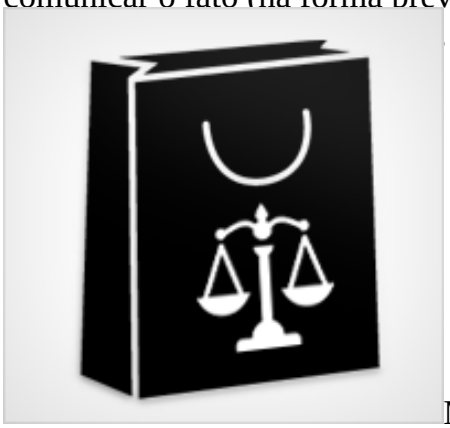
Vazamento de dados pessoais: mais do que vigiar e punir

São estarrecedoras as notícias de vazamentos de dados de brasileiros [1]. Ainda mais preocupante é o fato de os controladores apontados como prováveis fontes dos vazamentos não apenas terem deixado de comunicar o fato (na forma prevista no artigo 48 da Lei nº 13.709/2018, a Lei Geral de Proteção de



continuarem a negar a sua ocorrência.

Mas, para além de vigiar e punir, compete à Autoridade Nacional de Proteção de Dados determinar a adoção das providências necessárias para reverter ou mitigar os efeitos do incidente de vazamento. A efetiva proteção do cidadão pressupõe uma atuação conjunta das autoridades públicas que observe a amplitude da orientação principiológica e diretiva do microssistema de proteção e defesa do consumidor e sua aplicação harmônica em um verdadeiro *diálogo de fontes* [2] com as disposições normativas pertinentes à proteção de dados pessoais [3].

Notadamente, na sociedade de risco a indenidade é um valor inalcançável. Como revela a recente experiência do Superior Tribunal de Justiça, mesmo sistemas que contam com investimentos expressivos estão sujeitos a ataques cibernéticos [4]. Se por um lado a técnica de *naming and shaming* [5] pode servir com o incentivo aos investimentos na prevenção de danos [6], há uma segunda e perigosa face nessa mesma moeda: a que inibe a comunicação do fato lesivo dado o receio de redução do prestígio da empresa ou de imposição de graves sanções administrativas. Essa omissão dolosa do controlador que sofreu um incidente de segurança é a mais perigosa para o cidadão porque agrava o problema, obstando que as providências adequadas para conter os prejuízos do vazamento sejam adotadas tempestivamente. A passagem do tempo é, nesse caso, nefasta.

Para orientar os controladores de dados na decisão de como lidar com violações de dados e quais fatores a serem considerados durante a avaliação de risco, o Conselho Europeu de Proteção de Dados consolidou uma nova cartilha (*Guidelines 01/2021*), que está sujeita a consulta pública até o próximo dia 2 de março [7] e atua de forma complementar às *Guidelines* WP250, vigentes desde outubro de 2017 [8] . Lamentavelmente, os exemplos dos últimos vazamentos de dados de brasileiros equiparam-se aos casos mais graves (e de risco mais elevado aos cidadãos) exemplificados nas *Guidelines* europeias.

Embora seja de responsabilidade dos controladores estabelecer medidas adequadas para poder para prevenir, reagir e resolver uma violação de dados pessoais, há algumas diligências práticas que devem ser tomadas em todos os casos, tais como: a) informações relativas a todos os eventos relacionados à segurança devem ser direcionadas para um responsável, pessoa ou pessoas com a tarefa de tratar de incidentes, verificar a ocorrência de uma violação e avaliar os riscos; b) o risco para os indivíduos como resultado de uma violação deve então ser avaliado (probabilidade de não haver risco, há risco ou alto risco); c) notificação à Autoridade Nacional e comunicação da violação aos indivíduos afetados; e d) ao mesmo tempo, o controlador deve agir para conter e recuperar os dados pessoais violados.

Após ser informado de um possível incidente de segurança, o controlador pode empreender um curto período de a fim de estabelecer se ocorreu ou não uma violação de fato. Espera-se que a investigação inicial comece o mais rapidamente possível e estabeleça com um grau razoável de certeza se ocorreu uma violação, e as possíveis consequências para os indivíduos. Uma investigação detalhada deve ocorrer em seguida. Enquanto o artigo 48 da LGPD é omisso em relação ao que se considera prazo razoável para comunicação do episódio de vazamento à Autoridade Nacional (determinando apenas que a comunicação seja realizada *"em prazo razoável"*, a ser definido pela ANPD), a GDPR [9] limita esse intervalo a 72 horas desde o conhecimento do fato (GDPR, artigo 33).

É preciso estabelecer diretrizes claras para que os sistemas utilizados para o tratamento de dados pessoais sejam estruturados em consonância com os padrões de boas práticas e de governança (como prevê o artigo 49 da LGPD). No Brasil, a ABNT NBR ISO/IEC 27002:2013 orienta as práticas de gestão e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização [10]. A norma serve como diretriz das medidas mínimas necessárias para a prevenção de danos, mas ainda carecemos de regulamentação quanto às primeiras providências a serem implementadas diante de incidentes de segurança.

É imperioso comunicar à população, de maneira clara e ampla, quais os riscos envolvidos no vazamento de dados e quais cautelas devem ser, doravante, adotadas. Ainda que se reconheça que apagar as informações indevidamente disponibilizadas na *dark web* é missão quase impossível, a repreensão à comercialização do acesso a bancos de dados ilicitamente estruturados pode ser um primeiro passo para a efetiva proteção de dados pessoais. Os cidadãos têm, igualmente, o direito à informação acerca das providências implementadas pelas autoridades competentes para a prevenção e a reparação de danos.

Os procedimentos administrativos e judiciais adotados em face de episódios de vazamento de dados devem ser revestidos de uma natureza estrutural. As decisões estruturais [11] *"são decisões que se orientam para uma perspectiva futura, tendo em conta a mais perfeita resolução da controvérsia como um todo"* e são presentes em situações que *"exigem respostas difusas, com várias imposições ou medidas que se imponham gradativamente"* e buscam evitar que *"a decisão judicial se converta em problema maior do que o litígio que foi examinado"* [12].

A tutela coletiva pode ser significativamente aprimorada por meio de decisões estruturais ou convenções coletivas que estabeleçam, além do dever de reparação de danos, obrigações futuras e progressivas, exigindo-se dos envolvidos a apresentação de planos de ação adequados para assegurar a efetiva prevenção de novas ocorrências. O processo estrutural [13] (administrativo ou judicial) orienta-se para o futuro, ao invés de focar na lide que o ensejou, tem cabimento quando a complexidade da demanda exige uma visão mais ampla do contexto no qual está inserida, quando invoca a implementação de uma reforma global para prevenir novos litígios e danos, quando não se satisfaz adequadamente apenas com o arbitramento de uma indenização ou sanção administrativa. A repressão ao compartilhamento indevido de dados pessoais [14] exige uma atuação integrada das autoridades públicas e de todos os agentes do mercado, única maneira de mapear as falhas a serem corrigidas.

Que não se admita o surgimento, em pleno século 21, de uma nova forma de execuções em praças públicas, mas que o direito do cidadão à efetiva proteção de seus dados pessoais não seja menosprezado diante das dificuldades práticas da tutela. A constituição de uma sociedade livre, justa e solidária pressupõe que os agentes envolvidos ou atingidos por episódios de vazamentos de dados pessoais não se escondam sob o manto da incerteza, da insegurança ou da impunidade, mas assumam o protagonismo na busca por soluções céleres e eficazes reverter ou mitigar os efeitos do incidente de vazamento de dados. Mais do que vigiar e punir os culpados, é preciso, em primeiro lugar, proteger aqueles que foram afetados.

[1] “Juntos, os dois vazamentos continham: Dados básicos relativos ao CPF (nome, data de nascimento e endereço); Endereços; Fotos de rosto; Score de crédito (que diz se é bom pagador), renda, cheques sem fundo e outras informações financeiras; Imposto de renda de pessoa física; Dados cadastrais de serviços de telefonia; Escolaridade; Benefícios do INSS; Dados relativos a servidores públicos; Informações do LinkedIn.” Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml >. Acesso em: 15 fev. 2021.

[2] MARQUES, Claudia Lima. Diálogo entre o Código de Defesa do Consumidor e o novo Código Civil: o “Diálogo das Fontes”. *In:* MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 3. ed. rev., ampl. e atual. São Paulo: Revista dos Tribunais, 2010.

[3] Veja: MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (lei 13.709/2018): o novo paradigma da proteção de dados no brasil. São Paulo, Revista de Direito do Consumidor, v. 120, p. 555-587. nov./dez. 2018; DONEDA, Danilo (coord.). A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/Departamento de Proteção e Defesa do Consumidor, 2010.

[4] BRASIL. STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataqueâ?¯hacker. Disponível em: < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-informacoes-digitais-do-tribunal-apos-o-ataque%E2%80%AFhacker.aspx >. Acesso em: 15 fev. 2020.

[5] Metodologia de repressão de práticas abusivas, ilícitos civis ou criminais que busca atribuir um juízo negativo e socialmente inaceitável a determinada conduta.

[6] A sanção de imposição de contrapropaganda cominada ao fornecedor que incorrer na prática de publicidade enganosa ou abusiva é um dos seus primeiros exemplos no ordenamento jurídico brasileiro (arts. 56, XII, e 60 do CDC). Além da imposição de contrapropaganda há vários exemplos no ordenamento brasileiro de imposição legal de sanções de *shaming*, entre eles as aplicadas às pessoas jurídicas que tenham praticado infrações contra a ordem econômica (artigo 24, I e III, da antiga Lei de Concorrência – Lei 8.884/1994, atualmente correspondente ao artigo 38, incisos I e III, da Lei 12.529/2011); assim como previsão na Lei Anticorrupção de publicação de decisão condenatória (artigo 6º, inciso I, da Lei 12.846/2013) e a criação do Cadastro Nacional de Empresas Punidas – CNEP pela Lei 12.846/2013; entre outras. Veja mais em: SCANDELARI, Gustavo; POZZOBON, Roberson Henrique. Shaming como uma via para a sanção criminal de pessoas jurídicas no Brasil. São Paulo, *Revista Brasileira de Ciências Criminais*, v. 151, p. 75-114.

[7] EUROPEAN DATA PROTECTION BOARD. Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021. Disponível em: < https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexampl >. Acesso em: 15 fev. 2021.

[8] EUROPEAN DATA PROTECTION BOARD. Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018.

[9] *General Data Protection Regulation* (GDPR). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 15 fev. 2021.

[10] BRASIL. ABNT NBR ISO/IEC 27002:2013. Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Disponível em: < https://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em 15 fev. 2021.

[11] Fiss cita como surgimento da *decisão estrutural* o precedente da Suprema Corte dos Estados Unidos no caso Brown vs. Board of Education II (Brown II). Trata-se de caso marcante julgado pela Suprema Corte, que conclui ser inconstitucional as divisões raciais entre estudantes brancos e negros em escolas públicas no País. (FISS, Owen M. *The civil rights injunction.* Indiana University Press, 1978).

[12] ARENHART, Sérgio Cruz. Decisões Estruturais no Direito Processual Civil Brasileiro. São Paulo, *Revista de Processo*, v. 225, p. 389-410, nov. 2013. Veja a obra organizada pelo mesmo autor: ARENHART, Sérgio Cruz; JOBIM, Marco Félix (orgs.). *Processos Estruturais.* Salvador: JusPodivm, 2017.

[13] BERGSTEIN, Lais. *O tempo do consumidor e o menosprezo planejado.* São Paulo: Revista dos Tribunais, 2019. p. 220 et seq.

[14] Para os consumidores, atualmente a forma mais segura de verificar se os seus dados foram indevidamente utilizados é por meio do portal *Registrato*, disponibilizado pelo Banco Central em: < https://www.bcb.gov.br/cidadaniafinanceira/registrato>.