivos, são avanços satisfatórios, porém, há um retrocesso quando se estabelece a faculdade de arquivo dos registros de aplicação da *Internet* por parte do mantenedor de *site* que fornece o aplicativo.

---

[6] "VI - registro de conexão - conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; VII - aplicações de Internet - conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet; e VIII - registros de acesso a aplicações de Internet - conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP." (BRASIL, 2012b).

A faculdade que se concede ao provedor de aplicativos à *Internet* contraria os princípios norteadores do próprio PL n. 2.126/11, nomeadamente no que tange à concretização das responsabilidades, e implica em uma lacuna legislativa que inviabilizará a investigação de eventuais crimes praticados por meio da rede mundial de computadores num abuso da liberdade de expressão.

A proposta legislativa seria mais efetiva se o Marco Civil para a *Internet* estabelecesse a obrigatoriedade do servidor de aplicativos de *Internet* manter os registros de acesso por 6 meses, medida que possibilitaria tutelar, concomitantemente, a liberdade de expressão, a privacidade e a segurança jurídica do usuário.

Quando se toma em pauta um assunto tão complexo como a ponderação de princípios constitucionais, seja no plano da interpretação judicial, seja no plano da elaboração das leis, é preciso muito cuidado para não criar obrigações excessivas ou impedir o exercício de direitos humanos fundamentais. O que se espera de um Marco Civil para a *Internet* é a garantia de um exercício salutar e democrático do ambiente virtual, sem proteger os criminosos, mas ficando vedada a perseguição daqueles que utilizam a rede com boa-fé.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2011.

ABELSON, Hal; LEDEEN, Ken; LEWIS, Harry. **Blown to Bits**: your life, liberty and happiness after the digital explosion. Crawfordsville (Indiana/USA): Addison-Wesley, 2008.

BONAVIDES, Paulo. **Curso de direito constitucional**. 26. ed. São Paulo: Malheiros, 2011.

BRASIL. Poder Legislativo. Câmara dos Deputados. **Projeto de Lei n. 84 de 24 de fevereiro de 1999**. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 10 jun. 2012a.

_____. Poder Legislativo. Câmara dos Deputados. **Projeto de Lei n. 2.126 de 24 de agosto de 2011**. Disponível em: <http://edemocracia.camara.gov.br/documents/679637/277cc749-e543-4636-9ddb-736144a9b654>. Acesso em: 10 jun. 2012b.

_____. **Constituição da República Federativa do Brasil de 5 de outubro de 1988.** Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 10 jun. 2012c.

_____. Ministério das Comunicações e o Ministério da Ciência e Tecnologia. Comitê Gestor da *Internet* no Brasil. **Práticas de Segurança para Administradores de Redes *Internet***. Disponível em: <http://www.cert.br/docs/seg-adm-redes/>. Acesso em: 10 jun. 2012d.

_____. Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações. **NTP.br**: A Hora Legal Brasileira, via *Internet*. Disponível em: <http://ntp.br/>. Acesso em: 10 jun. 2012e.

_____. Superior Tribunal de Justiça. **Recurso Especial n. 1193764/SP**. Relator: Nancy Andrighi. Brasília, 14 de dezembro de 2010. Disponível em: www.stj.gov.br. Acesso em: 24 fev. 2012.

CASTELLS, Manuel. **A Sociedade em Rede**. 9. ed. São Paulo: Paz e Terra, 2006. v. 1.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da *Internet***. São Paulo: Saraiva, 2000.

DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. Cybercrimes. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito & *Internet***: Aspectos Jurídicos Relevantes. Bauru: Edipro, 2000. p. 117-129.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crime na *Internet* e Inquérito Policial Eletrônico**. São Paulo: Edipro, 2012.

_____; GARCIA, Bruna Pinotti. Liberdade de expressão e autocensura na *Internet*. In: XX Congresso Nacional do CONPEDI, 2011, Vitória/ ES. **Anais do XX Congresso Nacional do CONPEDI**. Florianópolis: Fundação Boiteux, 2011. p. 3530-3553.

_____; SANTOS, José Eduardo Lourenço dos. Crimes informáticos: furto qualificado mediante fraude. In: XIV Encontro Preparatório para o Congresso Nacional do CONPEDI, 2005, Marília/SP. **A construção do saber jurídico no século XXI**. Florianópolis: Fundação Boiteux, 2005. p. 611-618.

GARCIA, Bruna Pinotti; LUCA, Guilherme Domingos de. Democracia digital: os rumos da regulamentação legislativa no ordenamento jurídico brasileiro. **Democracia Digital e Governo Eletrônico**, v. 1, p. 146-179, 2012.

IDG NEWS SERVICE. Retenção de dados de internautas não minimiza cibercrimes. **IDG *News Service***, 28 jan. 2011. Disponível em: <http://computerworld.uol.com.br/seguranca/2011/01/28/retencao-de-dados-de-internautas-nao-minimiza-cibercrimes/>. Acesso em: 20 jun. 2012.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a *Internet***: uma abordagem top-down. 3. ed. Tradução Arlete Simille Marques. São Paulo: Pearson Addison Wesley, 2005.

LÉVY, Pierre. **Cibercultura**. Tradução Carlos Irineu da Costa. 2. ed. São Paulo: Editora 34, 2003.

PAESANI, Liliana Minardi. **Direito e *Internet***: Liberdade de Informação, Privacidade e Responsabilidade Civil. 3. ed. São Paulo: Atlas, 2006.

PAPÔT, Thijs. Comissão Europeia mantém diretriz controversa. **RNW *News***, 18 abr. 2011. Disponível em: <http://www.rnw.nl/portugues/article/comiss%C3%A3o-europeia-mant%C3%A9m-diretriz-controversa>. Acesso em: 20 jun. 2012.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores**: das LANs, MANs e WANs às Redes ATM. 2. ed. Rio de Janeiro: Campus, 2004.

TANENBAUN, Andrew S. **Redes de computadores**. 3. ed. Tradução Insight Serviços de Informática. Rio de Janeiro: Campus, 1997.

UE - União Europeia. **Proteção de dados pessoais na União Europeia**. Disponível em: <http://ec.europa.eu/justice/data-protection/files/eujls08b-1002_-_protection_of_personnal_data_a4_pt.pdf>. Acesso em: 20 jun. 2012.