

Legislando sobre crimes digitais

Publicado no Jornal O Popular – GO

Pedro Antônio Dourado de Rezende *
10 de Novembro de 2006

Parte I

O senador Eduardo Azeredo (PSDB-MG) tem defendido sua proposta de substitutivo a projeto de lei sobre crimes digitais rebatendo críticos. Qualificando-os de anarquistas (no Correio Braziliense, em 8/11/06), ou, a uma “boa parte” deles, de desinformados (no InfoNews)¹. O tema merece melhor debate. Desqualificando-me dessas rebatidas, cito de início o § único do art. 21º do seu substitutivo:

"A identificação do usuário de rede de computadores poderá ser definida nos termos de regulamento, sendo obrigatórios para a pessoa natural os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento, um número de documento hábil e legal de identidade e endereço completo,"

donde, naturalmente, surgem dúvidas. Quem fará o regulamento? Quem poderá definir quem faz o regulamento? Quem definirá o que é “identificação do usuário”? Com base em quais critérios?

Na falta de respostas, cabe lembrar que esse dispositivo só surgiu em versões recentes da sua proposta. Em versões anteriores, em vez de “ou similar” (à senha obrigatória) havia opção pelo uso de certificado digital da ICP-BR. Opção que, por sua vez, tinha um detalhe interessante: imunidade contra novos crimes, ali tipificados, ao provedor que a impusesse a seus usuários.

Essa opção desapareceu, mas não porque consultores do Senado a condenassem em parecer técnico. A versão consoante ao parecer, preparada pelos especialistas de carreira escalados para aconselhá-lo nessa relatoria, ele descartou momentos antes da votação sobre o mérito, na comissão de Educação, Ciência e Tecnologia do Senado em 23/05/06.

Mantida naquela votação, a opção pelo método “certificados ICP-BR, com vantagens a quem o impuser” só foi substituída, no atual artigo 21º, pelo método “similar, a ser definida”, em versão posterior, depois que certas críticas ganharam visibilidade.

Críticas assentes na natureza daquela opção, no modo estranho de se analisar o seu mérito, no seletivo e reduzido acesso às cambiantes versões (exceto à atual), nos intrigantes precedentes em outras tramitações sob tutela do senador², já notório pela criatividade com mirabolâncias contábeis de campanha, que deixaram, com o perdão da palavra, uma digital impressão de lobby de quem faz comércio com certificados digitais.

Neste cenário, cabe indagar se “termos de regulamento” ressuscitarão aquela opção. Cabe indagar quem, no caso, ficará exposto às novas imputabilidades criminais, com o uso de certificados ICP-BR. Análise e opinião a respeito³ já ofereci, por solicitação, à autarquia responsável pela ICP-BR, o ITI.

Se aquela opção ressurgir das cinzas, a afronta à privacidade de usuários obrigados a aceitá-la será devastadora. Como representante da sociedade civil no Comitê Gestor da ICP-BR, relatei sobre esse

tipo de “risco legislativo”⁴ no I Fórum de Certificação Digital, promovido pelo ITI em 2003.

Quanto à privacidade, o senador alega ao InfoNews: "Não queremos o registro sobre quais sites o usuário visitou. Nosso projeto não fala sobre conteúdos, não desrespeita a privacidade do usuário". Provedores não são hoje obrigados a manterem cadastro nos moldes propostos, e ele diz: "os grandes provedores já fazem isso, mas só se quiserem. Nós queremos que todos adotem esta prática".

Não será apenas pela obrigação cadastral, cujo impacto ele despreza, que sua proposta desrespeita a privacidade. Como é comum ao se legislar sobre informática, haverá efeitos colaterais. O senador não pode, por exemplo, querer que todos os provedores no ciberespaço a adotem.

Lá fora, ou no Brasil, provedores têm hoje meios de quebrar, além dos dados cadastrais, a privacidade de seus usuários colhendo e vazando informações, até onde permita a cautela destes. Por outro lado, ao provedor leniente na identificação de usuários também faltam incentivos para essa quebra. Tampouco os atrai, pois as informações colhidas teriam, salvo exceções pontuais, pouco valor no mercado da espionagem, oficial ou paralela, e no comércio de informações privilegiadas, devido à pouca confiabilidade para cruzamentos, via dados cadastrais, com outras informações.

Assim, um dos efeitos colaterais será o aumento desse valor. E esse aumento produzirá, no lado escuro do capitalismo, estímulo para a quebra de privacidade. Pelo provedor ou por funcionários ladinos, já que demanda, pelo que se vê em noticiários, não falta. Sem falar do apetite totalitarista que esse valor desperta, no Estado e no mercado, como mostra a galopante grampeagem audiovisual, anabolizado pelo inciso IV do art. 22º.⁵

Se aprovada, o risco à privacidade dos usuários aumentaria, portanto, em razão inversa ao empenho e despesas com segurança, dos provedores jurisdicionados. Se esse empenho lhes for imposto "nos termos de regulamento", a mera manutenção desse risco em níveis atuais implicará, com a valorização das informações traficáveis, em aumento no preço médio dos seus serviços, para absorver o custo adicional com segurança. Isso esvazia o argumento de que a proposta não afeta a inclusão digital.

Pelo que, duas rebatidas do senador são incompatíveis. Ou a privacidade, ou a inclusão digital, ou ambas seriam negativamente afetadas. Cabe indagar, então, se vale a pena. Talvez sim, se a proposta beneficiar mais, no combate ao cibercrime, o lado certo. Mas qual lado se beneficiaria mais?

Parte II

O senador tem dito não acreditar que sua proposta empurre usuários para provedores e serviços sediados fora do Brasil, como forma de escapar à legislação nacional. Talvez não empurre para escapar da Lei, mas sim do rastreamento. Especialmente a quem ler, e entender, o que estiver escrito no § 4º do art. 154-A do Código Penal, hoje art. 6º do seu substitutivo.

Ali se imputa culpa, por acesso indevido através de conexão via rede de computadores, dispositivo de comunicação ou sistema informático, incluindo-se "programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente." (art. 339-C do CP)

Para um leigo em Direito, mas nem tanto em segurança na informática e em teoria realista do Direito, isso significa que, sob tal regime, qualquer usuário cadastrado em um provedor sediado no Brasil estará sujeito a pena de seis meses a um ano de reclusão, e multa, por qualquer acesso indevido que um vírus, um programa malicioso ou espião venha a fazer, a partir do computador que ele estiver usando, enquanto o estiver usando.

E não se iluda quem pensar que a condenação só viria se o programa que acessou indevidamente tenha com isso causado dano a terceiros. O crime é de mera conduta: basta que o programa pratique "acesso indevido", independente do resultado, mesmo sem seu conhecimento, para que seja enquadrado. Em crime cuja autoria será rastreável a você, graças à identificação positiva que seu provedor jurisdicionado fornecerá à polícia, se solicitado, ou mesmo por bisbilhotice⁵.

Com respeito à negligência para condenação culposa, tem-se que, se tal conduta ocorrer pelo uso do sistema hoje instalado em metade dos computadores (Windows XP), com atualização automática o usuário assume, deliberadamente, pelos termos das licenças de programas ali instalados, os riscos decorrentes de acessos programados por terceiros, sem o seu conhecimento e a partir do seu computador, a sistemas desconhecidos.⁶

Mas então, como saber se uma conexão feita por um programa, à revelia do usuário, acessa devida ou indevidamente alhures? Que diabos constitui um acesso indevido? Se for "não autorizado", por quem? Baseado em quê? Como a autorização é informada? E se não o for? A razão presumida para algo "estar na internet", não seria a de poder ser acessado?

A definição do tipo penal "acesso indevido" é aberta. Não está em lei, nem nesse substitutivo, nem por ele delegada a "termos do regulamento", que a proposta "define" sem definir. Mas funciona como uma cunha afiada para controle político do ciberespaço.

Um juiz poderá acatar a definição que lhe convier. Poderá se ver forçado a acatar alguma, dentre as quais a da suposta vítima, posteriormente ao acesso. "Vítima" que poderá combinar bolsos fundos com escrúpulos rasos. Pode-se especular, por exemplo, o status do acesso se o usuário estiver "apenas usando" software não licenciado. Amir Sader que se cuide.

Salomônico ou não, cabe indagar como reagiriam a esse regime os usuários imbuídos de intenção criminosa. Será que vão fornecer dados verdadeiros a um provedor no Brasil, para serem identificados positivamente quando suas conexões forem rastreadas? Ou será que vão fugir das novas imputabilidades criminais buscando provedor fora do Brasil, que não os rastreie?

E os imbuídos de intenção são? Será que só malvados e paranóicos iriam evadir rastreamento? E os que não engolem a pílula azul de Matrix? Será que também não, uma vez acessados (devidamente, espero) conhecimentos sobre riscos, desequilíbrios e efeitos nefastos que um tal regime induz? É claro que o senador tem direito e inteligência para crer no que quiser, mas a comparação seguinte pode ajudar.

Se um *cracker* invade o sistema de um usuário inocente, cujo provedor está no Brasil, e dali ataca alhures praticando crime, como ocorre cada vez mais na internet, uma investigação competente não se encerra com o rastreamento desse usuário. Ainda, se o *cracker* vacilar deixando rastro, pelo qual seu acesso ao sistema do usuário é rastreado, o provedor do *cracker* pode se negar a confirmar a conexão e a fornecer sua identidade, como tem feito a Google Inc. (em casos de pedofilia no Orkut), noutra jurisdição impunemente. O usuário vai esperar se indiciado, pois sua identificação, como autor do tal crime, não seria positiva.

Doutra feita, no mesmo cenário mas no regime proposto, a investigação poderá acabar mais cedo. Haverá identificação positiva, do usuário que supõe a si inocente, mas que estaria enquadrado noutra crime, de acesso indevido culposo. Se não, enquadrado estaria o seu provedor (no Brasil), por não identificar a "origem" do ataque. Um processo judicial já pode ser instaurado, com ou sem esperneio do indiciado: se inocente, não o será por negligência. O investigador e o cracker se despreocuparão: missão cumprida, mãos à próxima. Isso se chamará "alta produtividade", também de advogados.

Se cadastro resolvesse problemas de cibercrime, seria fácil banir celular de prisão e rastrear dinheiro sujo: responsabilizando-se operadoras e bancos. Se responsabilizar prestador resolve, então que continuem os bancos arcando com perdas por fraude em seus sistemas informáticos: elas já estão diluídas nas taxas de seus serviços, sem impacto visível nos lucros, cada vez mais abusivos.

Sem entender as razões pelas quais a proposta do senador produziria apenas os efeitos que alardeia, resta-me examinar rebatidas doutra ordem. A de que “a União Européia já aprovou projeto similar”, e a de que “a tendência é que o mundo todo passe por um processo de maior controle da internet”.

Sobre a primeira, o senador talvez se refira à convenção de Budapeste, realizada no âmbito da União Européia, cuja adesão é voluntária, e a convite. A Estônia e a Lituânia aderiram, a Alemanha não ratificou. E lá, um tribunal acaba de obrigar um provedor a deletar dados sobre usuários, para preservar-lhes a privacidade. O Brasil, busca companhias no ciberespaço.

Com projetos similares? As recomendações de Budapeste incluem a imputabilidade penal por “acesso ilegal”; contudo, “acesso ilegal” é definido pela Lei, e “acesso indevido” o é em novilingua. Entre os dois tipos, cabe toda a teoria realista do Direito. Desde Trasímaco, na República de Platão, até a mais avançada das tecnologias. Cabe, por fim, indagar: se os pretensos donos do mundo querem fazê-lo atravessar um tal processo, por que cargas d’água o Brasil deveria ser boi-de-piranha? Por que não um projeto de lei menos pirotécnico?

Referências

- 1- <http://info.abril.com.br/aberto/infonews/112006/07112006-18.shl>
- 2- <http://www.cic.unb.br/docentes/pedro/trabs/azeredo.htm>
- 3- <http://www.cic.unb.br/docentes/pedro/trabs/ITI.htm>
- 4- <http://www.cic.unb.br/docentes/pedro/trabs/forumiti.htm>
- 5- O inciso IV do art. 22 determina que provedores têm de vigiar seus clientes. O texto diz que a empresa precisará "informar, de maneira sigilosa, à autoridade competente (...) fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade".
- 6- <http://www.cic.unb.br/docentes/pedro/trabs/wga.html>

Autor

* Pedro Antônio Dourado de Rezende é matemático, professor de Ciência da Computação na Universidade de Brasília (UnB), Coordenador do Programa de Extensão em Criptografia e Segurança Computacional da UnB, ex-representante da sociedade civil no Comitê Gestor da Infra-estrutura de Chaves Públicas brasileira (ICP-BR). www.cic.unb.br/docentes/pedro/sd.htm

Direitos autorais:

O autor publica este artigo sob licença Creative Commons (CC NC-ND-2.0): Livre para republicações com Atribuição, uso Não Comercial e Não Derivável. (outras republicações requerem autorização expressa) Texto da licença em: <http://creativecommons.org/licenses/by-nc-nd/2.0/deed.pt>