Consultoria Legislativa - Câmara dos Deputados

NOTA TÉCNICA

CONSEQUÊNCIAS DOS *MEGAVAZAMENTOS* DE DADOS PARA OS CIDADÃOS

Adriano da Nobrega Silva

Cassiano Luiz Crespo Alves Negrão

Claudio Nazareno

Guilherme Pereira Pinheiro

Thiago Rosa Soares

Consultores Legislativos da Câmara dos Deputados

Abril de 2021

SUMÁRIO

RESUMO

Esta Nota possui duas motivações principais. Em primeiro lugar, visa a esclarecer ao cidadão comum as possíveis consequências dos recentes *megavazamentos* de dados, fartamente noticiados pela imprensa. Como segundo desígnio, são oferecidas algumas reflexões sobre as medidas protetivas que poderiam ser implementadas de modo a diminuir o impacto desses recorrentes acontecimentos.

Após uma rápida contextualização acerca da importância do tratamento de dados pessoais para a vida das pessoas e das instituições, o trabalho apresenta a regulação do setor, ainda em processo de amadurecimento e de construção. Para se entender as implicações práticas dos *megavazamentos* na vida dos cidadãos, três grandes eixos de ações serão analisados. Em primeiro lugar, tendo em vista que o número 'universal' e aglutinador das atividades de uma pessoa é o Cadastro de Pessoas Físicas, serão apresentadas as possíveis ações com relação a esse número pessoal. Em seguida, considerando a profunda implicação desses vazamentos de dados na esfera de proteção e defesa dos consumidores, examina-se a eficiência da corrente infraestrutura normativa e cogita-se sobre os caminhos possíveis para fortalecer essa arquitetura. Como último eixo, aborda-se a dimensão judicial, instância definitiva de obrigações legais, responsabilização por abusos e de proteção dos direitos das pessoas atingidas pela disponibilização ilegal dos dados, e, alternativamente, as medidas administrativas possíveis diretamente junto às instituições.

Em conclusão, o trabalho sugere diversas ações protetivas tanto para promover uma maior transparência e facilidade de acesso às informações pessoais utilizadas pelos agentes de tratamento quanto para estabelecer mecanismos centralizados e imediatos de correção de uso indevido de dados pessoais.

Palavras-chave: tratamento de dados, vazamento de dados, privacidade, Lei Geral de Proteção de Dados Pessoais (LGPD)

INTRODUÇÃO

São cada vez mais comuns os casos de vazamentos de dados pessoais em território nacional. Apenas para ficarmos em alguns exemplos, tivemos recentemente notícias sobre a venda de pacote de dados, por R$ 38 mil, contendo informações de 112 milhões de pessoas. Dentre os dados tornados disponíveis estão o CPF, o nome completo, número de telefone e WhatsApp, a data de nascimento, nome da mãe, endereço, profissão, faixa salarial, eventual óbito, informações de cadastramento no Bolsa Família e de aposentadoria[1].

Outro caso trata do anúncio de venda de dados pessoais de 223 milhões de pessoas, incluindo CPF, números de telefones e outros, por cerca de R$ 94 mil. Os dados, nesse caso, teriam sido obtidos no Poupatempo, um programa de confecção de documentos do governo de São Paulo[2]. Inicialmente, a fim de atrair eventuais interessados, o vendedor dos dados ofertava gratuitamente 10 milhões de dados.

O vazamento de dados pessoais causa enormes transtornos para o cotidiano do cidadão e gera oportunidades de crimes de estelionato e os mais variados golpes. A vítima pode ter seu nome negativado, pagar contas indevidas, sofrer problemas junto à Receita Federal, ser chantageada, entre outros prejuízos e dissabores ainda piores, como furtos, roubos e até sequestros.

Esses acontecimentos de 2021 se somam a outros que foram ocorrendo paulatinamente de acordo com a digitalização dos serviços, públicos ou privados, e com o aumento do comércio eletrônico. Nesse ambiente digital, os dados passaram a ser insumos vitais para economia e consumidores, e, mais importante ainda, para a expressão e fruição de direitos e garantias individuais. Assim, se anteriormente para se ter acesso a serviços e bens de consumo, o indivíduo tinha que ser aceito pessoalmente em estabelecimentos públicos ou comerciais, na atualidade, a barreira se dá por uma senha pessoal e intransferível. Quando antes, para se fazer uma reclamação acerca de um serviço público o cidadão precisava ir até a repartição ou se utilizar de um telefone, atualmente, ele luta para não ser atendido por uma máquina. Para expressar sua opinião e ser ouvido, ele precisa entrar em uma rede social ou realizar um comentário em algum veículo de comunicação. Cartas aos jornais ou visitas pessoais

[1] Veja em: https://www.cnnbrasil.com.br/business/2021/03/16/megavazamento-hacker-quer-vender-dados-de-112-milhoes-de-pessoas-para-empresas . Acesso em 17/03/2021.

[2] Veja em: https://tecnoblog.net/421653/novo-vazamento-de-223-milhoes-de-cpfs-traz-celulares-e-mails-e-mais-dados/ . Acesso em 17/03/2021.

estão fora da realidade. A identidade digital é a mais importante hoje em dia, a que abre mais portas.

Nesse contexto de rápida transformação, em 2018 o Brasil se juntou a um grande grupo de países que possui uma lei específica para a proteção de dados das pessoas. Em que pese a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) não se encontrar totalmente em vigência,[3] um de seus principais objetivos é devolver ao cidadão a possiblidade de controlar seus próprios dados, garantindo assim o exercício do domínio sobre as suas próprias informações, sobre a sua própria vida, não apenas a digital.[4] Para isso o instrumento estabelece que o tratamento de dados pessoais, realizado tanto por entidades públicas quanto privadas, deve seguir uma série de princípios. Entre eles, destacam-se: serem utilizados para fins lícitos; serem processados e armazenados apenas o estritamente necessário (tanto em quantidade quanto no tempo); oferecer transparência; e garantia de segurança.[5]

De modo a regular essa atividade e estabelecer uma certa harmonia entre instituições e cidadãos, a LGPD determinou a criação de uma Autoridade Nacional de Proteção de Dados (ANPD). Caberá a essa entidade zelar pelas garantias dos direitos dos cidadãos nessa área. A LGPD revestiu a ANPD de diversos dispositivos para que esta exerça um verdadeiro poder regulatório. A autarquia poderá, por exemplo, fazer auditorias em empresas privadas e até no setor público, caso necessário. Ademais, foi indicada expressamente como "órgão central de

[3] As normas referentes à estruturação da autoridade nacional responsável pelo setor estão vigentes desde 28 de dezembro de 2018, enquanto as disposições gerais, direitos, princípios e finalidades já estão vigentes desde setembro de 2020. As sanções administrativas, por sua vez, só poderão ser aplicadas a partir de agosto de 2021.

[4] O art. 2º da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) determina:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

[5] O art. 6º da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) lista os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

interpretação" da LGPD e estabelecido que suas disposições deverão prevalecer na regulamentação das atividades de tratamento de dados.[6]

Assim, pode-se perceber que a ANPD possui figura central no endereçamento de procedimentos que visem a assegurar os direitos dos cidadãos na questão dos *megavazamentos*. Certamente não cabe à autarquia realizar procedimentos de investigação criminal, assim como, devido à sua recente e precária estruturação, não se espera que inaugure uma série de procedimentos operacionais nas empresas. Entretanto, o mandato legal é inconteste: caberá a ela estabelecer mecanismos – em coordenação e cooperação com os demais entes públicos e privados – visando à mitigação dos dissabores que poderão ser experimentados em *megavazamentos* por praticamente todos os brasileiros em curto, médio e longo prazo.

Todavia, o regramento dos dados pessoais não deve ser enxergado apenas sob a ótica da LGPD ou como sendo da alçada exclusiva da ANPD. É preciso ressaltar que todas as relações de consumo que envolvem ferramentas de comércio eletrônico, ou a simples coleta e guarda de dados, eram e continuam também sendo regradas pelas disposições gerais emanadas pelo Código de Defesa do Consumidor. Toda relação 'cidadão-instituição' mediada por dados, mesmo que sem vantagem econômica explícita e evidente, representa relação de consumo. Dessa maneira, os *megavazamentos* também devem ser analisados sobre a ótica do Código de Defesa do Consumidor (Lei nº 8.078/1990 - CDC), mesmo tendo este sido editado no início da década de 1990, portanto, em era anterior à internet comercial no País.

Outro viés de proteção e de reparação para o cidadão-consumidor é, obviamente, a via judicial. Em que pese o acesso ao Poder Judiciário ser um direito universal, deve ser avaliada a facilidade desse acesso e, neste caso específico, a dificuldade em se identificar os verdadeiros responsáveis pelos vazamentos. Embora a Polícia Federal já tenha realizado diligências e identificado diversos suspeitos,[7] a identificação da fonte de onde os dados provêm e foram extraídos (qual a empresa/instituição que foi *hackeada*) é tarefa árdua, ainda mais em se considerando a facilidade de replicação dos dados digitais e a possível multiplicidade de fontes. Outro ponto que dificulta a obtenção de sucesso pela via judicial é a necessidade de se provar

[6] Segue o art. 55-K da LGPD:

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.

[7] Ver em https://g1.globo.com/economia/tecnologia/noticia/2021/03/19/policia-federal-deflagra-operacao-contra-divulgacao-e-comercializacao-de-dados-pessoais-de-brasileiros.ghtml, acessado em 07/04/2021.

que houve negligência no trato dos dados, em alguns casos. Embora a regra geral da LGPD é de que qualquer entidade envolvida com o tratamento de dados é responsável por eventuais danos causados (reponsabilidade objetiva e solidária), o regramento excetua de responsabilidade determinados atores, quando eles atuaram de forma lícita ou tomaram as melhores precauções possíveis.[8]

Por último resta a alternativa administrativa. Os interessados devem verificar junto a cada órgão e instituição privada inconsistências em seu cadastro. Isso evidentemente possui diversos inconvenientes de ordem prática. Cabe ao cidadão todo o ônus de identificar os canais disponíveis e ele terá que contar com a boa vontade e a existência de canais amigáveis de atendimento. Esse procedimento ativo de busca não será nunca exaustivo, uma vez que o criminoso poderá abrir cadastros e contrair dívidas em empresas desconhecidas.

Como se vê, a livre circulação dessas informações poderá trazer imensuráveis problemas e os reflexos e mitigações devem se dar nas diversas esferas. As consequências desses vazamentos poderão se estender por anos a fio. Alguns terão a sorte de não sofrerem nenhum tipo de arranhão físico, moral ou patrimonial. Outros, no entanto, sofrerão os mais variados reveses. De certo é que, infelizmente, não existe a possibilidade de 'desvazamento' dos dados ou um retorno ao *status quo ante*. Nesse difícil cenário, as pessoas e autoridades terão a árdua tarefa de mitigar os efeitos negativos dessas ações.

Nesta introdução buscamos apresentar onde, no ordenamento jurídico institucional brasileiro, se encaixam os maléficos derrames multitudinários de dados. Neste documento iremos traçar algumas das ações individuais que poderiam ser tomadas e alternativas que carecem de aperfeiçoamento por parte do Poder Público.

No centro de todos esses cadastros, encontra-se o CPF. Por esse motivo, na seção seguinte, analisamos as consequências desses incidentes para o número de cadastro, mantido junto à Receita Federal e que está na raiz de todos os bancos de dados utilizados no Brasil.

[8] De acordo com o art. 42 da LGPD, entidades intermediárias envolvidas com o tratamento (denominadas operadoras) podem ser responsabilizadas se "descumprir[em] as obrigações da legislação de proteção de dados ou quando não tiver[em] seguido as instruções lícitas do controlador". Além disso, o art. 44, parágrafo único, combinado com o art. 46, permitiria a interpretação de que o agente de tratamento que adote "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas" poderia não responder por danos causados.

O CADASTRO DE PESSOAS FÍSICAS - CPF

O número do Cadastro de Pessoas Físicas (CPF), mantido pela Secretaria Especial da Receita Federal do Brasil, está na raiz de praticamente todos os processos de identificação das pessoas em território nacional. Desde a sua criação na década de 1960, o seu uso tem sido incentivado. Em 2018, se tornou obrigatório a sua inscrição, até nas certidões de nascimento, e, mais recentemente, com a aprovação da Lei nº 14.129/2021, o CPF é definido como "número suficiente para identificação do cidadão".[9] Assim, a manutenção da integridade desse binômio 'CPF-nome' possui fundamental importância ao longo de toda a vida das pessoas, para as instituições, ou, simplesmente para o bom funcionamento do país.

Conforme o art. 5º da Instrução Normativa RFB nº 1.548, de 13 de fevereiro de 2015, relativamente ao Cadastro de Pessoas Físicas administrado pela Secretaria Especial da Receita Federal do Brasil (RFB), o número de inscrição no CPF é atribuído à pessoa física uma única vez, vedada a concessão de mais de um número de CPF.

Assim, resta a questão do que fazer quando esse número atribuído para a vida toda passa a ser utilizado por outra ou outras pessoas, como pode vir a ser o caso devido aos vazamentos. Em que pese o número ser atribuído uma única vez para cada pessoa, conforme o mesmo diploma normativo, é possível a alteração de dados cadastrais nos seguintes casos:

> I - quando houver interesse da administração tributária;
>
> II - quando forem informadas por terceiros, em conformidade com convênios de troca de informações celebrados;
>
> III - em atendimento a determinação judicial; ou
>
> IV - para inclusão ou exclusão de nome social de pessoa travesti ou transexual.

Além dessas opções, a alteração de dados cadastrais pode ocorrer a pedido do interessado, especialmente nos seguintes casos[10]:

- mudança de endereço;
- mudança de nome (por motivo de casamento, divórcio, etc);
- inclusão/exclusão de nome social (somente para pessoas travestis e transexuais);

---

[9] A Lei 13.129/2021 que dispõe sobre o Governo Digital, determina:

Art. 28. Fica estabelecido o número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ) como número suficiente para identificação do cidadão ou da pessoa jurídica, conforme o caso, nos bancos de dados de serviços públicos, garantida a gratuidade da inscrição e das alterações nesses cadastros.

[10] Disponível em:
https://receita.economia.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/atos-cadastrais/alteracao-de-dados-cadastrais-no-cpf
Acesso em 17 mar 2021.

- inclusão de título de eleitor (ex: pessoas que não eram obrigadas a possuir o documento na época da inscrição); e

- corrigir dado cadastrado incorretamente na inscrição.

Não se estabelece em que condições é promovida alteração de ofício no interesse da administração tributária, mas apenas e tão somente que, quando realizada, ela será comunicada à pessoa física interessada. Uma situação em que isso pode ocorrer, a título de exemplo, é aquela em que é detectada incorreção no Cadastro em virtude de procedimento de fiscalização.

Relativamente às alterações promovidas pela prestação de informações por terceiros, é de se notar que podem ser praticados atos perante o Cadastro de Pessoas Físicas pelas seguintes entidades conveniadas:

I - Banco do Brasil S.A.;

II - Caixa Econômica Federal;

III - Empresa Brasileira de Correios e Telégrafos (ECT);

IV - instituições bancárias integrantes da Rede Arrecadadora de Receitas Federais (Rarf);

V - órgãos públicos estaduais e entidades públicas de atendimento ao cidadão;

VI - órgãos públicos federais;

VII - Associação dos Notários e Registradores do Brasil (ANOREG);

VIII - Associação dos Registradores de Pessoas Naturais do Brasil (ARPEN); e

IX - Comissão de Valores Mobiliários (CVM).

Conforme normativas da Receita Federal, desde julho de 2020 os Cartórios do Registro Civil, mediante convênio, podem prestar os serviços de inscrição, alteração, consulta e emissão de segunda via do comprovante de registro no CPF.

Também podem ser alteradas informações constantes do Cadastro de Pessoas Físicas em cumprimento de determinação judicial, o que pode se dar, por exemplo, no caso de casamento, separação judicial ou divórcio.

Como se nota, não é possível a alteração do número de inscrição no CPF pelas vias administrativas junto ao órgão gestor. Entretanto, vislumbra-se um possível caso de alteração por determinação judicial naquelas hipóteses em que a alteração de nome é concedida em razão de fundada coação ou ameaça decorrente de colaboração com a apuração de crime. Nessa hipótese, o juiz competente pode determinar a averbação no registro de origem de menção da existência de sentença concessiva da alteração. Porém, sem a averbação do nome alterado, que somente poderá ser procedida mediante determinação posterior, que levará em

consideração a cessação da coação ou ameaça que deu causa à alteração (Lei nº 6.015/1973, art. 57).

Além dessa hipótese, no caso de uso fraudulento dos dados de contribuinte, encontram-se decisões judiciais que determinam a alteração do próprio número de registro no Cadastro de Pessoas Físicas, conforme indica, a título de exemplo, o seguinte aresto:

> ADMINISTRATIVO. RESPONSABILIDADE CIVIL DO ESTADO. USO FRAUDULENTO DE CPF POR TERCEIRO. RECONHECIMENTO JUDICIAL DA NULIDADE DO DÉBITO OBJETO DOS AUTOS. DANOS MORAIS A CARGO DA UNIÃO. DESCABIMENTO. EXCLUDENTE DE NEXO DE CAUSALIDADE. EMISSÃO DE NOVO NÚMERO DE CPF. POSSIBILIDADE. PEDIDO GENÉRICO DE NULIDADE. NÃO CABIMENTO. [...]. 5. Comprovada a utilização indevida de CPF por terceiro é de se reconhecer o direito ao cancelamento e ao fornecimento de novo registro ao prejudicado, sob pena de perpetuação da fraude. [...]. 7. Remessa oficial e apelações improvidas. (TRF-5 - APELREEX Apelação / Reexame Necessário REEX 8001864120124058100)

Obviamente, não se pode cogitar de possibilidade ampla de alteração do próprio número do registro no CPF, dado que diversos órgãos e entidades fazem uso deste em seus cadastros.

Isso não obsta, todavia, que haja a previsão, na própria legislação que rege o procedimento administrativo de inscrição e alteração no Cadastro de Pessoas Físicas, de possibilidade de alteração do número de registro por solicitação do próprio contribuinte sem a necessidade de que este recorra ao Poder Judiciário mediante a comprovação do uso fraudulento de seus dados. Em virtude dos vazamentos de dados em larga escala, essa é uma alteração que deveria ser considerada, uma vez que é possível que contribuintes tenham seus dados utilizados de maneira indevida e reiterada, por terceiros, por tempo indeterminado. Lembrando que uma das mazelas do mundo digital é a impossibilidade de evitar a replicação contínua dos dados.

Tendo analisado a importância e a necessária rigidez do principal dado cadastral utilizado no país, passamos a avaliar o impacto das disseminações criminosas desses dados dos cidadãos sob o aspecto consumerista.

O DIREITO DO CONSUMIDOR

Sob o ponto de vista do direito do consumidor, é importante lembrar que o Código de Defesa do Consumidor (CDC) não aborda especificamente o tratamento de dados de consumidores por meios digitais. Como destacado na introdução, quando de sua edição, em 1990, o Código não poderia mesmo prever a ampla e rápida evolução das tecnologias digitais. A internet ainda engatinhava.

Não obstante, sua bem delineada arquitetura principiológica presta-se, ainda hoje, para resolver muitas das questões que se colocam em casos de preservação precária e uso inadequado de dados fornecidos no mercado de consumo. Vale lembrar que a relação de consumo se estabelece – e a cobertura protetiva do CDC, consequentemente, se aplica – nos serviços remunerados, ainda que a forma de remuneração do fornecedor se apresente fluida e indireta como em programas de milhagem, fidelidade e, no que importa particularmente ao tema aqui em discussão, nas informações pessoais concedidas às redes sociais e aplicativos de internet. Esses dados têm expressão econômica evidente para seus depositários e podem viabilizar uma variada sorte de negócios diretos ou indiretos.

Sendo assim, princípios como os da informação ampla e adequada, transparência, boa-fé, equilíbrio, dever de qualidade, efetiva reparação e prevenção dos danos causados, auxiliam o equacionamento de eventuais lesões, individuais e coletivas, independentemente do segmento de mercado em que ocorra e da tecnologia empregada. Nesse conjunto de princípios, aquele que estabelece a responsabilidade objetiva e solidária de toda a cadeia de fornecimento, por exemplo, tem sido frequentemente utilizado para retirar dos consumidores os ônus dos danos econômicos causados por falhas nas prestações de serviços que empregam meios eletrônicos.

Ao mesmo passo, as disposições que abordam os chamados bancos de dados e cadastros de consumidores, concebidas para tratar dos serviços de proteção de crédito (geridos pelos denominados birôs de créditos) e, mais recentemente, dos serviços de *scoring,* oferecem também algumas diretrizes quanto ao dever de fidedignidade dos dados, de sigilo relativo e, quanto aos direitos do consumidor, ao de acesso e à correção de inconsistências, dentre outras.

Obviamente, permanecem lacunas. E as dificuldades enfrentadas pelos consumidores prejudicados em situações de vazamentos de dados comprovam isso. O advento do Marco Civil da Internet e da Lei Geral de Proteção de Dados trouxe novas camadas de

direitos e obrigações no ambiente virtual. Ainda assim, é preciso pensar em ferramentas mais eficazes de prevenção, repressão e reparação dos prejuízos gerados pelo mau acondicionamento ou mau uso de dados pessoais dos consumidores.

Uma das dificuldades que, de imediato, despontam refere-se à impossibilidade prática de os consumidores saberem quem são os detentores de suas informações e, consequentemente, quais são os agentes envolvidos com o tratamento dos seus dados. A falta de um mecanismo prático que permita ao consumidor ter conhecimento sobre quais dados estão disponíveis e quem os detém traduz, de fato, um enorme desafio.

Outro desafio consiste na inexistência de meios eficazes para interceptar eventuais fraudes ou corrigir inexatidões, uma vez descobertas pelo consumidor.

É preciso constatar, contudo, que a solução mais adequada para assegurar proteção eficiente dos dados e responsabilizar os agentes pelo mau uso não deve residir exclusivamente nas leis de defesa do consumidor, ainda que se possa cogitar sobre o aprimoramento do instrumental de prevenção e reparação nelas existente. Trata-se de questão de implicações transversais, que ultrapassam o universo consumerista e que se comunicam com relações não albergadas pelo Código, como o uso e preservação dos dados por órgãos públicos e as relações entre agentes de tratamento e empresas (ou outras pessoas jurídicas).

Enquanto uma reflexão mais aprofundada sobre as formas sistêmicas de se mitigar os vazamentos de dados e de cobrar responsabilidades não se concretiza, pode-se, entretanto, pensar em medidas conjunturais de aplicação imediata.

Nos segmentos regulados, por exemplo, justamente aqueles onde as fraudes aparentemente mais têm-se multiplicado, é possível discutir novos modelos regulatórios ou novas ações administrativas que possam reduzir os transtornos enfrentados pelos consumidores que sofrem com o vazamento de seus dados. Atalhos poderiam ser oferecidos para a devida reparação de suas lesões morais ou materiais.

No campo do setor financeiro, campeão de fraudes, a existência do Conselho Monetário Nacional e do Banco Central, com competências normativas e fiscalizatórias – e de uma rede bastante eficiente de tráfego de informações no sistema de pagamentos – parece sugerir um caminho viável para facilitar a identificação e correção de fraudes com dados vazados. Atualmente, o Banco Central já disponibiliza o sistema "Registrato", que permite ao

consumidor (e empresas), consulta gratuita a relatórios de chaves Pix, empréstimos e financiamentos, contas em banco e contratos de câmbio.

Não há, entretanto, um sistema que permita ao cliente bancário ter acesso a uma comunicação direta, centralizada e imediata com as instituições financeiras, a partir da identificação de inconsistências lançadas no sistema "Registrato", com a finalidade de suspender as operações não reconhecidas. Cabe destacar que o Banco Central já disponibiliza o Sistema de Registro de Demandas do Cidadão – RDR (popularmente chamado de "Denúncia Bacen") por meio do qual o cliente que identificar operações não autorizadas no sistema financeiro pode registrar uma reclamação. Por meio desse registro, cabe à Autarquia encaminhá-la à instituição financeira que tem, por regulamento, prazo determinado para a resposta ao cliente.

O "Denúncia Bacen" é um modelo bastante parecido com o sistema "Anatel Consumidor", de suporte aos usuários de serviços de telecomunicações ou o "Cadastropré", lançado pelas operadoras para verificar a existência de linhas de telefonia pré-paga sob o mesmo CPF.

É relevante frisar que o Banco Central, embora não interfira individualmente nas reclamações, divulga *ranking* acerca do número de ocorrências recebidas e resolvidas pelas instituições e pode, eventualmente, dar início à fiscalização sobre um determinado ator, em vista de um número excessivamente elevado de reclamações congêneres apresentadas contra ele.

O uso do RDR, porém, não oferece a agilidade e a precisão desejadas para oferecer comunicação imediata com as instituições financeiras e permitir que sejam suspensas imediatamente as operações suspeitas, impedindo, assim, maiores prejuízos às vítimas de fraudes por dados vazados.

Um caminho possível, ao menos em tese, poderia consistir no uso da infraestrutura do "BacenJud" – sistema empregado pelo Poder Judiciário para identificar ativos em nome de partes em ações judiciais e promover a penhora *online*. Sabe-se que, atualmente, o Banco Central apenas viabiliza o curso das comunicações entre a autoridade judicial e as instituições financeiras, sendo o sistema acionado diretamente pelo Juízo, sem interveniência da Autarquia.

Em princípio, parece factível imaginar uma ferramenta que integrasse os sistemas "Registrato" e a interface de acesso e comunicação que o BacenJud oferece para propiciar o alerta instantâneo à instituição financeira envolvida na fraude ou, até, a imediata

suspensão de movimentação da conta ou de prosseguimento da operação de crédito. A grande dificuldade seria criar uma estrutura normativa que desse segurança jurídica a essa operação. Seria necessário assegurar à instituição financeira, sem que fosse preciso aguardar uma decisão judicial para tanto, que se trata de comando válido e emitido pelo cliente efetivamente lesado pela fraude. Isso, por um lado, conferiria a agilidade necessária para impedir maiores prejuízos aos clientes e, por outro, evitaria abusos e possibilitaria o retorno ao *status quo ante* caso a operação, posteriormente, se mostrasse regular.

Talvez, pudesse ser adotado o modelo que se aplicava à sustação de cheques, utilizado pelos bancos, em que a iniciativa do emitente se mostrava suficiente para impedir o pagamento do cheque ao portador, respondendo o emitente por eventuais abusos. Essa inspiração poderia desenhar um novo sistema a ser concebido para lidar com as fraudes no sistema financeiro aqui em debate.

Em síntese, do ponto de vista das relações de consumo, infelizmente, não há um sistema que centralize todas as demandas de modo a simplificar ações administrativas pelos consumidores eventualmente lesados. Cabe ao cidadão consumidor descobrir quais os canais de reclamação e verificar a existência de fraudes. Certamente uma unificação, como a que o Banco Central assegura com o sistema "Registrato", seria de extrema relevância, pelo menos para todos os serviços públicos, em que pesem os diferentes níveis federativos envolvidos de acordo com cada serviço. Faltaria, ainda, conceber uma ferramenta que pudesse congregar todas as iniciativas de comércio eletrônico.

Independentemente da falta de centralização e da obscuridade quanto aos canais a serem utilizados, o cidadão sempre poderá se utilizar da via judicial para procurar a devida reparação. As ações propostas no âmbito do Poder Judiciário são objeto da seção seguinte.

AÇÕES JUDICIAIS E ADMINISTRATIVAS

Diante dessa situação de aparente descontrole acerca dos dados pessoais, emerge a questão da via judicial e da responsabilização pelos danos causados. Quais os caminhos que a legislação já prevê para permitir ao cidadão lesado e vítima do vazamento de seus dados a obtenção da devida reparação? Quais ações administrativas podem ser tomadas diretamente junto às instituições envolvidas?

O cidadão comum precisa de certo conhecimento mínimo que o ajude a enfrentar processos que deveriam ser simples e diretos. Por exemplo, na rápida reparação por danos materiais junto aos estabelecimentos (bancos, operadoras de telefonia, lojas, etc) que autorizarem contratação de serviços com a utilização fraudulenta de dados. Outro procedimento que deve ser facilitado é a notificação formal das autoridades envolvidas e competentes, de acordo com cada caso, no sentido de indicar que seus dados foram vazados e estão sendo utilizados criminosamente por terceiros. Existiria alguma forma de rito judicial sumário que poderia ser aplicado?

Felizmente, a legislação já fornece algumas alternativas. As demandas de reparação de danos materiais (e também morais) já encontram guarida na Lei nº 9.099/1995, que criou os Juizados Especiais, que costumam ser mais expeditivos na resolução das demandas. Essas ações podem ser formuladas pelo próprio cidadão prejudicado, desde que limitadas a 20 salários mínimos. Já quando o valor da causa for superior a esse montante e inferior a 40 salários mínimos, é obrigatória a assistência por advogado.

Com relação à notificação de autoridades competentes (por exemplo, Receita Federal, instituições bancárias ou comerciais), é fundamental que o juiz inclua na sentença a remissão dos autos (ou cópia da sentença) para as referidas autoridades. Dessa maneira, a instituição teria acesso a uma prova pré-constituída, o que permitiria a aplicação de sanção administrativa, simplificando o rito administrativo necessário. Se não houver a remissão, o próprio interessado poderia deflagrar o processo investigativo junto ao órgão competente notificando-o administrativamente acerca do resultado dessa ação legal.

Em paralelo às ações individuais, as instituições de cuja falha ou negligência de seu dever de guarda dos dados decorreram os vazamentos em larga escala poderiam ser responsabilizadas mediante o manejo de uma ação coletiva.

Por se tratar de direitos individuais homogêneos (CDC, art. 81, III), a tutela do interesse individual dos consumidores que tiveram seus dados vazados pode ser requerida. Nesse caso, a ação é proposta pelo Ministério Público ou outro legitimado (CDC, art. 82), habilitando-se a vítima ou seus sucessores a promover a liquidação (quantificação do dano) e a execução (CDC, art. 97). No entanto, seria controvertido exigir uma indenização por danos morais pelo simples vazamento de dados, cujo reconhecimento tende a ser dificultado quanto maior for a escala do vazamento.

Outra forma de atendimento ao interesse da coletividade é pelo manejo da ação civil pública por danos morais coletivos, destinando-se o valor da condenação ao fundo de defesa dos direitos do consumidor (Lei nº 9.008/95). Essa possibilidade é expressamente admitida na própria LGPD (art. 42, § 3º).[11]

Como se vê, a reparação pela via judicial é um caminho possível, individual ou coletivamente, porém é necessária a indicação da fonte primária desses vazamentos (qual foi a empresa *hackeada*), assim como do responsável pela conduta negligente na guarda dessas informações.

Se do ponto de vista judicial é necessária a identificação de responsáveis, o Poder Público não pode se eximir de implementar algumas medidas corretivas e de ajuda a seus cidadãos. Algumas destas questões passamos a incluir na próxima seção.

REFLEXÕES FINAIS E AÇÕES PROTETIVAS NECESSÁRIAS

Como visto, as providências a serem tomadas visando a coibir o uso indevido de dados originados dos *megavazamentos* são diversas, algumas destas inconclusivas. Tendo em vista que, como já foi dito, não existe a possibilidade de "desvazar" os dados, isto é de se restaurar a proteção original à privacidade, o cidadão terá que conviver com a possibilidade de mais cedo ou mais tarde tornar-se vítima de algum golpe mediante o uso de suas informações pessoais.

Há procedimentos administrativos que podem ser realizados junto a cada controlador de dados. Entretanto, é certo que esses procedimentos não irão exaurir as possibilidades de checagem e de bloqueio. A ferramenta "Registrato", do Banco Central, pode ser vista como a melhor resposta do Poder Público no sentido de centralizar as informações de uma determinada atividade, no caso o sistema financeiro. A via judicial também é possível. Entretanto, no caso dos dados pessoais que trafegam em formato digital, a identificação dos responsáveis é atividade extremamente complexa.

Diante desse cenário, é oportuno que o Poder Público facilite a solução do problema, conjugando solução que contemple: (i) transparência e fácil acesso do cidadão às

[11] "Art. 42. [...] § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente".

informações sobre o uso de seus dados para os mais variados produtos e serviços; e (ii) possibilidade de correção imediata da situação de uso indevido de dados do titular.

Com esse espírito de promoção da transparência e de oferecer canais ágeis para a reparação, apontamos algumas soluções que poderiam ser implementadas pelas autoridades e promovidas por associações representativas dos cidadãos e consumidores:

(i) Determinar que todos os provedores de aplicações de internet sejam obrigados a disponibilizar a seus usuários a quantidade de contas existentes e utilizadas em seu nome, bem como a relação de quais atividades foram realizadas com uma conta cadastrada com determinado número de telefone ou nome. Além disso, é necessário que provedores de aplicações de internet corrijam eventual erro ou uso impróprio da conta, com base no princípio da qualidade dos dados, previsto na LGPD. O objetivo aqui é facilitar o acesso do cidadão, individual e separadamente, a cada provedor de aplicação na internet, alvo mais constante dos ataques de *hackers* e de vazamentos de dados pessoais;

(ii) Determinar que, além da possibilidade de consulta individual a cada provedor de aplicação na internet, haja também um canal integrado com informações de todos os provedores de aplicações que possuam mais de 50 mil usuários no Brasil, mostrando ao usuário, sob consulta específica, se, quando, por quem, em qual plataforma e em que extensão seus dados foram vazados ou utilizados de forma irregular;

(iii) Determinar que empresas com delegação de serviço público (concessionárias, permissionárias ou autorizatárias), como serviços públicos de luz, água e esgoto, telefonia, entre outros, mantenham cadastro com acesso fácil e seguro para consulta do consumidor acerca de todos os produtos e serviços que estão contratados, cadastrados e cobrados em seu nome. Além disso, é oportuno criar mecanismos regulatórios que permitam estabelecer a obrigação para que as empresas delegatárias corrijam eventual erro ou uso impróprio da conta, com base no princípio da qualidade dos dados. A possibilidade do conhecimento mais imediato do mau uso de seus dados é indispensável para a solução mais célere do problema;

(iv) Consultar as autoridades de supervisão e normatização do Sistema Financeiro Nacional (SFN) quanto à possibilidade de aperfeiçoamento do mecanismo

"Registrato" e viabilidade de integração desse modelo com as demais ferramentas de comunicação entre os órgãos e entidades do SFN com vistas a permitir, em canal centralizado, acesso imediato dos clientes a irregularidades, suspensão e correção de operações suspeitas;

(v) Determinar que todos os Controladores de dados pessoais divulguem em veículos de comunicação social e em mídias sociais a ocorrência de eventuais vazamentos e tomem medidas imediatas para mitigar o incidente de segurança. A LGPD já traz previsão semelhante no seu art. 48, determinando que "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares". No entanto, vê-se que a obrigação somente se aplica a casos de risco ou danos relevantes, sendo que tal interpretação caberá ao controlador.

(vi) Criar iniciativas, incluindo campanhas de divulgação massivas, para consulta gratuita da existência de crediários abertos, na medida e nas condições de segurança e de sigilo, com as principais empresas de comércio eletrônico, à semelhança do portal "Cadastropré", mantido pelas operadoras de telefonia, e outras de escore de crédito.

As medidas acima representam um primeiro, mas importante passo para a transparência e possibilidade de reparação do uso indevido de dados pessoais, especialmente por empresas de internet de grande porte e por delegatárias de serviços públicos essenciais, aumentando a publicidade e clareza de incidentes de segurança.

A nosso ver, cabe à ANPD a condução e a coordenação desse processo de implementação de medidas de proteção, visto trazerem aplicações práticas de princípios já constantes da LGPD, como os princípios da transparência, do livre acesso, da qualidade dos dados pessoais e da responsabilização e prestação de contas por parte dos agentes de tratamento, sejam eles públicos ou privados.

2021-3268