

## O dever de fornecer conteúdo no Marco Civil e a prova pericial

A recente polêmica envolvendo a prisão do diretor do Facebook no Brasil por descumprimento de uma ordem judicial trouxe à lume debates acalorados tanto sobre a obrigatoriedade de tais empresas cumprirem a legislação nacional quanto sobre os critérios para aplicação das sanções eventualmente cabíveis em caso de não atendimento.

Pouco, no entanto, tem-se discutido sobre ponto crucial nesse e em outros casos semelhantes: a verificação da alegação de impossibilidade técnica para o cumprimento da ordem, por não haver o armazenamento do material requisitado. Nesse breve artigo, busca-se trazer elucidacões sobre esse ponto cuja análise prévia é indispensável para, somente então, se chegar ao debate daquelas outras questões, como obrigatoriedade e proporcionalidade das sanções.

O Marco Civil da Internet (Lei 12.965/14) é muito claro em seu artigo 10 ao prever que “*A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Parágrafo 2º: O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do artigo 7º*”.

Não se tem dúvida, assim, que o MCI prevê o fornecimento do conteúdo das comunicações, desde que nos casos previstos em lei – como no caso de investigação criminal (inciso XII do artigo 5º da Carta Magna<sup>[1]</sup>) –, porém não prevê obrigatoriedade da guarda de tais dados. Diferentemente dos registros de acesso à aplicação e de conexão, para os quais a lei não só prevê a guarda obrigatória como também permite a requisição até mesmo para processos cíveis.

Ora, se o provedor de aplicações não é obrigado a armazenar o conteúdo de comunicações, uma ordem que determina esse fornecimento, diante da recusa do provedor sob essa alegação, deve estar pautada em questões técnicas e não em meros “achismos”, como verificado em algumas decisões judiciais nos últimos meses, que vêm compelindo provedores de aplicações a fornecerem os conteúdos de comunicação.

Um entendimento existente é o de que as disposições do Marco Civil já seriam suficientes para que os provedores se estruturassem para registrar e armazenar tais comunicações, que seriam custodiadas com absoluta segurança e fornecidas somente por ordem judicial. Não restam dúvidas que esta é uma corrente minoritária.

Grande parte da doutrina, no entanto, indica que se o provedor não armazena o conteúdo das comunicações, não é obrigado a fornecer, referenciando ainda se tratar de “opção” das aplicações.

Nesta esteira de entendimento, a simples informação dos provedores de que “não guardam” tais comunicações seria suficiente para afastar o dever de fornecimento. Para os que assim pensam, o provedor estaria obrigado a fornecer o conteúdo, mediante ordem judicial, quando o armazenar.

A questão é polêmica, pois à parte contrária e ao Judiciário não se conferem elementos para apurar se realmente custodiam ou não os dados requisitados. Quem saberá o que se passa dentro da caixa preta dos provedores de aplicações?

A simples declaração unilateral de que "não armazenam" ou que se trata de medida "impossível" seria suficiente? Um dos exemplos polêmicos vem do WhatsApp, cujo provedor responsável, Facebook, se nega a fornecer o conteúdo de conversas realizadas entre dois indivíduos ou de "grupos", informando que não registra tais informações.

Embora negue, alguns indícios existem de que algum armazenamento de conteúdo (ainda que temporário) acontece, pois o reenvio de um conteúdo (um vídeo por exemplo) já enviado ao aplicativo não demonstra novo carregamento, o que supõe-se um "armazenamento paralelo".

Mas percebe-se, especulações, considerando que os usuários, vítimas e judiciário não sabem o que se passa "intramuros".

Assim, batalhas e divergências entre vítimas, autoridades e aplicações desta natureza continuarão existir, se não forem permitidos aos interessados meios de se comprovar a informação prestada pelo provedor de aplicações. Tramita no Senado o PLS 330/2013 (PL com tramitação mais adiantada), que trata da proteção dos dados pessoais, trazendo regras para as empresas que fazem o tratamento de informações pessoais, como deveres de relatórios, se submeterem a fiscalização e até a previsão de governança em privacidade, mecanismos que somada a uma fiscalização de um futuro órgão competente, com profissionais técnicos em seu quadro, contribuirão para amenizar tais dúvidas, inclusive relacionadas a dados de comunicação quando associados a dados pessoais.

Enquanto isto não ocorre, a mera "declaração de não guarda" feita pelos mesmos em casos específicos em que são demandados não pode ser enfrentada como verdade absoluta, cabendo ao provedor demonstrar neste sentido tal impossibilidade técnica.

A apresentação pelos provedores de seus termos de uso ou declarações não pode ser considerada verdade absoluta, eis não ser totalmente esclarecedora do ponto técnico e controvertido: guarda ou não guarda dos dados.

Neste sentido, não bastasse a inversão do ônus da prova, que poderá ser determinada inclusive com fulcro no artigo 373 do Novo CPC (Lei 13.105), a prova pericial poderá ser fundamental nestes casos, apta a demonstrar qual o limite técnico da contribuição que uma aplicação pode oferecer em um caso concreto. Nesse aspecto, o artigo 464 do NCPC facilitou a oitiva do *expert*, permitindo ao juiz, diante de controvérsias, valer-se da prova técnica simplificada, ouvindo especialista com formação acadêmica sobre o tema, que proferirá seu parecer sobre a possibilidade ou não no fornecimento, podendo se valer de outros casos idênticos no Brasil e Mundo.

Saber o que os provedores de aplicações efetivamente armazenam não se trata apenas de um uma medida para esclarecer pontos controvertidos em juízo, mas de garantia a privacidade dos milhões de usuários destas aplicações. Se não guardam as comunicações para fins de cooperação com autoridades, não devem guardar para suas finalidades corporativas, mormente se feita às escondidas dos

titulares dos dados (usuários das aplicações). Lembrando que nesse aspecto o Marco Civil prevê em seu artigo 7º, inciso IX, o consentimento expresso para coleta de dados pessoais.

Assim, o uso de prova técnico pericial, ainda que simplificada, e o estabelecimento de uma Autoridade de proteção de dados que igualmente desenvolva um padrão de cooperação para que possa conduzir auditorias neste sentido contribuirão não só para esclarecer grandes debates judiciais sobre o que é armazenado e não é, mas principalmente, para evitar que dados excessivos sejam armazenados e tratados por aplicações, sem que seus titulares tenham sequer conhecimento.

[1] XII – 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;**

**Date Created**

12/03/2016