

Provedor de serviços de armazenamento de arquivos armazenados em “nuvem”

A internet, reconhecida mundialmente como relevante ferramenta para realização de direitos fundamentais como a liberdade de expressão (entendida também como o direito à informação), é hoje utilizada também como instrumento para arruinar a vida de muitas pessoas. Instrumento, pois não é a tecnologia responsável diretamente pelos inúmeros casos de difamação ou vazamento de fotos e vídeos íntimos como no recente caso das atrizes americanas que tiveram suas imagens espalhadas pela web depois de terem sido acessadas por terceiros no serviço *iCloud* da Apple. Tais atos são promovidos por pessoas, que muitas vezes utilizam a tecnologia para tentar anonimato e, conseqüentemente, impunidade.

É importante registrar ser possível a identificação da autoria mesmo com o uso de subterfúgios tecnológicos e, a partir disso, buscar a punição, inclusive criminal, do autor da façanha. Vale lembrar que desde o início de 2013 a invasão de dispositivos informáticos é, no Brasil, conduta punível como crime pela Lei 12.737/12, a chamada Lei Carolina Dieckmann.

Entretanto, o que chama atenção nesse caso das atrizes americanas, não é o viés da punição criminal do envolvido diretamente pela obtenção ilícita (cuja punição no país norte-americano é bem mais grave do que em terra tupiniquim), mas sim a responsabilização civil do provedor de aplicações que armazena conteúdo do usuário na “nuvem”.

Analisando o caso como se tivesse ocorrido em nosso país (evitando assim esbarrar nas controvertidas questões acerca da jurisdição na internet), pode-se concluir que, sem dúvidas, a empresa ofertante desse tipo de serviço seria obrigada a indenizar os danos provocados à vítima. Pouco importando se o conteúdo vazado era de vídeos ou fotos íntimas, um artigo acadêmico em fase de produção ou um projeto sigiloso da empresa, por exemplo.

Ao contratar a hospedagem dos dados na nuvem, ao usuário é prometida a segurança de um armazenamento em servidores acessíveis a qualquer tempo, bastando estar conectado à rede mundial de computadores. Pode se dar como relação de consumo, daí aplicando-se o previsto no artigo 14 da Lei 8.078/90, quando sequer é necessário apurar eventual culpa do provedor ou, ainda, numa relação entre empresas (B2B), aplicando-se para tanto o disposto no artigo 927 combinado com o artigo 186, ambos do Código Civil Brasileiro, dada a negligência no armazenamento dos dados.

Ainda, a recente Lei 12.965/14, conhecida como Marco Civil da Internet, reforça o dever de reparação, bem como os cuidados com o armazenamento e tratamento dos dados do usuário. Logo em seu artigo 3º, ao estabelecer os princípios para o uso da Internet no Brasil, a novel legislação inclui em seus incisos II e III a proteção da privacidade e dos dados pessoais, sendo inevitável abranger nessa compreensão não só o conteúdo íntimo, mas como todos os arquivos armazenados na nuvem de titularidade do usuário adquirente do serviço.

Mais à frente, pela leitura do inciso I do artigo 7º, percebe-se o reforço ao dever indenizatório em caso de violação, quando inclui entre as garantias do internauta “a inviolabilidade da intimidade e da vida privada, sua proteção pelo dano material ou moral decorrentes de sua violação”.



Por sua vez, em relação ao dever de revisitar as políticas internas de proteção e tratamento dos dados, buscando a conformidade legal dos procedimentos de segurança da informação, encontramos diversas passagens na lei, visto que pela adequação dos documentos legais (incisos VI, VII, VIII, IX, XI do artigo 7º, parágrafo único do artigo 8º) surge, inevitavelmente, necessidade de maior controle interno.

De todo modo, o inciso 4º do artigo 10 não deixa dúvidas ao estatuir que: “*as medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais*”. Embora esse dispositivo remeta à futura regulamentação, entendemos que as empresas já devem se atentar, buscando utilizar as melhores práticas de segurança da informação.

Infelizmente, tem sido comum às novas empresas de tecnologia (startups) certa displicência quanto aos riscos que o negócio pode causar aos seus usuários, seja pelo uso de cópia de documentos legais, como termos de uso e políticas de privacidade sem observar a realidade de seu negócio e a legislação aplicável, ou mesmo pela ausência de gestão clara e efetiva dos dados manipulados (*compliance* em segurança da informação).

As recentes normas (Decreto do E-commerce e Marco Civil da Internet) começam a surtir efeitos na conscientização sobre a importância e cuidados necessários no tratamento dos dados, cabendo ao Estado agora o cumprimento de suas determinações, buscando minimizar ocorrências como as ocorridas com as atrizes americanas.

É preciso compreensão de que um vazamento de fotos ou vídeos íntimos, por exemplo, é extremamente grave, merecendo sanções severas e indenizações que realmente possam inibir a negligência na segurança dos dados. Às empresas cabe investir em boas práticas, reduzindo os riscos inerentes à atividade.