# Opinião: Megavazamentos de dados pessoais: o que fazer?


Recentemente, fomos surpreendidos com as notícias de megavazamentos de dados pessoais em nosso O primeiro, divulgado em janeiro deste ano, envolve a exposição de informações pessoais de mais de 200 milhões de brasileiros. Foram divulgados dados tais como CPF, informações sobre veículos, números de celulares, informações sobre razão social de empresas etc. O segundo, noticiado em fevereiro, afetou cerca de cem milhões de brasileiros com a divulgação de conteúdo relacionado a dados de celulares: número, CPF, tipo de conta, minutos gastos em ligações telefônicas, entre outros dados. Em ambos os vazamentos, entre as vítimas, há também pessoas famosas, tais como os jornalistas William Bonner e Fátima Bernardes e o presidente Jair Bolsonaro. O terceiro, ainda nas primeiras semanas de fevereiro, apontou um banco de dados contendo informações de oito milhões de pessoas foi posto à venda em um fórum por US$ 320.

Devido ao grande volume de informações pessoais divulgadas em ambos os vazamentos, e face ao grande número de indivíduos atingidos, já imaginamos que diante disso, teremos um aumento considerável dos índices de fraudes eletrônicas e todo o tipo de golpe.

Portanto, estejam atentos! Todo o cuidado é pouco! Principalmente após grandes incidentes como estes.

Tendo em vista que tais incidentes nos mostram o quão somos vulneráveis na era digital, é comum ter inúmeras dúvidas sobre o assunto. Por isso procuramos responder aos questionamentos mais recorrentes.

**Por qual motivo os dados têm valor?**
Dia a dia deparamos com novas reconfigurações sociais e culturais que estão diretamente relacionadas com o avanço das tecnologias inseridas em nossa sociedade. Não por menos, na medida em que as pessoas desenvolvem novos hábitos dentro de suas atribuladas rotinas ainda buscam pelo elixir do tempo (de vida, lazer e trabalho). O advento da internet aliado ao crescimento progressivo de usuários serviu para que novas tecnologias viessem suprir algumas necessidades.

E nessas tecnologias a criação de cadastros com inserção de dados pessoais era e ainda é a principal regra para acesso a uma gama de dispositivos e funcionalidades para navegar no mundo digital.

Uma vez os dados de interesse estando acessíveis, o problema central que se impõe é como lidar com a complexidade, diversidade e o gigantesco volume de circulação das informações ali contidas e contingenciar ameaças de todo tipo, seja coibir práticas delituosas (fraudes) ou por meio da mineração de dados, prospecção de dados, ou *data mining* como é mais conhecida, que propicia um verdadeiro fenômeno na coleta de dados para empresas capazes de melhorar suas vendas e lucratividade a partir do comportamento online ou perfil, para fazer previsões de compra dos clientes em potencial, e, por fim, atingirem seu público-alvo em tempo real.

Há de se repetir as lições de Leandro Augusto da Silva [1], para quem *"[o] dado é um fato, um valor documentado ou um resultado de medição. Quando um sentido semântico ou um significado é atribuído aos dados, gera-se informação (…) [q]uando estes significados se tornam familiares, ou seja, quando um agente os aprende, este se torna consciente e capaz de tomar decisões a partir deles, e surge o conhecimento"*.

Podemos dizer que a mineração de dados representa um processo de explorar em alta performance grandes quantidades de dados pessoais à procura de padrões consistentes.

Para viabilizar a compreensão do grau de importância do uso inapropriado e/ou sistemático dessas bases de dados é imprescindível que se comece pela definição em torno da preocupação levantada constantemente sobre o direito à privacidade e ao espaço íntimo — poder correspondente ao dever de não se imiscuir na intimidade alheia.

Erros precisam ser detalhados para que se encontre sua fonte permitindo as correções necessárias e resposta à gravidade dos danos sofridos.

**Como ocorrem os vazamentos de dados?**
Há inúmeras formas de vazamentos de dados, mas geralmente as mais comuns são:

— *Invasão:* o site, servidor ou sistema de uma instituição é atacado por um *cracker*, que quebra mecanismos de segurança e acessa conteúdos restritos e eventualmente, poderá divulgar esse material, vender ou utilizar para futuros crimes. Essa prática poderá caracterizar o crime de invasão de dispositivo informático alheio, definida no artigo 154-A do Código Penal [2].

— *Falhas de segurança ou vulnerabilidades:* o site, servidor ou sistema da instituição possui alguma falha de segurança/ vulnerabilidade, que passa a ser explorada pelo *cracker*. Ele não precisa quebrar mecanismos de segurança para acessar o conteúdo, mas simplesmente descobre alguma vulnerabilidade, que o leva a acessar conteúdos sigilosos.

— *Colaboradores:* o elo mais fraco da segurança são as pessoas. Nesse ponto, os próprios colaboradores da instituição, podem, de má-fé, por já terem acesso aos conteúdos restritos, repassar informação confidencial a terceiros ou mesmo vende-las. Essa atitude pode caracterizar o crime de violação de segredo profissional, descrito no artigo 154 do Código Penal [3].

— *Extorsão:* após acessar indevidamente o sistema e obter as informações privilegiadas, o indivíduo exige um pagamento em troca da não divulgação do conteúdo ou da liberação do acesso aos dados criptografados *(ramsonware).* Além da eventual invasão (artigo 154-A do Código Penal), o criminoso poderá incidir também no crime de extorsão, previsto no artigo 158 do Código Penal [4].

**Como terceiros têm acessos aos nossos dados?**
Há diversas maneiras de empresas, órgãos públicos e pessoas terem acesso às nossas informações pessoais, seja por um cadastramento voluntário do titular do dado ou de forma involuntária. Algumas formas de fornecimento e obtenção de dados pessoais:

— *Cadastramento voluntário:* o próprio titular dos dados fornece as informações solicitadas.

— *Mineração de dados:* é a exploração de massas de dados com padrões consistentes, gerando informações valiosas para quem os trata.

— *Engenharia social:* é a análise minuciosa das redes sociais e informações disponíveis na internet sobre determinado indivíduo, sendo possível montar um perfil quase que completo do sujeito, com base no conteúdo que ele mesmo publica e também nos materiais encontrados.

**É possível se proteger de um vazamento de dados? Como prevenir ou minimizar os riscos?**
Uma vez que os dados já foram divulgados, não há muito o que possa ser feito para reverter a situação. Em alguns casos, onde é possível encontrar informação específica na internet publicada por determinados sites, uma alternativa eventualmente possível será o contato com cada site solicitando a retirada do conteúdo, mas na maioria dos casos, o vazamento de dados é irreversível.

Pensando nisso, é importante que tenhamos algumas medidas em mente, para incrementarmos a segurança de informações pessoais:

— *Usar redes seguras:* evitar ao máximo o uso de redes wi-fi públicas ou abertas, pois você não sabe qual é o seu nível de segurança. Caso esteja fora de casa ou do ambiente de trabalho, utilize seu 3G, 4G do celular, principalmente para acessar redes sociais, contas pessoais e internet *banking*.

— *Usar nuvens seguras:* atenção ao uso de serviços de *cloud computing* gratuitos, pois geralmente o nível de segurança das redes é baixo. Procure sempre utilizar nuvens que possuem criptografia e prefira por serviços pagos.

— *Separar conteúdo pessoal e profissional em dispositivos diferentes:* utilizar *smartphones* diferentes para uso profissional e pessoal. Mantendo todos os seus contatos e conteúdos profissionais em um único aparelho, e fazendo o mesmo do ponto de vista pessoal, automaticamente você diminui o risco de vazamento de informações indevidas, caso um desses aparelhos seja alvo de um incidente. Ao proibir o compartilhamento de seu computador em home office, você evita que outras pessoas da família instalem programas frutos de pirataria e outros materiais indevidos, que podem deixá-lo mais vulnerável ou colocar em risco seu conteúdo profissional ou mesmo a empresa para a qual você trabalha.

— *Utilize senhas fortes:* com uso de números, letras e caracteres especiais; e troque-as periodicamente. Não utilize a mesma senha para todos os serviços.

— *Seja o mais restrito possível em suas redes sociais:* mantenha suas redes sociais pessoais fechadas, com seus conteúdos pessoais restritos aos seus contatos, evitando, assim, postagens públicas de cunho pessoal. Evite a publicação de fotos de seus filhos menores de idade publicamente, bem como utilizar a geolocalização em fotos em tempo real.

— *Assine termos de confidencialidade:* com seus colaboradores, prestadores de serviços, parceiros e terceirizados: a assinatura de um termo de confidencialidade (*N.D.A. — Non Disclosure Agreement* ) ou a inserção de uma cláusula de confidencialidade em contratos pode evitar a divulgação de informação sigilosa, mantendo-se, assim, a privacidade das partes e aumentando o nível de segurança da informação.

— *Estabeleça normas e políticas de segurança da informação em seu ambiente de trabalho:* a adoção de documentos específicos relacionados à segurança da informação pode fornecer toda a orientação necessária aos colaboradores quanto à forma de tratamento das informações que trafegam pela empresa, bem como conscientizá-los sobre a privacidade das pessoas envolvidas e aumentar o nível de cultura de proteção de dados.

— *Questione sempre:* "Qual é a finalidade desta informação que estou fornecendo? Para quê servirá esse dado? Será que é informação demais?". Esse raciocínio fará refletir imediatamente se eventualmente o nível de informações solicitadas está sendo excessivo. Havendo qualquer dúvida, você poderá entrar em contato com o encarregado do tratamento de dados pessoais (D.P.O. — Data Privacy Officer) da instituição e esclarecer suas dúvidas.

**O que fazer se for vítima de um vazamento de dados?**
Se você teve dados vazados, certifique-se de que você tem como provar esse vazamento, bem como a origem do incidente. Se você conseguir descobrir de onde surgiu este vazamento e possui provas concretas disso (ex.: determinado dado somente a empresa X detinha), armazene todas essas provas. Com esse material em mãos, procure um advogado especialista na área que analisará a viabilidade de ajuizar uma ação contra a empresa responsável pelo vazamento, cobrando indenização por danos morais devido à indevida exposição.

Você também poderá denunciar a ANPD (Autoridade Nacional de Proteção de Dados), Ministério Público ou Procon de sua cidade.

Se não souber de onde surgiu o vazamento e não tem provas disso, não há como responsabilizar alguém judicialmente.

Se após o vazamento, passou a ser vítima de fraudes eletrônicas praticadas por conta do uso indevido desses dados: registre um boletim de ocorrência através da delegacia eletrônica de seu Estado ou diretamente na delegacia de polícia mais próxima de seu endereço e procure a orientação de um advogado especialista na área. Esse profissional orientará qual melhor medida a ser adotada, a exemplo da ação judicial (cível ou criminal) para descobrir o autor do delito, caso não seja facilmente identificável, entre outras ferramentas. Com as características e especificidades do criminoso identificado, você poderá buscar reparação pelos danos morais sofridos com os transtornos ocasionados pelo fato, bem como a condenação criminal pelo ilícito praticado.

**Como saber se utilizaram seus dados para abrir conta ou pedir empréstimo?**
Outra forma de saber se utilizaram os seus dados pessoais para abertura de contas correntes ou realização de empréstimos, é através do site Registrato, ferramenta do Banco Central do Brasil. É possível localizar se o seu CPF foi utilizado nas principais instituições bancárias do país.

**Quais são os cuidados a partir de agora?**
Ninguém sabe ao certo o que vai acontecer daqui em diante, visto que o evento é recente e os órgãos fiscalizadores ainda estão investigando os responsáveis pelo megavazamento. Por ora, o que nos resta a fazer é tomar os principais cuidados: acompanhar extratos bancários e de cartão de crédito e suspeitar se acontecer alguma consulta atípica utilizando o número de seu CPF.

Após esse incidente que expôs praticamente dados pessoais de todos os brasileiros, inclusive de pessoas já falecidas, muito se questionou a respeito da efetividade da Lei Geral de Proteção de Dados Pessoais (LGPD) (em vigência desde setembro/2020) e sobre a atuação da Autoridade Nacional de Proteção de Dados (ANPD).

A ANPD, vinculada à Presidência da República, é um órgão que tem por objetivo editar normas e fiscalizar procedimentos sobre proteção de dados pessoais. Apesar do órgão ter emitido uma nota oficial dias após o incidente, informando que as devidas providências seriam tomadas, a ANPD ainda não está totalmente consolidada, trazendo muita insegurança jurídica.

Antes mesmo de a LGPD entrar em vigor, especialistas da área já alertavam que o sucesso da lei dependeria diretamente da ANPD e, diante desse cenário, se percebe que o dispositivo legislativo está passando por grandes provações, evidenciando que o mais importante momentaneamente é estabelecer novos padrões de segurança e descentralizar os bancos de dados para que os cidadãos fiquem menos vulneráveis.

Evidente que é um trabalho coletivo, visto que empresas detentoras de dados também necessitam se adequar a LGPD, uma vez que cabem a elas a aplicação correta dos parâmetros estabelecidos para uma efetiva proteção das informações pessoais dos titulares de dados. Os riscos de vazamento não deixarão de existir, mas poderão contribuir na redução dos incidentes.

Outros órgãos fiscalizadores, tais como Procon e Ministério Público, estão desenvolvendo um papel muito importante enquanto a ANPD não está completamente solidificada. É essencial que a promoção à conscientização das instituições, empresas e pessoas físicas sejam concretizadas, principalmente no período inicial de vigência da LGPD e diante de tantos vazamentos que ocorreram em menos de um mês.

[1] SILVA, Leandro Augusto; PERES, Sarajane Marques; BOSCARIOLI. Introdução à mineração de dados. Rio de Janeiro: Elsevier, p. 384-6, 2016.

[2] "*Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência*
*Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.*
*§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.*
*§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.*
*§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:*
*Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.*
*§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos".*

[3] "*Art. 154 – Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:*
*Pena – detenção, de três meses a um ano, ou multa de um conto a dez contos de réis".*

[4] "*Art. 158 – Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:*
*Pena – reclusão, de quatro a dez anos, e multa.*
*§ 1º – Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade.*
*§ 2º – Aplica-se à extorsão praticada mediante violência o disposto no § 3º do artigo anterior".*

**Date Created**
02/03/2021