Opinião: Os alertas que vêm do megavazamento de dados

No dia 12 de janeiro deste ano, o site Ciso Advisor publicou a notícia de um megavazamento de dados de mais de 220 milhões de brasileiros [1]. Além disso, foram vazados dados de 40 milhões de CNPJs e 104 milhões de registros de veículos. Fotos de rosto, informações sobre o poder aquisitivo e score de crédito representam alguns dos dados vazados. Evento denominado *"o vazamento de dados do fim do*

gital Ronaldo Lemos. Lemos [3] atribui a excessiva dimensão do banco de dados vazado à Lei do Cadastro Positivo (Lei nº 12.414/2011), que fez incluir nos cadastros positivos todos os brasileiros, e não somente os que pedissem a inclusão. Isso criou bancos de dados enormes, aumentando a vulnerabilidade. Ele alertou, quando ainda estava em análise o projeto de lei, que esse risco existia. Para ele, é preciso reduzir os bancos de dados, que compara a navios petroleiros que, antigamente, eram compostos por um único tanque, o que fazia com que vazassem todo o petróleo no caso de acidente. Petroleiros mais modernos têm vários tanques independentes, o que diminui a dimensão dos vazamentos.

Ainda não são claras todas as consequências do megavazamento. Especialistas falam em efeitos que se estenderão por anos. Com os dados em mãos, criminosos podem se passar pelo titular dos dados e cometer diversos crimes. Dados já são vendidos na *dark web*. Inclusive, dados de autoridades públicas estão sendo vendidos separadamente [4].

O nosso vazamento é maior do que o que ocorreu nos Estados Unidos em 2017, quando uma empresa de análise de crédito, a Equifax, deixou vazar dados de cerca de 145 milhões de americanos [5]
. A Equifax aceitou pagar até US$ 700 milhões por sua responsabilidade pelo vazamento, em acordo com a Comissão Federal de Comércio (FTC), autoridade de defesa dos consumidores, e com os Estados. Desse dinheiro, em torno de de US$ 300 milhões serão destinados aos afetados, US$ 175 milhões irão para os Estados e US$ 100 milhões irão para o governo federal, como pagamento de multas.

Não há, ainda, informação segura sobre o responsável pelo vazamento brasileiro. Os indícios apontaram para a empresa Serasa Experian, principalmente o fato de que há dados do seu Mosaic, instrumento de classificação de consumidores. No entanto, a empresa nega que seja a origem do vazamento. Nossa sociedade depende hoje, fortemente, da atividade de coleta e tratamento de dados, tanto por entidades públicas, que planejam e executam políticas públicas a partir da análise de dados, como por entidades privadas, que fornecem às empresas dados fundamentais para que fechem contratos. À medida em que aumentamos essa dependência, precisamos também reforçar a responsabilidade de quem tem a guarda desses dados.

A negativa da Serasa Experian leva à necessidade de aprofundar as investigações. Mas também aumenta a sua responsabilidade, caso a investigação a aponte como origem do vazamento. É certo que não podem, ainda, ser aplicadas as penalidades previstas na Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709, de 14 de agosto de 2018), que, por força de dispositivo nela introduzido pela Lei nº 14.010, de 10 de junho de 2020, só poderão ser aplicadas a partir de 1º de agosto deste ano. Mas isso não afasta outras formas de responsabilização administrativa, por força da legislação de defesa do consumidor e civil que, como no caso norte-americano, pode ser apurada em ações individuais propostas por prejudicados ou em ações coletivas que venham a ser propostas. A empresa responsável precisaria comunicar qualquer incidente de segurança (48 da LGPD) e demonstrar as ações adotadas para minimizar dano. Esconder propositadamente agravaria a sua situação.

Pouco podemos fazer em uma atitude individual. Já podemos saber quais dos nossos dados foram objeto de vazamento. O site fuivazado.com.br permite o acesso a essa informação. Não adianta muito saber, pois não teremos como recolher tais dados e lhes dar nova proteção, mas, ao menos, nos alerta sobre o que tem circulado ao nosso respeito, informação que poderá ser usada, no futuro, na solução de possíveis usos ilegítimos dos dados por terceiros.

Já do ponto de vista coletivo, muita coisa precisa ser feita. É necessário que exista uma estratégia de convivência com as consequências desse vazamento. Autoridades públicas e entidades privadas precisam, daqui para a frente, considerar em suas políticas que os principais dados de todos os brasileiros circulam livremente na internet. Por isso, precisam repensar procedimentos que dependiam apenas desses dados. Novos protocolos de segurança devem ser adotados, o que não vai significar, ainda assim, a garantia de que a maioria das pessoas não sofrerá consequências negativas do vazamento.

Não imaginávamos que iríamos precisar tão cedo de uma atuação tão complexa da Autoridade Nacional de Proteção de Dados, instaurada recentemente. Ainda sem o seu principal instrumento para esse tipo de atuação, que são as punições às empresas, a nova agência precisa "amadurecer a carbureto", em diálogo com diversos agentes públicos e privados envolvidos no caso.

[1] https://www.cisoadvisor.com.br/registros-de-223-milhoes-de-brasileiros-e-40-milhoes-de-empresas-a-venda/.

[2] https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml.

[3] https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml.

[4] https://www.conjur.com.br/2021-fev-02/megavazamento-dados-ministros-stf-sao-postos-venda.

[5] https://exame.com/negocios/equifax-pagara-ate-us-700-milhoes-por-vazamento-de-dados-pessoais/.

Date Created
05/02/2021