CÂMARA DOS DEPUTADOS

PROJETO DE LEI Nº 2.126 DE 2011

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

EMENDA DE PLENÁRIO Nº 35

(Ao Substitutivo do PL 2.126 de 2011)

Dá nova redação ao art. 17 do Substitutivo ao Projeto de Lei nº 2.126 de 2011 [redacted].

Art. 17 Os provedores de aplicações de internet são obrigados a guardarem os registros de acesso a aplicações de Internet pelo prazo de 12 meses, ficando o fornecimento das informações submetido ao disposto na Seção IV deste capítulo.

JUSTIFICATIVA

O substitutivo apresentado pela Comissão Especial destinada a analisar o popularmente chamado 'Marco Civil da Internet', não contemplou a guarda de registro de aplicações de internet, insculpindo no art. 17 como sendo vedada a guarda daqueles dados.

Ora, com a devida vênia do relator, aquela redação não merece prosperar, vez que a guarda, desde que sigilosa daqueles dados, podem ajudar sobremaneira uma investigação e/ou uma instrução criminal, pois aquela guarda deixará os rastros de quem acessou indevidamente contas de terceiros, que pode ser usado para cometer qualquer tipo de crime.

Pesquisando em legislações de outros países percebe-se de forma inequívoca que, todos os países do porte e representatividade do Brasil, trabalham no sentido de que suas legislações sobre internet obriguem a guarda de dados de auditoria. Também se constata que as recomendações de boas práticas exaradas pelas normas do COBIT(1), normas essas mundialmente reconhecidas, também

mostram que se deve guardar/manter os registros dos dados relativos aos acessos aos sistemas, via internet.

Ainda no campo internacional temos a **ISO 17799** (*International Standartization Organization*), devidamente homologada pela ABNT em setembro de 2001, estabelecendo que deva ser provida cópia da trilha de auditoria do uso das operações do sistema, inclusive, das concessões e revogações de contas em sistemas para ser auditada.

Outrossim, no âmbito de nosso pais, o **Manual de Auditoria de Sistemas do Tribunal de Contas da União (TCU)** já recomenda de forma insofismável que os órgãos devem guardar os registros das denominadas trilhas de auditoria(2).

São dados/informações que permitem a elucidação de casos rumorosos como os já conhecidos casos de violação do e-mail de Sua Excelência a Presidente da República Dilma Rousseff, quando ainda candidata(3) e o caso da invasão do computador da Atriz Carolina Dieckmann(4). Se porventura não estivessem guardados os dados necessários, não se teria a elucidação de tais situações expondo, no mínimo, aquelas pessoas a dúvida terrível de suas condutas que, já se provaram ilibadas, e os responsáveis devidamente identificados.

Também merece destaque as investigações levadas a efeito pela Polícia Federal na '**Operação Porto Seguro**', onde servidores públicos somente foram identificados, pelo fato de terem sido flagrados pelas auditorias de sistemas utilizados de forma indevida e que tinham as auditorias(dados) guardadas por tempo indeterminado (Ex.: Rede Infoseg do Ministério da Justiça).

Imperioso destacar que, na Lei nº 9.613 de 1998 (que Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências) já prevê o armazenamento de dados em seu art. 17-B, senão vejamos:

> Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas

telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

Como se vê no artigo supra, o armazenamento de dados é devido e instrutivo na apuração de crimes. Deixar de prever esse armazenamento temporário dos dados de aplicações da internet seria uma forma de revogar tacitamente o referido artigo da Lei de Crimes de Lavagem de Dinheiro, que é usado hoje como forma de ajudar e dar maior celeridade nas investigações criminais.

Não podemos fazer confusão entre a liberdade e o anonimato, ou estaremos criando os *"Black Blocs"* da Internet, além de, de certa forma, prejudicar ainda a economia do país, fazendo com que servidores aqui instalados se mudem para outros países, vez que nossa emenda resguarda estes servidores em futuras ações patrimoniais, vez que terão como dizer quem foi o usuário que cometeu determinado delito.

Assim sendo, pela fundamentação que demonstra de forma peremptória os riscos a que está exposto o cidadão que utiliza a internet, rogo aos nobres pares que apoiem esta iniciativa, para tornar obrigatória a guarda daqueles dados pelo prazo mínimo de 12 (doze) meses, sob pena de termos o Brasil como exemplo negativo no que concernem as boas práticas e normas reconhecidas internacionalmente.

Sala das Sessões, de de 2013

Deputado FERNANDO FRANCISCHINI
Lider do SDD

PSDB

DEM. PE

PPS

(1) **COBIT** (*Control Objectives for Information and related Technology* - Objetivos de Controle para Informações e Tecnologia correspondente), uma estrutura de governança de TI aceita internacionalmente e usada por grandes empresas em todo o mundo. O COBIT proporciona um conjunto de práticas internacionais geralmente aceitas e respeitadas que ajudam os conselhos diretores, executivos e gerentes a aumentar o valor de TI e reduzir os riscos correspondentes.

(2) **TRILHAS DE AUDITORIA (TCU)** - São rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. Conjunto cronológico de registros que proporcionam evidências do funcionamento do sistema. Estes registros podem ser utilizados para reconstruir, revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bom como para rastrear o uso do sistema, detectando e identificando usuários não autorizados.

(3) De acordo com o jornal "Folha de S. Paulo", em 2010, um hacker teria roubado informações de e-mails recebidos por Dilma durante o período eleitoral. Segundo o jornal, o rapaz tentou vender os arquivos à oposição, que recusou. A PF instaurou inquérito para apurar o caso. (Questionado sobre a suposta violação dos e-mails da presidente Dilma Rousseff, em 2010, enquanto ainda era candidata, divulgada pelo jornal "Folha de S.Paulo", ***Michel Temer afirmou que todos estão expostos***, não apenas Dilma. "Não é porque é a presidente da República. Eles invadem todo e qualquer site. É uma coisa que tem que ser regulamentada, de difícil regulamentação, não é fácil essa regulamentação, mas acho que o Congresso deve se debruçar sobre esse tema para verificar de que maneira apena aqueles que invadem os sites como têm invadido", argumentou Temer.)

(4) O caso Carolina Dieckmann - Em maio de 2012, crackers do interior de Minas Gerais e São Paulo invadiram o e-mail de Carolina Dieckmann, de onde baixaram as fotos íntimas da atriz. O conteúdo foi publicado na internet após Carolina resistir às chantagens dos criminosos, que pediram 10.000 reais para apagar as imagens. O caso da atriz serviu de combustível para agilizar a aprovação da nova lei. Foi aprovada a Lei 12.737, em dezembro de 2012 em caráter emergencial, após o vazamento de mais de 30 fotos digitais nas quais a atriz aparece nua. O episódio foi fruto de uma invasão ao computador pessoal de Carolina ocorrida em maio daquele ano. O texto da lei estabelece que pessoas que violem senhas ou obtenham dados privados e comerciais sem consentimento do proprietário sejam punidas com penas que variam de três meses a dois anos de prisão, além do pagamento de multa.