ADMINISTRAÇÃO PÚBLICA E INTERVENÇÃO EXTRAJUDICIAL NA VIOLAÇÃO DE DADOS PESSOAIS DECORRENTE DE FALHAS DE SEGURANÇA DIGITAL (*DATA BREACH*)

Natália Garcia de Freitas Leite[1]

RESUMO: Reproduzindo tendências mundiais, no Brasil deve-se proteger o dado pessoal, considerado pela normativa geral como a informação relacionada à pessoa natural identificada ou identificável, em respeito aos direitos fundamentais de liberdade e de privacidade e ao livre desenvolvimento da personalidade. Todavia, uma vez inseridos em determinados sistemas, os dados pessoais não raro são devassados e expostos a terceiros não autorizados. Para prevenir e reprimir a violação de dados pessoais, autoridades competentes podem adotar medidas administrativas (extrajudiciais) em face dos controladores, mesmo quando a exposição é resultante de falhas de segurança digital (*data breach*). A presente pesquisa objetiva explorar as medidas administrativas que foram empregadas nos casos mais simbólicos de vazamento de dados pessoais decorrentes de falhas de segurança digital no Brasil, em especial os que envolvem as empresas Uber, Netshoes, Banco Inter, Facebook e Vivo, para, partindo de casos concretos, identificar possibilidades de responsabilização para os abusos cometidos no tratamento dos dados pessoais na era pré-LGPD. Além disso, busca traçar um paralelo para o fundamento utilizado na aplicação dessas medidas administrativas e a regulação trazida pela LGPD, que, uma vez em vigor, passa a normatizar as infrações nesta matéria. Os resultados trazem desdobramentos práticos para subsidiar a proteção de interesses coletivos *lato sensu*, como a defesa do consumidor e de garantias fundamentais da pessoa humana. Tem-se que o Ministério Público do Distrito Federal e Territórios (MPDFT) vem se destacando por sua atuação pioneira para coibir e responsabilizar os controladores por violações aos dados pessoais no país. Com a LGPD, aplicar sanções administrativas aos agentes de tratamentos de dados será tarefa da chamada Autoridade Nacional de Proteção de Dados (ANPD). A efetividade da proteção dos dados pessoais passa pelo reconhecimento por parte dos controladores quanto à necessidade de estimular boas práticas e governança de tecnologia da informação, sendo a LGPD uma importante propulsora para esse ajuste de conduta e para o desenvolvimento do tema.

---

[1] Pós-graduanda em nível de especialização em Direito Penal e Processo Penal pela Universidade Potiguar (UNP). Bacharela em Direito pela Universidade Federal do Rio Grande do Norte (UFRN). Técnica em Informática pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN). Residente Jurídica no programa do Ministério Público do Estado do Rio Grande do Norte (MPRN). E-mail: nataliagfleite@gmail.com.

Palavras-chave: Violação de dados. Dados pessoais. Privacidade. Regulação. LGPD.

INTRODUÇÃO

No Brasil, a proteção de dados pessoais é consequência da previsão constitucional de garantia de inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de violação (art. 5º, X), do sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII), e, ainda, do *habeas data* (art. 5º, LXXII).

Nessa esteira, ementada como Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei n. 13.709/2018 dispõe sobre o tratamento protetivo de dados pessoais por pessoa natural ou jurídica de direito público ou privado. Trata-se da primeira normativa geral sobre a matéria, apesar de existirem outras normas que podem ser utilizadas para se buscar salvaguardar a privacidade e a proteção de dados, a exemplo do Código de Defesa do Consumidor (Lei n. 8.078/1990), da Lei do Cadastro Positivo (Lei. 12.414/2011), da Lei de Acesso à Informação (Lei n. 12.527/2012), do Marco Civil da Internet (Lei n. 12.965/2014) e de seu decreto regulamentador (Decreto n. 8.771/2016).

Para os efeitos da LGPD, dado pessoal é considerado como a informação relacionada à pessoa natural identificada ou identificável, titular do dado. É assim considerada qualquer informação que possa ser usada para distinguir ou rastrear a identidade de uma pessoa, como nome, data e local de nascimento, número de identificação, dados de localização, e-mail etc.

Já controlador é considerado como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Neste trabalho, os controladores objeto de estudo são as empresas Uber, Netshoes, Banco Inter, Facebook e Vivo.

Com o aumento da complexidade social trazida pelo surgimento da Internet e do ciberespaço verifica-se também a dificuldade de o Direito acompanhar a evolução social no campo das tecnologias da informação (BARRETO, 2009).

Cada vez mais as pessoas confiam nas transações online e se vinculam a contratos eletrônicos diversos para fazer compras ou uso de sistemas de interesse em sites e aplicativos.

Os dados coletados por muitas empresas fora do comércio eletrônico também são frequentemente guardados em servidores online (*cloud computing*).

Falhas de segurança nesses sistemas, que permitam pessoas não autorizadas a acessar dados pessoais protegidos, resultam em violação de dados pessoais (ou *data breach*).

As ocorrências de vazamentos de dados pessoais têm sido noticiadas com frequência na atualidade, e causam transtorno e preocupação aos titulares das informações, que podem ser vítimas de golpes diversos aplicados por pessoas más intencionadas, como engenharia social, *phishing* e outras atividades perniciosas.

A autodeterminação informativa, expressão desenvolvida na jurisprudência alemã, refere-se ao "direito de um indivíduo de se proteger contra a coleta, o armazenamento, o uso e a revelação de seus dados pessoais, efetuados de modo ilimitado", o que só admite restrição em caso de um interesse público superior com fundamento constitucional (LEONARDI, 2011, p. 70).

O Estado, à medida que desperta para o reconhecimento do direito à autodeterminação informativa, correlato ao dever de se proteger efetivamente os dados pessoais, busca também instrumentos para prevenir e reprimir violações, como a responsabilização dos controladores.

A responsabilização dos controladores pode ocorrer mesmo quando o vazamento dos dados pessoais é decorrente de ciberataques oportunizados por falhas de segurança digital. Isso ocorre na Jurisdição e fora dela, nesse último caso através de mecanismos decorrentes do poder de polícia administrativa, conceituada por Hely Lopes Meirelles (2000, p. 122) como "a faculdade de que dispõe a Administração Pública para condicionar e restringir o uso e gozo de bens, atividades e direitos individuais, em benefício da coletividade e do próprio estado", ou através de competências extrajudiciais próprias como as do Ministério Público para o compromisso de ajustamento previsto na Lei da Ação Civil Pública (art. 5º, § 6º, da Lei n. 7.347/1985, com redação dada pela Lei n. 8.078/1990).

O Ministério Público do Distrito Federal e Territórios (MPDFT) tem se destacado através da sua atuação pioneira no combate aos muitos abusos cometidos no dever de proteção dos dados pessoais no Brasil.

A presente pesquisa objetiva explorar as medidas administrativas (extrajudiciais) que foram empregadas nos casos mais simbólicos de vazamento de dados pessoais decorrentes de falhas de segurança digital no Brasil, em especial os que envolvem as empresas Uber, Netshoes, Banco Inter, Facebook e Vivo, para, partindo de casos concretos, identificar possibilidades de responsabilização para os abusos cometidos no tratamento dos dados pessoais na era pré-LGPD.

Além disso, busca traçar um paralelo para o fundamento utilizado na aplicação dessas medidas administrativas e a regulação trazida pela LGPD, que, uma vez em vigor, passa a normatizar as infrações nesta matéria.

DATA BREACH NO BRASIL E MEDIDAS ADMINISTRATIVAS EMPREGADAS NA ERA PRÉ-LGPD

Hackers atuam para descobrir vulnerabilidades nos sistemas. Os chamados *hackers* éticos trabalham para auxiliar a fortalecer o tratamento e a criptografia dados, fazendo comunicação aos controladores quando verificam que os sistemas não estão tolerantes a falhas. Os *hackers* não éticos ou *crackers*, por sua vez, agem de forma mal-intencionada (MARTINS, 2018).

Entre os anos de 2017 e 2019 irromperam notícias acerca de vazamentos de dados pessoais decorrentes de falhas de segurança digital no Brasil e no mundo. No Brasil, dentre os casos mais simbólicos estão os que envolveram as empresas Uber, Netshoes, Banco Inter, Facebook e Vivo, objeto de análise deste trabalho sob o enfoque das medidas administrativas (extrajudiciais) adotadas caso a caso.

1 Caso Uber

Em novembro de 2017 tornou-se público um ciberataque mundial sofrido pela empresa Uber ao final de 2016, que tinha sido abafado. Estima-se que o vazamento de dados atingiu cerca de 196.000 (cento e noventa e seis mil) usuários brasileiros, que tiveram expostos nome, telefone e e-mail (CIRIACO, 2018).

Aos 23 de janeiro de 2018, através da Comissão de Proteção dos Dados Pessoais (CPDP), o Ministério Público do Distrito Federal e Territórios (MPDFT) requisitou, por ofício endereçado à Uber, informações sobre a constatação de incidente de segurança relacionado à sua base de dados, detalhes sobre sua natureza e as medidas que foram tomadas, além de quantos motoristas e clientes brasileiros foram afetados. Frisou-se no documento que o MPDFT visava requerer o compartilhamento de provas com as autoridades de dados que investigam o incidente em outros países, como as do Reino Unido (*Information Commissioner's Office - ICO*) e da Holanda (*Dutch Data Protection Authority*) (MPDFT cobra..., 2018).

A Uber notificou os usuários brasileiros acerca do incidente durante o mês de abril de 2018, após acordo firmado no bojo do procedimento instaurado pelo MPDFT para averiguar o caso. A comunicação foi feita por mensagem enviada aos e-mails cadastrados na plataforma da empresa. Com a averiguação não se chegou a comprovar que os dados circularam pela internet, o que causaria mais dano, ficando somente em poder dos *hackers*. O acordo foi

considerado um importante avanço, atinente com o Código de Defesa do Consumidor (art. 10, § 1º, da Lei n. 8.078/1990). A empresa também disponibilizou uma página virtual sobre o incidente (UBER..., 2018).

2 Caso Netshoes

Em dezembro de 2017 veio à tona um incidente de segurança envolvendo a base de dados de clientes da empresa Netshoes, no qual foram comprometidos dados pessoais como nome, cadastro de pessoa física, e-mail, data de nascimento e informações de pedidos, incluindo dados pessoais sensíveis, de 1.999.704 (um milhão, novecentos e noventa e nove mil e setecentos e quatro) contas (MAIA, 2018; BORINI, 2018).

Através da Comissão de Proteção dos Dados Pessoais (CPDP), da 2ª Promotoria de Justiça Criminal e da 1ª Promotoria de Justiça de Defesa do Consumidor, o Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou o Inquérito Civil Público (ICP) n. 08190.04481318-44 (um procedimento administrativo inquisitivo no âmbito do Ministério Público) para apurar o caso. No inquérito considerou-se que as medidas adotadas pela empresa, em um primeiro momento, eram insuficientes, já que tinha ocorrido somente o "envio de e-mail genérico para a base de consumidores" (BRASIL, 2018b, p. 06).

Nesse cotejo, aos 25 de janeiro de 2018 foi expedida a Recomendação n. 01/2018, assinada pelo Promotor de Justiça Frederico Meinberg Ceroy, coordenador da CPDP, orientando a empresa a: i) informar aos clientes afetados pelo incidente de segurança, através de correspondência com aviso de recebimento ou por meio de ligação telefônica, os dados pessoais que foram comprometidos, sob pena de ajuizamento de Ação Civil Pública por danos morais e materiais causados aos consumidores; ii) abster-se de efetuar qualquer tipo de pagamento ao suposto autor do incidente de segurança (*hacker*), na forma de moeda física ou de criptomoeda, sob pena de configuração do crime de fraude processual; iii) informar, no prazo de 03 (três) dias úteis, a contar do recebimento da recomendação, seu acatamento ou não, elencando de maneira clara, objetiva e precisa quais as medidas implementadas, e expondo as razões de eventual recusa, sendo a ausência de manifestação interpretada como recusa de acatamento (BRASIL, 2018b, p. 07-08).

Além da Recomendação, aos 16 de janeiro de 2019, no bojo do ICP n. 08190.04481318-44 foi pactuado Termo de Ajustamento de Conduta (TAC) entre a empresa Netshoes, representada pelo CEO Marcio Kumruian, e o MPDFT, através do Promotor de

Justiça Frederico Meinberg Ceroy, coordenador da Unidade Especial de Proteção de Dados e Inteligência Artificial (ESPEC).

Esse compromisso de ajustamento, previsto na Lei da Ação Civil Pública (art. 5º, § 6º, da Lei n. 7.347/1985, com redação dada pela Lei n. 8.078/1990), pode ser considerado uma forma de transação ou ato administrativo negocial em relação ao modo e ao tempo da reparação do dano coletivo (CABRAL, 2015, p. 193-210), vez que a defesa dos interesses sociais e individuais indisponíveis está na esfera de incumbência do Ministério Público.

O TAC n. 01/2019 (BRASIL, 2019) foi fundamentado na Constituição Federal de 1988, no Código de Defesa do Consumidor (Lei n. 8.078/1990), no Marco Civil da Internet (Lei n. 12.965/2014) e no seu decreto regulamentador (Decreto n. 8.771/2016), além de na novíssima Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei n. 13.709/2018), mesmo em vacância, a título de orientação.

Quanto à Constituição Federal, o compromisso de ajustamento afirmou ser inviolável a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de violação (art. 5º, X, da Constituição Federal).

No tocante ao Marco Civil da Internet, tratou-se da garantia aos titulares dos dados pessoais quanto aos direitos de inviolabilidade da intimidade e da vida privada, bem como o direito de não fornecimento a terceiros dos dados pessoais, salvo mediante consentimento livre, expresso e informado (art. 7º, I e VII, da Lei n. 12.965/2014).

Na linha do decreto regulamentador do Marco Civil da Internet, falou-se da definição de dado pessoal como "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (art. 14, I, do Decreto n. 8.771/2016) e do tratamento dos dados pessoais como sendo:

> "[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração." (Art. 14, II, do Decreto n. 8.771/2016).

O TAC destacou, a título de orientação, que a LGPD determina aos agentes de tratamento a adoção de medidas de segurança, técnicas e administrativas capazes de proteger "os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (art. 46, *caput*, da Lei n. 13.709/2018). Além disso, tratou do dever do controlador de

comunicar ao titular do dado atingido a ocorrência de incidente de segurança que possa lhe acarretar risco ou dano relevante, em prazo razoável (art. 48, § 1º, da Lei n. 13.709/2018), e da necessidade de sopesar, para aplicação de sanções pela autoridade nacional, os seguintes critérios (art. 52, § 1º, da Lei n. 13.709/2018):

> "[...] a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infrator; a condição econômica do infrator; a reincidência; o grau do dano; a cooperação do infrator; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; a adoção de políticas de boas práticas de governança; a pronta adoção de medidas corretivas, além da proporcionalidade entre a gravidade da falta e a intensidade da sanção. [...]" (BRASIL, 2019, p. 03).

O TAC previu o pagamento por parte da empresa de R$ 500.000,00 (quinhentos mil reais) a título de indenização pelos danos morais coletivos de caráter nacional em razão do incidente, a ser revertido ao Fundo de Defesa dos Direitos Difusos (FDD) criado pela Lei n. 7.347/1985 (Lei da Ação Civil Pública) e regulamentado pela Lei n. 9.008/1995. Não obstante, a empresa também se comprometeu a: i) implantar medidas adicionais ao seu Programa de Proteção de Dados, com gerenciamento de riscos e vulnerabilidades no portal Netshoes, ações de adequação à LGPD e atualização contínua de sua Política de Segurança Cibernética; ii) realizar esforços de orientação de consumidores, a aumentar o nível de conhecimento sobre os riscos cibernéticos e medidas de proteção de seus dados pessoais, por meio de campanha de conscientização; e a iii) disseminar ao mercado as melhores práticas para privacidade e proteção de dados pessoais, por meio da participação em fóruns e eventos especializados, e difusão de boas práticas de proteção de dados. Para o descumprimento está prevista a judicialização do caso como penalidade. Com a homologação do TAC, o ICP n. 08190.04481318-44 será suspenso e posteriormente arquivado com o cumprimento dos termos acordados (BRASIL, 2019).

A resolução administrativa mediante TAC ganha relevo pela autocomposição, isto é, pelo acordo das partes, com ausência de uma decisão impositiva, como costuma ocorrer na Jurisdição. Foi anotada a boa vontade da empresa em colaborar com a investigação, que tão logo tomou ciência do acontecimento demonstrou monitoramento proativo e remoção de conteúdo na Internet, seguiu as recomendações do Órgão Ministerial e se engajou para cientificar os consumidores através de ampla divulgação em meios de comunicação, evitando o ajuizamento de ação civil coletiva de responsabilidade contra si, uma medida mais gravosa.

3 Caso Banco Inter

No início de maio de 2018 foi divulgado na imprensa que o Banco Inter, considerado o primeiro banco inteiramente digital no Brasil, sofreu uma tentativa de extorsão de *hackers* em razão do vazamento de dados pessoais de 19.961 (dezenove mil, novecentos e sessenta e um) correntistas, como nome, telefone, e-mail, senhas de cartões de débito e crédito e registros bancários. O banco enviou nota aos correntistas afirmando que a exposição dos dados foi de "baixo impacto", notificando também os clientes mais gravemente afetados. Além disso, de acordo com o banco, não houve ataque *hacker*, mas vazamento de informações por pessoa autorizada (HIGA, 2018; VENTURA, 2018; FERREIRA, 2018; BANCO Inter confirma..., 2018).

Aos 04 de maio de 2018, através da Comissão de Proteção dos Dados Pessoais (CPDP), o Ministério Público do Distrito Federal e Territórios (MPDFT) expediu o Ofício n. 07/2018-CPDP/MPDFT (BRASIL, 2018c) requisitando informações ao Banco Inter sobre a constatação de incidente de segurança relacionado à sua base de dados, detalhes sobre sua natureza e as medidas que foram tomadas, além de quantos clientes ou colaboradores foram afetados (MPDFT investiga suposto..., 2018).

Ademais, em 08 de maio de 2018 foi instaurado o Inquérito Civil Público (ICP) n. 08190.097749/18-95, através da Portaria n. 05/2018 (BRASIL, 2018d), objetivando investigar as circunstâncias do comprometimento dos dados pessoais dos clientes do Banco Inter, bem como apurar as responsabilidades pelos danos causados.

No decorrer investigativo, o Centro de Produção, Análise, Difusão e Segurança da Informação (CI) do Órgão Ministerial constatou o comprometimento dos dados de 19.961 (dezenove mil, novecentos e sessenta e um) correntistas e não-correntistas do Banco Inter, bem como a exposição de certificados digitais e da chave privada do banco, comprovando a veracidade, a fragilidade e a vulnerabilidade do sistema (ROHR, 2018).

Aos 30 de julho de 2018 foi ajuizada a Ação Civil Pública por danos morais coletivos n. 0721831-64.2018.8.07.0001, perante a 15ª Vara Cível de Brasília (MPDFT ajuíza..., 2018). Nos fatos, relatou-se que o Banco Inter se negou a responder questionamentos do MPDFT, que uma testemunha do caso se sentiu ameaçada por representantes da empresa e que os dados pessoais obtidos com o vazamento estavam sendo comercializados na chamada *Deep Weeb* ou Web Profunda. De acordo com o coordenador da CPDP, o Promotor de Justiça Frederico Meinberg Ceroy, que assina a petição inicial que judicializou o caso:

> "[...] as tentativas de encobrir o incidente de segurança, promovidas pelo Banco Inter, geraram prejuízos morais e insegurança aos clientes, não clientes, investidores, acionistas, ecossistemas de Fintechs e Startups brasileiros de dados, bem como na

> confiabilidade da migração dos serviços de processamento, armazenamento e de computação em nuvem das instituições financeiras." (MPDFT ajuíza..., 2018).

Embora o caso não tenha obtido uma resolução administrativa (extrajudicial), saliente-se que aos 18 de dezembro de 2018 foi alcançado um acordo no bojo da ação judicial vergastada, prevendo o pagamento pelo banco da importância de R$ 1.500.000,00 (um milhão e quinhentos mil reais), que, homologado pelo Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), arquivou os autos do processo. O montante tem destinação especificada à caridade e ao combate de crimes cibernéticos (BANCO Inter: acordo..., 2018). Ganha relevo a transação ocorrida, isto é, a autocomposição do conflito.

4 Caso Facebook

Em março de 2018 foi revelado um escândalo de vazamento de dados pessoais em razão de um aplicativo da rede social Facebook.

Descobriu-se que, em 2014, cerca de 270.000 (duzentos e setenta mil) usuários utilizaram o aplicativo do Facebook chamado "*This is your digital life*", da empresa Global Science Research (GSR), respondendo a um teste de personalidade e concordando com a coleta de seus dados para uso acadêmico. Entretanto, em seu funcionamento, o aplicativo coletou também dados dos amigos das pessoas que realizaram o teste, chegando a capturar informações de 50.000.000 (cinquenta milhões) de usuários ou mais. A empresa Cambridge Analytica então, sem autorização, teria comprado esses dados para, por meio da construção de perfis psicográficos, direcionar de forma personalizada propaganda política pró-Trump nos Estados Unidos (MARTÍ, 2018; MPDFT investiga uso..., 2018).

Aos 20 de março de 2018 o Ministério Público do Distrito Federal e Territórios (MPDFT), por sua Comissão de Proteção dos Dados Pessoais (CPDP) e a 1ª Promotoria de Justiça de Defesa do Consumidor, através da Portaria n. 02/2018 (BRASIL, 2018e), instaurou Inquérito Civil Público para apurar a ocorrência de violações dos dados dos usuários do Facebook no Brasil. O procedimento tem caráter preventivo e repressivo. As investigações estão sendo conduzidas sob sigilo. Na Portaria afirma-se que:

> "[...] existem suspeitas de que a **Cambridge Analytica** pode estar fazendo uso, de forma ilegal, dos dados pessoais de milhões de brasileiros, usuários do **Facebook** ou não, para fins da construção de perfis psicográficos em escala nacional e regional (*Psychographic Profiles*); [...] os perfis psicográficos podem ser usados para predizer crenças políticas, crenças religiosas, orientação sexual, cor da pele e comportamento político; [...] a **Cambridge Analytica** deixa claro que o foco de atuação da empresa é a alteração do comportamento das pessoas por meio do uso

> dos dados (*Data-Driven Behavior Change*); [...]" (grifo do autor) (MPDFT investiga uso..., 2018).

Na sequência, após a confirmação da rede social Facebook de que os dados pessoais de 87.000.000 (oitenta e sete milhões) de usuários e de 443.000 (quatrocentos e quarenta e três mil) brasileiros foram captados pela Cambridge Analytica, aos 13 de abril de 2018 a Fundação Programa de Proteção e Defesa do Consumidor de São Paulo (Procon/SP) anunciou que notificou o Facebook no Brasil, questionando sobre como e quando o caso aconteceu, que tipo de dados foram expostos e quais providências já foram tomadas pela companhia. O órgão fundamentou sua atuação no Marco Civil da Internet (Lei n. 12.965/2014) e no Código de Defesa do Consumidor (Lei n. 8.078/1990) (PROCON-SP..., 2018).

Esse não é o único escândalo de vazamento de dados pessoais e violação da privacidade envolvendo o Facebook. A rede social vem se envolvendo em incidentes deste tipo desde 2016, e sofre várias investigações por parte de autoridades internacionais.

5 Caso Vivo (Telefônica Brasil)

Aos 04 de novembro de 2019 uma denúncia do grupo "WhiteHat Brasil" informou uma grave falha de segurança no portal de serviços "Meu Vivo", da Telefônica Brasil, que expôs dados cadastrados de pelo menos 24.000.000 (vinte e quatro milhões) de usuários. De acordo com a denúncia, informações como nome completo, endereço, data de nascimento, registro geral, cadastro de pessoa física, e-mail, nome da mãe e número de telefone ficaram desprotegidas. A empresa reconheceu o ocorrido por meio de uma nota, na qual informou que neutralizou a vulnerabilidade e que revisa constantemente suas políticas e procedimentos de segurança (SCHAEFFER, 2019; GOMES, 2019; SCHAEFFER; JUNQUEIRA, 2019; BEMBOM, 2019; ARRUDA, 2019).

Nesse ínterim, foi noticiado que a Fundação Programa de Proteção e Defesa do Consumidor de Santa Catarina (Procon/SC) e a Agência Nacional de Telecomunicações (Anatel) solicitaram esclarecimentos à Telefônica. O Procon/SC notificou a empresa para informar, no prazo de 10 (dez) dias, quando ocorreram os vazamentos, quais foram os dados expostos e quais providências já foram tomadas. Por sua vez, a Anatel teria dito que apuraria o fato. A fundação e agência, após definirem sua posição, podem aplicar sanções administrativas como multa, suspensão do serviço, cassação de licença etc. à empresa com base na defesa do consumidor (art. 56 da Lei n. 8.078/1990) (NAKAGAWA, 2019; BONATELLI, 2019; OPERADORA..., 2019).

CONSIDERAÇÕES FINAIS

Viu-se que o Ministério Público do Distrito Federal e Territórios (MPDFT) tem inovado na atuação voltada à proteção da privacidade e dos dados pessoais, atuando na tutela de interesses coletivos judicial e extrajudicialmente, com especial fundamento na defesa do consumidor e nas legislações que estão surgindo na temática de internet e dados. Contudo, a resolução de conflitos pelo Órgão Ministerial fora da Jurisdição depende de cooperação dos controladores dos dados, a fim de reparar ou mitigar os danos nesta matéria. Além da atuação ministerial há a possibilidade de responsabilização dos controladores por órgãos fiscalizadores e agências reguladoras com base na defesa do consumidor (art. 56 da Lei n. 8.078/1990), que não se mostrou muito efetiva nos casos estudados.

Com a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei n. 13.709/2018), aplicar sanções administrativas aos agentes de tratamentos de dados será também tarefa da chamada Autoridade Nacional de Proteção de Dados (ANPD), prevista no art. 5º, XIX, como o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional". Poderão ser aplicadas sanções de advertência, multas de até R$ 50.000.000,00 (cinquenta milhões de reais) por infração, publicização da infração, bloqueio e eliminação dos dados pessoais (art. 52 da LGPD).

As novas possibilidades de aplicação de sanções pela ANPD coexistirão com as previstas no diploma consumerista e em outras legislações específicas, por força do § 2º do art. 52 da LGPD. Isso representa um endurecimento na forma de lidar com as violações de dados pessoais, ainda mais se considerarmos que as sanções da ANPD independerão da Jurisdição para serem aplicadas e de cooperação dos controladores, por força do poder de polícia administrativa da ANPD.

A reorganização da segurança da informação no Brasil para adequação aos fins propostos pela LGPD se impõe, inclusive com a indicação nos quadros das organizações do Encarregado de Proteção de Dados (EPD) ou Diretor de Proteção de Dados (DPD), muito similar ao *Data Protection Officer* (DPO) previsto na *General Data Protection Regulation* (GDPR) europeia para instituições que processam grande quantidade de dados.

Independentemente das sanções que possam ser aplicadas, a efetiva proteção dos dados pessoais passa pelo reconhecimento por parte dos controladores quanto à necessidade de estimular boas práticas e governança de tecnologia da informação.

REFERÊNCIAS

ARRUDA, Wellington. Vazamento na Vivo afeta também quem não é cliente da operadora. **It Forum 365**. São Paulo, 12 nov. 2019. Disponível em: <https://www.itforum365.com.br/vazamento-na-vivo-afeta-tambem-quem-nao-e-cliente-da-operadora/>. Acesso em: 24 nov. 2019.

BANCO Inter confirma vazamento de dados e culpa "pessoa autorizada. **Tilt Uol**. 17 ago. 2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm>. Acesso em: 24 nov. 2019.

BANCO Inter: acordo destinará R$ 1,5 milhão para caridade e combate a crimes cibernéticos. **Ministério Público do Distrito Federal e Territórios**. Brasília, 19 dez. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31>. Acesso em: 24 nov. 2019.

BARRETO, Ricardo Menna. Contrato eletrônico como cibercomunicação jurídica. **Revista Direito GV**, São Paulo, v. 10, p. 443-458, jul./dez. 2009.

BEMBOM, Giovanna. Vivo admite vazamento de dados em app com milhões de clientes. **Metrópoles**. Brasília, 05 nov. 2019. Disponível em: <https://www.metropoles.com/brasil/ciencia-e-tecnologia-br/vivo-admite-dados-vazados-de-clientes-e-milhoes-estariam-expostos>. Acesso em: 24 nov. 2019

BONATELLI, Circe. Procon e Anatel analisam sanção contra Vivo por vazamento de dados. **Estadão**. São Paulo, 07 nov. 2019. Disponível em: <https://link.estadao.com.br/noticias/geral,procon-e-anatel-analisam-sancao-contra-vivo-por-vazamento-de-dados,70003080299>. Acesso em: 24 nov. 2019.

BORINI, Guilherme. MP cobra ações da Netshoes sobre vazamento de dados de usuários. **It Forum 365**. São Paulo, 26 jan. 2018. Disponível em: <https://www.itforum365.com.br/mp-cobra-acoes-da-netshoes-sobre-vazamento-de-dados-de-usuarios/>. Acesso em: 24 nov. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da República Federativa do Brasil, Brasília, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 28 nov. 2019.

BRASIL. **Decreto n. 8.771, de 11 de maio de 2016.** Diário Oficial da República Federativa do Brasil, Brasília, 11 maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 28 nov. 2019.

BRASIL. **Lei n. 12.414, de 09 de junho de 2011**. Diário Oficial da República Federativa do Brasil, Brasília, 09 jun. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 28 nov. 2019.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Diário Oficial da República Federativa do Brasil, Brasília, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 28 nov. 2019.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Diário Oficial da República Federativa do Brasil, Brasília, 23 abr. 2014. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 nov. 2019.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Diário Oficial da República Federativa do Brasil, Brasília, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 nov. 2019. (BRASIL, 2018a)

BRASIL. **Lei n. 7.347, de 24 de julho de 1985.** Diário Oficial da República Federativa do Brasil, Brasília, 24 jul. 1985. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7347orig.htm>. Acesso em: 28 nov. 2019.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Diário Oficial da República Federativa do Brasil, Brasília, 12 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 28 nov. 2019.

BRASIL. Ministério Público do Distrito Federal e Territórios. Comissão de Proteção dos Dados Pessoais, 2ª Promotoria de Justiça Criminal e 1ª Promotoria de Justiça de Defesa do Consumidor. **Recomendação n. 01/2018**. Distrito Federal: Ministério Público do Distrito Federal e Territórios, 25 jan. 2018. Disponível em: <http://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Recomendacao_Comissao_Protecao_Dados_2018_01.pdf>. Acesso em: 24 nov. 2019. (BRASIL, 2018b)

BRASIL. Ministério Público do Distrito Federal e Territórios. Comissão de Proteção dos Dados Pessoais. **Ofício n. 07/2018 – CPDP/MPDFT**. Distrito Federal: Ministério Público do Distrito Federal e Territórios, 08 maio 2018. Disponível em: <http://www.mpdft.mp.br/portal/pdf/noticias/maio_2018/Oficio_Banco_Inter_II_LockCERTO.pdf>. Acesso em: 24 nov. 2019. (BRASIL, 2018c)

BRASIL. Ministério Público do Distrito Federal e Territórios. Comissão de Proteção dos Dados Pessoais. **Portaria n. 05/2018**. Distrito Federal: Ministério Público do Distrito Federal e Territórios, 08 maio 2018. Disponível em: <http://www.mpdft.mp.br/portal/pdf/noticias/maio_2018/Instaura%C3%A7%C3%A3o_de_ICP_Banco_Inter_Sigilosas_Lock.pdf>. Acesso em: 24 nov. 2019. (BRASIL, 2018d)

BRASIL. Ministério Público do Distrito Federal e Territórios. Comissão de Proteção dos Dados Pessoais e 1ª Promotoria de Justiça de Defesa do Consumidor. **Portaria n. 02/2018**. Distrito Federal: Ministério Público do Distrito Federal e Territórios, 20 mar. 2018. Disponível em: <http://www.mpdft.mp.br/portal/pdf/noticias/Mar%C3%A7o_2018/Instauracao_de_ICP_Cambridge_Analytica.pdf >. Acesso em: 24 nov. 2019. (BRASIL, 2018e)

BRASIL. Ministério Público do Distrito Federal e Territórios. Unidade Especial de Proteção de Dados e Inteligência Artificial (ESPEC). **Termo de Ajustamento de Conduta (TAC) n. 01/2019 - ESPEC**. Distrito Federal: Ministério Público do Distrito Federal e Territórios, 16 jan. 2019. Disponível em: <http://www.mpdft.mp.br/portal/pdf/tacs/espec/TAC_Espec_2019_001.pdf>. Acesso em: 24 nov. 2019.

CABRAL, Antonio do Passo. As convenções processuais e o termo de ajustamento de conduta. *In*: DIDIER JR., Fredie (coord.) *et al*. **Ministério Público**: Coleção Repercussões do Novo CPC. Salvador: Juspodivm, 2015, v. 6, cap. 8, p. 193-210.

CIRIACO, Douglas. Vazamento de dados da Uber atingiu 196 mil brasileiros. **Tecmundo**. São Paulo, 12 abr. 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/129236-vazamento-dados-uber-atingiu-196-mil-brasileiros.htm>. Acesso em: 24 nov. 2019.

FERREIRA, Carlos Dias. Banco Inter atribui vazamento de dados a ação interna "de baixo impacto". **Canaltech**. 15 ago. 2018. Disponível em: <https://canaltech.com.br/hacker/banco-inter-atribui-vazamento-de-dados-a-ataque-interno-de-baixo-impacto-120346/>. Acesso em: 24 nov. 2019.

GOMES, Helton Simões. CPF e endereço: falha em site da Vivo expõe dados de 24 milhões de clientes. **UOL Tilt**. São Paulo, 05 nov. 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/11/05/cpf-e-endereco-falha-em-site-da-vivo-expoe-dados-de-24-milhoes-de-clientes.htm>. Acesso em: 24 nov. 2019.

HIGA, Paulo. Banco Inter vazou dados de quase 20 mil clientes, diz investigação do MP. **Tecnoblog**. 2018. Disponível em: <https://tecnoblog.net/253895/banco-inter-vazou-dados-correntistas-acao-mp/>. Acesso em: 24 nov. 2019.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011, p. 70.

MAIA, Flávia. Dados de 2 milhões de clientes da Netshoes vazam e MPDFT recomenda que empresa tome providências. **Correio Braziliense**. Brasília, 26 jan. 2018. Disponível em: <http://blogs.correiobraziliense.com.br/consumidor/dados-de-2-milhoes-de-clientes-da-netshoes-vazam-e-mpdft-recomenda-que-empresa-tome-providencias/>. Acesso em: 24 nov. 2019.

MARTÍ, Silas. Entenda o escândalo do uso de dados do Facebook. **Folha de São Paulo**. São Paulo, 22 mar. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-do-facebook.shtml>. Acesso em: 24 nov. 2019.

MARTINS, Ana Paula. Vazamento e mercantilização de dados pessoais e a fragilidade da segurança digital do consumidor: um estudo dos casos Netshoes e Uber. **XIV Congresso Brasileiro de Direito do Consumidor**. São Paulo, 2018. Disponível em: <https://www.researchgate.net/publication/327416131_VAZAMENTO_E_MERCANTILIZACAO_DE_DADOS_PESSOAIS_E_A_FRAGILIDADE_DA_SEGURANCA_DIGITAL_DO_CONSUMIDOR_um_estudo_dos_casos_Netshoes_e_Uber>. Acesso em: 24 nov. 2019.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 25. ed. São Paulo: Malheiros, 2000, p. 122.

MPDFT ajuíza ação contra o Banco Inter por vazamento de dados pessoais. **Ministério Público do Distrito Federal e Territórios**. Brasília, 31 jul. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10211-mpdft-ajuiza-acao-contra-o-banco-inter-por-vazamento-de-dados-pessoais>. Acesso em: 24 nov. 2019.

MPDFT cobra esclarecimentos da Uber sobre impacto de vazamentos de dados pessoais para usuários brasileiros. **Ministério Público do Distrito Federal e Territórios**. Brasília, 23 jan. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9781-mpdft-cobra-esclarecimentos-da-uber-sobre-impacto-de-vazamentos-de-dados-pessoais-para-usuarios-brasileiros>. Acesso em: 24 nov. 2019.

MPDFT investiga suposto vazamento de dados de clientes do Banco Inter. **Ministério Público do Distrito Federal e Territórios**. Brasília, 09 maio 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10035-mpdft-investiga-suposto-vazamento-de-dados-de-clientes-do-banco-inter>. Acesso em: 24 nov. 2019.

MPDFT investiga uso ilegal de dados pessoais de brasileiros disponíveis no Facebook. **Ministério Público do Distrito Federal e Territórios**. Brasília, 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9910-mpdft-vai-investigar-uso-ilegal-de-dados-de-brasileiros-disponiveis-no-facebook-por-empresa-americana>. Acesso em: 24 nov. 2019.

NAKAGAWA, Liliane. Vivo pode ser multada em R$ 10 milhões por vazamentos de dados. **Olhar Digital**. São Paulo, 07 nov. 2019. Disponível em: <https://olhardigital.com.br/noticia/vivo-pode-ser-multada-em-r-10-milhoes-por-vazamentos-de-dados/92714>. Acesso em: 24 nov. 2019.

OPERADORA de telefonia é notificada para explicar vazamento de dados de milhões de clientes. **Procon/SC**. 2019. Disponível em: <http://www.procon.sc.gov.br/index.php/outros-destaques/1038-operadora-de-telefonia-e-notificada-para-explicar-vazamento-de-dados-de-milhoes-de-clientes>. Acesso em: 24 nov. 2019.

PROCON-SP notifica Facebook por uso ilícito de dados de 443 mil brasileiros. **Época**. 13 abr. 2018. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2018/04/epoca-negocios-procon-sp-notifica-facebook-por-uso-ilicito-de-dados-de-443-mil-brasileiros.html>. Acesso em: 24 nov. 2019.

ROHR, Altieres. Certificado digital do Banco Inter é revogado após chave vazar na web. **G1**. São Paulo, 14 maio 2018. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/certificado-digital-do-banco-inter-e-revogado-apos-chave-vazar-na-web.html>. Acesso em: 24 nov. 2019.

SCHAEFFER, Cesar; JUNQUEIRA, Daniel. Vivo corrige falha de segurança em portal de serviços. **Olhar Digital**. São Paulo, 05 nov. 2019. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/vivo-corrige-falha-de-seguranca-em-portal-de-servicos/92572>. Acesso em: 24 nov. 2019.

SCHAEFFER, Cesar. [EXCLUSIVO] Falha de segurança expõe dados de 24 milhões de usuários da Vivo. **Olhar Digital**. São Paulo, 04 nov. 2019. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/-exclusivo-falha-de-seguranca-expoe-dados-de-24-milhoes-de-usuarios-da-vivo/92520>. Acesso em: 24 nov. 2019.

UBER termina de notificar usuários brasileiros afetados por vazamento de dados. **Ministério Público do Distrito Federal e Territórios**. Brasília, 27 abr. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10012-uber-termina-de-notificar-usuarios-brasileiros-afetados-por-vazamento-de-dados>. Acesso em: 24 nov. 2019.

VENTURA, Felipe. Banco Inter paga R$ 1,5 milhão e encerra processo sobre vazamento de dados. **Tecnoblog**. 2018. Disponível em: <https://tecnoblog.net/272056/banco-inter-acordo-mpdft/>. Acesso em: 24 nov. 2019.