Segurança e combate ao terrorismo: uma breve análise da lei de retenção de dados na Alemanha

*Por **Prof. Dr. Jorge Alberto S. Machado**, Docente do curso Gestão de Políticas Públicas, da Universidade de São Paulo*

Data da publicação:

Novembro de 2008

Imagine, leitor, todas as suas comunicações por telefone, celular, e-mail e navegação na Internet sendo registradas e armazenadas durante três anos. Refiro-me a seus dados pessoais, a origem, destino e conteúdo dos e-mails enviados, suas ligações telefônicas, dados de horários de conexão com a Internet e com servidores, etc. Essa informação toda não estaria apenas acessível a órgãos de segurança, mas também a empresas (para controlar, por exemplo, se houve violação dos direitos de propriedade intelectual), e mesmo a pessoas físicas – talvez algum desafeto, seu chefe ou algum concorrente. E mais, todos os provedores de seu país onde estão armazenadas as contas de e-mail estariam obrigados a entregar aos organismos de segurança nacional a senha administrativa de acesso. Estes poderiam navegar livremente nesse oceano de informações dos usuários. Isso não é ficção, já existe. Desde janeiro de 2008, está vigorando na Alemanha a lei de segurança sobre informações, a *Telemediengesetz* ("Lei de Telemédia"). Seu objetivo é reter dados de telecomunicações entre os cidadãos com o objetivo de combater o crime e, em especial, o terrorismo.

O alcance da lei é relativamente semelhante, em termos de quebra da privacidade do cidadão, às emendas à FISA[1], aprovadas em 10 de julho de 2008 nos Estados Unidos. A lei de Telemédia, entre outras medidas, prevê a retenção de dados de todas as comunicações telefônicas (telefonia fixa e móvel), e-mails, assim como as informações sobre remetentes, destinatários, origem, data, local, máquinas utilizadas. Isso significa que todas as comunicações entre os cidadãos no país podem ser rastreadas, monitoradas e analisadas, não havendo mais privacidade entre as mensagens pessoais. São coletadas informações sobre preferências, hábitos pessoais e circunstâncias de vida de cada cidadão. O acesso a tais dados é garantido à policia, a promotores públicos, a serviços secretos e a autoridades de outros países. Tudo para "combater o crime".

UMA LEI QUE PODE VIRAR MODA NA EUROPA

A Lei de Telemédia se insere no quadro da Diretiva Européia 2006/24/EC. Aprovada em 15 de março de 2006 pelo Parlamento Europeu, a diretiva trata sobre "a retenção de dados gerados ou processados em conexão com a provisão de publicidade dos serviços eletrônicos de comunicações públicas ou redes de comunicações públicas, emendando a Diretiva 2002/58/EC". Seu objetivo é combater spam, identificar autores de páginas na Internet e obrigar os servidores a dispor os dados pessoais dos usuários de serviços no caso de conflitos privados específicos sobre conteúdos disponibilizados na rede.

Embora seja apenas "complementar" à diretiva européia, a lei alemã apresenta vários problemas:

• o escopo da retenção de dados constitui uma invasão excessiva na privacidade pessoal;

• ameaça atividades profissionais (como jornalismo) e políticas que demandam sigilo por questões éticas ou morais;

• viola o direito humano à privacidade;

• seu custo, em termos dos direitos fundamentais infringidos, é muito alto e não há evidencias de que seja

eficiente no combate ao terrorismo;

• causa constrangimentos aos cidadãos e aos negócios;

• discrimina e promove uma invasão excessiva na intimidade dos usuários de telefonia e serviços de Internet em comparação com quaisquer outros meios de comunicação (por isso tem sido chamada de Lei “Big Brother”).

A parte mais polêmica está no seu artigo 14. Há uma cláusula nele que diz que os provedores de Internet têm que entregar os dados pessoais- como nome, endereço ou senha pessoal - aos órgãos responsáveis para o cumprimento da lei. A justificativa para isso pode ser: “perseguição de crimes”, “o cumprimento dos dispositivos de ‘proteção ao cidadão’ da Constituição alemã e dos Estados federativos”, “prover de informações o serviço secreto federal *(Bundesnachrichtendienst)* e o Serviço da Proteção Militar *(Militärischer Abschirmdienst)*” e, pasmem, “garantir o direito de propriedade intelectual”. Isso significa que os interesses da indústria da música e do filme são colocados no mesmo nível dos serviços secretos. Formulada de maneira muito imprecisa, a lei permite, por exemplo, que tanto a indústria como indivíduos possam pedir dados pessoais no caso de dúvidas sobre a violação da propriedade intelectual.

Sendo tão amplas as possibilidades de quebra de sigilo nos dados, se antes eram as exceções que permitiam que isso ocorresse, agora o sigilo é que pode ser considerado uma exceção. A lei também é criticada por não regular as condições nas quais os órgãos públicos podem ter o acesso aos dados pessoais. Ela também aumenta a pressão sobre a autoria dos conteúdos que circulam na rede. Em um de seus artigos, a lei atribui mais responsabilidade aos bloggers, que passam a ser tratados como jornalistas. No entanto, deixa muitas dúvidas em relação a responsabilidade sobre conteúdos, links e serviços nos sítios Web. Como não há uma regulamentação específica sobre isso, na prática não há limites à aplicação da lei.

INOVAÇÕES JURÍDICAS E POLÍTICAS

A lei alemã saiu na frente e chama a atenção pelas seguintes características:

• é a mais rígida já implementada – complementar às diretivas européias de segurança, recrudesce-a enormemente;

• pode influenciar a implementação de leis semelhantes de combate ao terrorismo que têm sido discutidas nos países-membros da União Européia, servindo assim como paradigma para o tratamento de dados das comunicações digitais por parte de governos;

• impõe severas limitações às liberdades civis constitucionais, em especial à privacidade e à liberdade de expressão;

• traz inovações jurídicas ao contrapor o princípio da segurança às liberdades civis, dando mais peso ao primeiro, propiciando assim novas abordagens - não só jurídicas, como políticas - ao tema.

O “combate ao crime”, em especial ao terrorismo e à pedofilia, tem sido usado como justificativa para convencer legisladores e cidadãos pouco informados a aceitar leis tão invasivas. Os lobbies dos grandes veículos de comunicação e das organizações que reúnem gravadoras e estúdios de cinema têm pego carona na discussão para defenderem a manutenção de seus lucros, corroídos pela difusão das modernas tecnologias digitais, que tornaram banal o ato de transmitir e compartilhar arquivos. Mesmo considerando a diferença da natureza dos crimes, essa estratégia tem dado certo e a “violação da propriedade intelectual” tem sido posta como delito de igual importância ao terrorismo e à pedofilia.

O Comissário de Justiça e Segurança da União Européia, Franco Fratini, indicado por Berlusconi, defende a implementação de um sistema de filtragem em toda a Europa. Em boa parte dos países-membros tem se discutido propostas de controles sobre a rede que afetam a privacidade dos cidadãos e/ou a neutralidade da rede. Na Dinamarca e na França, tem sido discutidas propostas que permitem a quebra de sigilo dos provedores para controle sobre o compartilhamento de arquivos protegidos por copyrights. Na Grã-Bretanha estuda-se a implementação de medidas semelhantes a partir de 2009, caso os provedores não entreguem os dados dos usuários de forma amigável quando solicitados. Na Itália, para facilitar as investigações policiais, há um sistema nacional de filtragem aplicado ao único backbone que serve ao país. Curiosamente, o primeiro-ministro Silvio Berlusconi conseguiu aprovar no dia 22 de julho de 2008 uma lei que lhe garante a imunidade contra os processos

de investigação que responde enquanto for primeiro-ministro.

O BIG BROTHER ESTARÁ CHEGANDO À INTERNET BRASILEIRA

A implementação da lei alemã deve ter influência sobre as políticas de segurança nos meios digitais adotadas por outros países do mundo. No Brasil, tramitam no Congresso vários projetos de leis sobre cibercrime, de defesa à propriedade intelectual e combate à “pirataria” que resultariam, se aprovadas, na aplicação de medidas invasivas em nome do aumento da segurança e da proteção de negócios nas redes digitais. O senador mineiro Eduardo Azeredo (PSDB) apresentou um substitutivo, aprovado no Senado, para três projetos que visam regular a Internet no Brasil (PLS 76/2000, PLS 137/2000 e PLC 98/20030).

proposta do senador Azeredo, que vai à votação na Câmara dos Deputados, tem sido objeto de grande polêmica. Ela obriga a identificação dos internautas pelos provedores de acesso. A estes cabe impedir o acesso anônimo à rede, registrar e armazenar dados de conexões - como horários de entrada e saída, tempo de permanência na rede, os dados capturados (como músicas e imagens) -, e guardá-los por no mínimo três anos. O provedor terá de arquivar também informações do internauta como nome, endereço completo, data de nascimento, número do CPF, carteira de identidade e telefone. O projeto de lei determina que cabe aos provedores a responsabilidade sobre a veracidade das informações prestadas pelo usuários, e coloca-os sob pena de responderem judicialmente por possíveis incorreções. Aos provedores cabe também denunciar usuários suspeitos às autoridades – o projeto de lei atribui aos primeiros a tarefa de vigilância e controle que deveria caber ao poder público.

Alguns dos pontos mais polêmicos do Projeto são os que mudam os artigos 285-A e 285-B do Código Penal:

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

O projeto de lei define de forma muito ampla o que é um “dispositivo de comunicação” ou “sistema informatizado”:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

Assim, qualquer coisa que transmita ou armazene dados pode ser enquadrada como tais dispositivos ou sistemas, segundo a descrição do artigo 285-A. Como a lei de direitos autorais não permite cópia sem autorização, qualquer cópia simples que o usuário faça de um CD ou DVD legalmente adquirido, incorre em crime.

Pela lei do senador Azeredo, dezenas de milhões de brasileiros poderiam ser condenados de um a três anos de reclusão. A descrição do artigo 285-B força o estabelecimento na prática de um sistema de autorizações na Internet, uma vez que, por padrão legal, os direitos autorais sobre obra artísticas ou culturais são automaticamente protegidos, já tendo, portanto, proteção expressa por lei.

O projeto do senador Azeredo prevê também a retenção de dados dos usuários por três anos. Mesmo a

Convenção de Budapeste de combate ao cibercrime, bastante rígida em suas disposições, estabelece o prazo de três meses para isso.

Tal projeto afronta direitos fundamentais de privacidade, liberdade de expressão e acesso à cultura, consagrados respectivamente nos artigos 12, 19 e 22 da Declaração Universal dos Direitos Humanos e consagrados na Constituição Brasileira. Se implementada, essa lei poderia ser o primeiro passo para transformar a Internet brasileira num Big Brother, acabando com a liberdade e a privacidade dos usuários, sujeitando os internautas à bisbilhotagem geral e deixando-os a mercê de ação de juízes – freqüentemente não bem informados com respeito às características do ambiente digital.

Sabe-se que os verdadeiros criminosos da Internet dominam técnicas avançadas de criptografia, navegam anonimamente – não tendo dados privados a defender – e, às vezes, a partir de máquinas localizadas fora de seus países. Do ponto de vista prático, esse projeto é pouco eficaz no combate aos grandes criminosos na rede. Ele afeta principalmente o cidadão médio, que tem alguns de seus consagrados direitos fundamentais severamente ameaçados.

O argumento da necessidade de monitorar a Internet no combate ao crime tem sido usado com eficácia para convencer legisladores - e mesmo a parcelas da sociedade - a engrossar a cruzada para acabar com a privacidade dos cidadãos e a intimidá-los no exercício de suas liberdades de expressão e de comunicação. A Internet, para onde convergem outras tecnologias de armazenamento e transmissão de dados, permite o controle e monitoramento sobre as pessoas nunca antes visto na história. Esta discussão tem sido feita sem profundidade e com pouco debate junto à sociedade. O mais grave é que essas “exceções” legais aos direitos fundamentais têm sido aproveitadas com perspicácia por grandes corporações para defender seus supostos direitos comerciais. Isso ocorre mesmo em países desenvolvidos, como a Alemanha, e pode vir a ocorrer aqui no Brasil - se a sociedade não reagir a tempo.

Referências

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:p...

Backbone é a “espinha dorsal” por onde passam toda a troca de dados num sistema mais amplo.

http://www.senado.gov.br/comunica/agencia/pags/01.html

http://conventions.coe.int/Treaty/EN/Treaties/PDF/185-POR.pdf

---

1. N.E.: Foreign Intelligent Surveillance Act. Ver em http://www4.law.cornell.edu/uscode/50/ch36.html

Categoria:

- poliTICs 2