Marco civil da Internet quer garantir que haja leis, sem restringir liberdades

O Marco Civil da Internet é uma excelente iniciativa conjunta da Secretaria de Assuntos Legislativos do Ministério da Justiça e da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (FGV), com o objetivo de combater a tendência de se estabelecerem restrições, condenações ou proibições relativas ao uso da Internet. O foco do projeto é o estabelecimento de uma legislação que garanta direitos, e não uma norma que restrinja liberdades.

Por meio de um trabalho colaborativo, com a participação de vários setores da sociedade, o texto final foi encaminhado ontem pelo Poder Executivo ao Congresso Nacional recebendo a denominação de Projeto de Lei 2.126/2011. Em rápida leitura, fica claro que haverá uma expectativa muito grande para o debate em torno do texto apresentado, especialmente em razão de alguns pontos específicos que já despertam preocupação entre os juristas e que, com absoluta certeza, deverão sofrer uma série de alterações.

Os princípios de proteção à privacidade e aos dados pessoais elencados no artigo 3º – são muito relevantes. Devemos vigiar o Estado (e também empresas privadas) nessas questões tão sensíveis envolvendo a tutela constitucional da intimidade/privacidade.

Sempre repito que: “Precisamos ficar extremamente vigilantes e atentos às ações governamentais em todo o mundo no processo regulatório da Internet.” E volto a afirmar também a grande importância do direito à liberdade de expressão e à privacidade neste século.

O direito de acesso à Internet a todos os cidadãos, previsto no inc. I, artigo 4º, também é outra importante disposição – sobre a qual, já comentei em março de 2010

De fato, não há mais como negar o status fundamental ao direito de acesso à internet. E a legislação constitucional brasileira, também não oferece nenhum impedimento para essa interpretação – por conta, especialmente, da grande importância que a internet ocupa em vários aspectos do nosso cotidiano, inclusive na relação entre o Estado e o cidadão. Eis a razão do artigo 7º – “O acesso à Internet é essencial ao exercício da cidadania”. No mesmo artigo, encontramos a excelente disposição acerca da inviolabilidade e sigilo das comunicações do usuário pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Muito conveniente também a disposição do artigo 9º, determinando que o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços, conforme regulamentação.

Essa disposição procura combater o absurdo desrespeito ao consumidor promovido por algumas empresas de telefonia e provedores por meio do conhecido “Traffic shaping”- como exemplo, com a

imposição de dificuldades técnicas para o tráfego de pacotes de dados em VoIP em detrimento da utilização do plano de voz contratado pelo usuário – entre outros abusos rotineiramente cometidos. O parágrafo único é relevante no tocante ao *Sniffing* em rede de computadores.

Já o artigo 10, que trata da Guarda de Registros – apresenta um ponto polêmico. Há quem critique o parágrafo primeiro, entendendo absurda a exigência de ordem judicial. No meu entendimento, é corretíssima e excelente a disposição do texto ao exigir que o provedor responsável pela guarda somente seja obrigado a disponibilizar as informações que permitam a identificação do usuário mediante ordem judicial.

No entanto, muitos problemas do art. 12 até o art. 16. O mesmo fenômeno que ocorre nas discussões do Projeto de Lei 84/99 – parece se repetir no Marco Civil (agora PL 2.126/2011), ou seja, a inevitável animosidade política entre governo e oposição continua repercutindo sobre a discussão técnica do tema que é de grande importância para o país. Há alguns colegas que insistem em causar perplexidade sobre o recorrente tema do registro de “logs”. Parece já ter ficado clara a diferença entre “dados de conexão” e “dados de tráfego”. Os dados que serão armazenados (segundo prometem – quero deixar isso bem destacado) serão somente os “dados de conexão” preservando a privacidade/intimidade dos usuários, exatamente como já acontece com a telefonia, onde é possível saber o número de quem fez a ligação, mas não o teor da conversa.

O registro de acessos não pode ser facultado, tem que ser obrigatório. Apesar de em algumas situações, não servir para absolutamente nada – como já expliquei em 2001 e novamente em recentes escritos sobre o PL 84/99: http://www.direitodainformatica.com.br/?p=952

Exemplo: a utilização por criminosos de Proxy servers, TOR, JAP, acesso a redes wireless desprotegidas, etc. O IP não é a solução de todos os problemas. Muitas vezes não vai servir para absolutamente nada em uma investigação policial. O criminoso pode ter utilizado uma rede wireless desprotegida, feito um proxy com JAP/TOR em vários layers, cometido os atos ilícitos e deixado rastros para um inocente que nada tem a ver com a questão. Os métodos tradicionais de investigação podem ser muito mais eficazes nesses casos. A astúcia humana e a capacidade de inovação desses “cibercriminosos” são incríveis.

É extremamente razoável que o provedor de conexão à Internet não seja responsabilizado por danos decorrentes de conteúdo gerado por terceiros. Seria um absurdo (especialmente tecnicamente) pensar de forma diversa. Logo, correta a disposição do artigo 14. Idem em relação a disposição do art. 15 – e parágrafo único. Corretíssimo ao exigir – salvo disposição legal em contrário – que o provedor de aplicações de Internet somente possa ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente. A ordem judicial é o meio idôneo para a remoção de conteúdos. O dispositivo está em harmonia com a garantia da liberdade de expressão, comunicação e manifestação de pensamento.

Já em relação ao artigo 16, precisamos refletir sobre o alerta de Renato Opice Blum: “O autor do crime poderá eliminar as provas ao ser avisado”, já que a redação é a seguinte: “Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o artigo 15, caberá ao

provedor de aplicações de Internet informarlhe sobre o cumprimento da ordem judicial.” – Há investigações em que o sigilo é fundamental para se conseguir encontrar o criminoso e todo o material probatório.

Veja que no artigo 18, cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, vida privada, honra e imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro. Também seguindo Opice Blum, o artigo 22 deveria promover a educação digital – e não apenas a inclusão digital.

Date Created
27/08/2011