

São Paulo, 03 de fevereiro de 2021.

Ao Sr. Waldemar Gonçalves Ortunho Júnior, Diretor-Presidente da ANPD;

Ao Sr. André Mendonça, Ministro da Justiça;

À Sra. Juliana Oliveira Domingues, Secretária Nacional do Consumidor;

Ao Sr. Pedro Aurélio de Queiroz Pereira da Silva, Diretor do Departamento de Proteção e Defesa do Consumidor (DPDC);

Ao Subprocurador-geral da República Luiz Augusto Santos Lima, Coordenador da 3ª Câmara de Coordenação e Revisão (Consumidor e Ordem Econômica), do Ministério Público Federal;

Ao Sr. Alfredo Carlos Gonzaga Falcão Júnior, Procurador da República e Coordenador do GT do Sistema Financeiro Nacional da 3ª CCR;

Ao Sr. Alexandre Assunção e Silva, Procurador da República e Coordenador do GT de Tecnologias da Informação e da Comunicação da 3ª CCR;

À Sra. Mariane Guimarães de Mello Oliveira, Procuradora da República e Coordenador do GT do Consumidor da 3ª CCR;

Ao Sr. Carlos Alberto Vilhena, Subprocurador-Geral da República da PFDC;

Ao Senador Rodrigo Pacheco, Presidente do Senado;

Ao Deputado Arthur Lira, Presidente da Câmara dos Deputados;

Ao Sr. Roberto Campos Neto, Presidente do Banco Central;

Ao Sr. Otávio Damaso, Diretor de Regulação do Banco Central;

Ao Sr. Pedro Duarte Guimarães, Presidente da Caixa Econômica Federal (CEF)

Ref.: Gravíssimo vazamento de dados pessoais de mais de 220 milhões de brasileiros

1. O **Idec - Instituto Brasileiro de Defesa do Consumidor** é uma associação de consumidores, sem fins lucrativos, de utilidade pública federal, criada em julho de 1987 e mantida por seus associados. O Idec atua em pesquisas, conscientização do consumidor, incidência em políticas públicas e ações civis públicas com a missão de promover a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica. Desde a sua fundação, o Idec atua na defesa do consumidor, com foco ativo na aprovação de

- importantes legislações do consumidor, como o **Código Brasileiro de Defesa do Consumidor**, em 1990.
2. Ao longo de suas três décadas de existência, este instituto consolidou forte atuação nas esferas judicial e extrajudicial para a proteção dos direitos dos consumidores, inclusive no âmbito da proteção de dados pessoais.
 3. Entre as principais áreas de atuação do Idec tem como objetivo institucional a **proteção dos dados pessoais como direito fundamental dos cidadãos**. Trata-se de tema cada vez mais relevante na agenda de proteção ao consumidor, tendo em vista a centralidade atual dos dados pessoais, com repercussão direta em várias esferas de sua vida, inclusive de segurança, de acesso aos serviços essenciais e de acesso ao crédito.
 4. Sobre o tema, mais recentemente, o Idec participou ativamente das discussões que levaram à aprovação do **Marco Civil da Internet**¹, em 2014, e da **Lei Geral de Proteção de Dados (LGPD)**², aprovada no ano de 2018 após nove anos de debate no Congresso Nacional.
 5. Participamos também das discussões sobre a reforma do **Cadastro Positivo**, em 2019, quando nos opusemos ao cadastro impositivo, cuja abertura é feita de forma automática, não mais voluntária, abrangendo todos os brasileiros com CPF, e que acarreta um grande risco discriminatório e envolve várias questões relacionadas com o processamento de dados pessoais para fins de crédito³. Alertamos para o enorme risco da expansão da análise de dados financeiros de consumidores brasileiros sem uma legislação de proteção de dados em vigor com uma Autoridade atuante e independente para proteger de fato os consumidores⁴.
 6. Esse aviso já vinha sendo feito desde 2018, quando o Idec enviou contribuições ao Banco Central do Brasil sobre "Cadastro positivo e direitos dos consumidores". Neste, o Idec alertava: “[É] *melhor prevenir do que remediar. Não é preciso aguardar um próximo “caso Serasa” para que medidas e normas de incidentes de segurança sejam pensadas no Brasil.*”⁵. Um "caso Serasa" pode ser justamente do que se trata esse incidente.
 7. O Instituto também trabalha para promover e divulgar informações sobre o assunto para

¹ Mais informações em: <https://idec.org.br/conquista/marco-civil-da-internet>.

² A atuação do Idec para aprovação da LGPD pode ser verificada neste link <https://idec.org.br/dadospessoais/linha-do-tempo>.

³ Mais informações em: <https://idec.org.br/cadastro-positivo>.

⁴ <https://www1.folha.uol.com.br/opiniaio/2018/04/rafael-zanatta-e-teresa-liporace-o-que-ha-de-errado-com-o-novo-cadastro.shtml>

⁵ https://idec.org.br/sites/default/files/arquivos/cadastro_positivo_e_direitos_dos_consumidores_0.pdf

milhões de consumidores brasileiros, com a produção de conteúdos relacionados aos direitos dos cidadãos e com informações sobre como se defender em casos de violação de seus direitos⁶. **Portanto, o Idec busca a promoção de uma cultura de proteção de dados em toda a sociedade, incluindo consumidores, empresas e governos.**

8. Deve-se lembrar ainda a decisão paradigmática do **Supremo Tribunal Federal** no julgamento da Medida Cautelar na ADI 6.387/DF, Rel. Min. Rosa Weber, em face da Medida Provisória (MP) n. 954, de 2020, por meio da qual autorizou-se o compartilhamento de dados pessoais de consumidores de serviços de telefonia com o IBGE (Instituto Brasileiro de Geografia e Estatística) para fins de “produção estatística oficial”. Em seu voto extremamente didático, o Min. Gilmar Mendes cravou de modo certo que existe “**um verdadeiro direito fundamental à proteção de dados pessoais**”, a partir da leitura da Constituição Federal. Diante da evolução do conceito de privacidade e das novas tecnologias, o Min. Mendes enfatiza que há um “*direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo*”.
9. Desde 2019, o Idec vem cobrando as autoridades sobre vazamento de dados do Instituto Nacional da Seguridade Social (INSS) e da Empresa de Tecnologia e Informações da Previdência Social (Dataprev), que faz a gestão da Base de Dados daquele instituto⁷. Naquela ocasião foram encaminhadas denúncias e pedidos de providências para várias autoridades, alertando sobre o vazamento de dados e práticas abusivas relacionadas ao empréstimo consignado, apontando falta de eficácia da Administração Pública no combate às práticas ilegais de compartilhamento não autorizado de dados ou vazamentos dentro de seus quadros. Apesar de o INSS ter constituído um Grupo de Trabalho visando apurar as causas do vazamento de dados dos beneficiários do INSS, Portaria n° 844/PRES/INSS, ainda não há notícias sobre a conclusão desses trabalhos.
10. É dentro deste contexto que o Idec, cumprindo com sua missão institucional de defesa do consumidor, tem acompanhado com total atenção as notícias que dão conta de episódio gravíssimo, consistente no vazamento de dados e informações pessoais de, aproximadamente, 223 milhões de brasileiros.
11. **O Instituto vem, completamente estupefocado, perante Vossas Excelências, clamar pela efetivação dos direitos dos cidadãos e dos consumidores, diante do maior vazamento de dados ocorrido no país, com consequências drásticas para toda a**

⁶ Por exemplo, o especial sobre Dados Pessoais, produzido pelo Instituto: <https://idec.org.br/dadospessoais>.

⁷ Mais informações em: <https://idec.org.br/golpe-aposentadoria>.

sociedade brasileira.

12. Tomamos conhecimento de que a **Secretaria Nacional do Consumidor** encaminhou ofício à Serasa Experian, investigada no caso⁸; que a **OAB Nacional** encaminhou ofício à Autoridade Nacional de Proteção de Dados (ANPD) para que esta investigue o caso; que a **ANPD** se manifestou sobre o caso, acionando a Polícia Federal, a empresa que divulgou o vazamento de dados, o **Gabinete de Segurança Institucional da Presidência da República** e o **Comitê Gestor da Internet no Brasil (CGI.br)**⁹; que até mesmo o **Supremo Tribunal Federal** pediu ao **Ministério da Justiça** para tomar as providências que sejam pertinentes, tendo em vista que o vazamento também se deu com relação aos dados dos Ministros daquele Tribunal¹⁰⁻¹¹.
13. Nesse contexto, por se tratar de evento de tamanha monta e de repercussão tão drástica na vida de todos os cidadãos brasileiros, se faz extremamente necessária uma atuação intensa e articulada das instituições para minimizar os danos a todos, assim como investigações profundas para se determinar os responsáveis por esse grave dano ao consumidor que irá perdurar por décadas, aplicando-se as sanções determinadas na lei, além de permitir a reparação integral dos danos sofridos.
14. Só no último trimestre, ocorreram dois outros vazamentos importantes: o de dados do Ministério da Saúde e o da Enel, concessionária de energia elétrica de São Paulo. Em ambos os casos o Idec acionou as autoridades para tomarem providências, mas ainda sem resultados efetivos.
15. No vazamento da Enel, ocorrido em novembro de 2020, ao menos 300 mil cidadãos de Osasco tiveram diversos de seus dados vazados, como CPF e RG e incluindo até mesmo o tipo de imóvel e o endereço. Foram relatados aumentos de fraudes decorrentes do incidente e o Idec pediu esclarecimentos à empresa e oficiou a ANEEL (Agência Nacional de Energia Elétrica) e a ARSESP (Agência Reguladora de Saneamento Básico de São Paulo).
16. Mais preocupante ainda foi o vazamento de dados de 243 milhões de pessoas pelo Ministério da Saúde, através de sistemas informacionais do Hospital Israelita Albert

⁸ <https://valor.globo.com/empresas/noticia/2021/01/26/senacon-notifica-serasa-sobre-sobre-vazamento-de-dados-de-223-milhoes-de-pessoas.ghtml>

⁹ <https://valor.globo.com/empresas/noticia/2021/01/29/anpd-aciona-pf-governo-e-empresa-de-seguranca-para-investigar-vazamento-de-dados.ghtml>

¹⁰ STF pede providências sobre comercialização de dados de ministros.

<http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=459655&ori=1>.

¹¹ <https://link.estadao.com.br/noticias/cultura-digital,dados-de-bolsonaro-e-ministros-do-stf-estao-a-venda-na-internet-apos-megavazamento,70003600653>

Einstein, com quem o Ministério tem um convênio. A ONG Open Knowledge Brasil identificou falha grave, tendo inclusive feito registro em cartório e reportado o caso à Ouvidoria Geral da União, que arquivou a denúncia¹². Os dados incluem informações sobre infectados pela Covid. O Idec enviou representação para a Procuradoria da República de São Paulo¹³ e participou de uma audiência na Câmara dos Deputados sobre o tema¹⁴.

17. Os reiterados casos demonstram que é imperiosa uma atuação conjunta das instituições para melhor regulamentar a matéria, tendo em vista as falhas que sejam encontradas nesta investigação e a dimensão do acontecimento.
18. Ao encaminhar a presente notificação às autoridades competentes, dadas suas atribuições e a natureza dos fatos aqui colocados¹⁵, o Idec pretende dar ciência, colaborar com o grave momento e cobrar atuação firme diante do maior e mais extenso vazamento de dados que ocorreu no nosso país.

I. IMPACTOS SEVEROS E LONGEVOS PARA TODOS OS CIDADÃOS DIANTE DO GRAVÍSSIMO CASO DE VAZAMENTO DE DADOS

19. Foi noticiado, em 11 de janeiro, que um vazamento teria abrangido dados extremamente detalhados de 223 milhões de brasileiros. São cerca de 40 GB em dados pessoais¹⁶.

¹² OKBR. Ministério da Saúde já havia deixado dados pessoais expostos no próprio sistema da Covid-19 em junho; aqui está a prova. <https://www.ok.org.br/noticia/ministerio-da-saude-ja-havia-deixado-dados-pessoais-expostos-no-proprio-sistema-da-covid-19-em-junho-aqui-esta-a-prova/>

¹³ <https://idec.org.br/idec-na-imprensa/idec-pede-ao-mpf-que-estime-vazamento-de-dados-da-saude-deputado-aciona-tcu>

¹⁴ <https://www.correiobraziliense.com.br/brasil/2020/12/4893352-camara-chama-ministerio-da-saude-para-explicar-vazamento-de-dados.html>

¹⁵ **Autoridade Nacional de Proteção de Dados Pessoais**, art. 55-J, caput e incisos, Lei 13.709/2018; **Secretaria Nacional do Consumidor**, art. 55, §1º, e art. 56, CDC; **Ministério Público Federal**, art. 128, I, “a” c/c 129, III, CF/1988; **Banco Central**, art. 10, inc. VI e IX, Lei 4.595/1964 c/c art. 18, Decreto n. 9.936/2019 e art. 14, Resolução Bacen 4737/2019; **Caixa Econômica Federal**, art. 4º e 7º, incisos, Lei 8.036/1990.

¹⁶ **Fontes:**

- <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml>
- <https://link.estadao.com.br/noticias/cultura-digital,senacon-e-procon-sp-vao-notificar-serasa-sobre-vazamento-de-dados-anpd-nao-se-pronuncia,70003593260>
- <https://link.estadao.com.br/noticias/cultura-digital,vazamento-de-220-milhoes-de-cpfs-pode-ser-o-mais-lesivo-do-brasil-diz-especialista,70003592780>
- <https://exame.com/tecnologia/vazamento-de-dados-de-220-milhoes-de-brasileiros-nao-aconteceu-da-noite-para-o-dia/>
- <https://tecnoblog.net/405877/senacon-e-procon-sp-notificam-serasa-sobre-vazamento-de-220-milhoes->

20. O vazamento, descoberto pelo dfndr lab, laboratório especializado em segurança digital da startup PSafe, ainda não teve sua origem identificada. Seu volume é superior à população brasileira porque inclui informações de pessoas falecidas, além de CNPJs, compilados em agosto de 2019.
21. Hoje, entende-se que existe mais de um vazamento, potencialmente interligados. Um primeiro vazamento incluiria informações básicas de CPF e CNPJ (os dois primeiros itens da lista a seguir) e estaria disponível gratuitamente na internet para quem tem o link. Já um segundo vazamento estaria disponível na *deep web* e seria liberado mediante pagamento. A lista inclui os seguintes dados:
 - 21.1. **CPF, nome, sexo e data de nascimento:** Um arquivo de 14 GB com dados básicos referentes a 223 milhões de CPFs. As informações que constam neste arquivo são: nome, sexo e data de nascimento. As informações só incluem pessoas nascidas até 2019.
 - 21.2. **CNPJ:** Um arquivo semelhante ao primeiro, mas com dados do CNPJ (Cadastro Nacional de Pessoas Jurídicas). Em vez do nome das pessoas está o nome da empresa e, no lugar da data de nascimento, consta a data de abertura do CNPJ. Essas informações são públicas – a Receita Federal permite consultar diversos dados referentes aos números de CNPJ. Inclui dados de 40 milhões de empresas.
 - 21.3. **Dados de veículos:** Uma tabela de 23 GB com dados de 104 milhões de veículos, incluindo placa, modelo e até tipo de combustível. Os dados neste arquivo estão aparentemente limitados ao ano de 2007.
 - 21.4. **Outros dados:** Uma tabela de 37 colunas, nesse caso de 140 milhões de CPFs e CNPJs, que servem de referência para saber quais dados estão disponíveis nos 37 pacotes que foram colocados à venda. Além dos dados já incluídos nos pacotes anteriores, os pacotes contêm:
 - 21.4.1. Endereços;
 - 21.4.2. Fotos de rosto;
 - 21.4.3. Imposto de renda de pessoa física (IRPF);
 - 21.4.4. Participantes do Bolsa Família;
 - 21.4.5. *Score* de crédito, renda, cheques sem fundo e outras informações financeiras;
 - 21.4.6. Telefone e dados cadastrais de serviços de telefonia;
 - 21.4.7. Escolaridade;

-
- [de-cpfs/
https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-saiba-como-fraudadores-sacam-o-fgts-e-o-que-fazer-para-evitar-o-golpe.ghtml](https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-saiba-como-fraudadores-sacam-o-fgts-e-o-que-fazer-para-evitar-o-golpe.ghtml)

- 21.4.8. Benefícios do INSS;
 - 21.4.9. Dados relativos a servidores públicos;
 - 21.4.10. Informações do LinkedIn.
22. Para se ter uma ideia da quantidade e expressividade dos dados vazados, a título de exemplo, no caso IBGE, julgado pelo STF, estavam em jogo o compartilhamento de dados por empresas de telecomunicação prestadoras do STFC (telefonia fixa) e do SMP (telefonia móvel), que deveriam disponibilizar à Fundação IBGE, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.
23. A decisão emblemática do STF enfatizou que *“na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais não de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos”*. Ou seja, no caso presente de vazamento de dados de mais de 220 milhões de brasileiros, com muito mais dados quantitativa e qualificativamente em comparação com aqueles descritos na ADI julgada pelo STF, há uma violação massiva e frontal à Constituição Federal e todo o ordenamento jurídico de proteção de dados e do consumidor.
24. Até a data de 28 de janeiro de 2021, tivemos conhecimento de que alguns desses dados foram baixados por 68 usuários¹⁷. Segundo divulgado pela imprensa, o **pagamento** é feito em bitcoins, mais difícil de serem rastreados, e estima-se que a venda desses dados pode render até US\$15 milhões para o responsável, o que equivale a aproximadamente R\$ 80 milhões. No fórum de vendas das informações, o *cracker* afirma que a compra mínima é de US\$ 500 (R\$ 2.693,75) e que cada lote de dados com até 100 pessoas físicas ou jurídicas custaria cerca de US\$50 (R\$269,90), valor que pode chegar a US\$100 (R\$538,80) caso envolva os dados do Mosaic, da Serasa¹⁸.
25. A **origem do vazamento** ainda é desconhecida e estima-se que pode decorrer de diferentes fontes, mas alguns dos dados vazados podem sinalizar ao menos uma das origens do incidente. Isso porque, uma das bases de dados incluída no vazamento supostamente pertence ao Mosaic, serviço do birô de crédito Serasa Experian. Além de

¹⁷ <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-saiba-como-fraudadores-sacam-o-fgts-e-o-que-fazer-para-evitar-o-golpe.ghtml>

¹⁸ <https://www1.folha.uol.com.br/mercado/2021/02/dados-vazados-podem-render-r-808-milhoes-ao-criminoso.shtml>

ser uma informação específica do birô, o responsável pela venda dos dados afirma que esta é sua origem.

26. No entanto, a empresa nega seu envolvimento. Segundo o Serasa, “[m]uitos dos dados analisados incluem elementos que não temos em nosso sistema e os dados atribuídos à Serasa não correspondem aos dados em nossos arquivos.”
27. Para além da Serasa, algumas das informações incluem telefones celulares e o tipo de plano de clientes da operadora Vivo, de modo que pelos indícios aqui apontados, se demonstra extremamente relevante o envio de ofícios com pedido de explicações para tais empresas, assim como para outras que forem indicadas como envolvidas, após apuração.
28. Trata-se de **caso paradigmático**. Isso porque seu volume e sua abrangência corresponde à totalidade da população brasileira - e até a supera, já que também inclui dados de falecidos e dados de empresas. Este pode ser um dos vazamentos mais sérios do mundo, tanto pela quantidade de pessoas afetadas quanto pela diversidade e relevância dos dados¹⁹.
29. Referido vazamento tem potencial de se tornar mais relevante que o caso Equifax (2017), o mais sério vazamento de um birô de crédito ocorrido até o momento. Naquela oportunidade, o vazamento desta empresa norte-americana afetou 145 milhões de pessoas. Dentre as informações vazadas, estavam nomes, número da seguridade social, aniversários, endereços e, em alguns casos, placas de carros e números de cartão de crédito - bem semelhante a alguns dos dados vazados no episódio brasileiro-, que inclui ainda mais informações. A empresa firmou um acordo com a Federal Trade Commission (FTC) no valor de US\$ 650 milhões (aproximadamente R\$ 3,49 bilhões)²⁰.
30. A **consequência de vazamentos** de dados, especialmente da monta deste, é grave. Os consumidores ficam expostos e vulneráveis à fraudes, como roubo de identidade, ou *phishing*; manipulações e discriminações por inserções em base de dados para fins publicitários ou eleitorais desconhecidos. Ainda, há risco de submeterem-se à sérios prejuízos financeiros, como utilizar-se dessas informações para saque do FGTS, que se tornou ainda mais relevante com o FGTS emergencial, disponível para saque no momento da pandemia²¹.
31. Isso porque, como afirma Bruno Bioni, “[é] um conjunto de informações muito rico

¹⁹ <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

²⁰ <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>

²¹ <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-saiba-como-fraudadores-sacam-o-fgts-e-o-que-fazer-para-evitar-o-golpe.ghtml>

sobre as pessoas. Isso torna o incidente de segurança mais crítico, mais lesivo, como a gente não havia visto até então no Brasil."²². Já Ronaldo Lemos sintetiza o caso como "vazamento de dados do fim do mundo", cujas consequências perdurarão por anos²³.

32. Não obstante a gravidade desses fatos, ainda foi noticiado em 02 de fevereiro de 2021, que um vazamento teria afetado mais de 270 milhões de brasileiros²⁴. Desta vez, a origem seria atribuída à DataPrev, empresa de tecnologia da informação da Previdência Social. Os fatos ainda não foram suficientemente apurados, mas por também se relacionaram com sérios dados dos consumidores e que podem implicar em altos riscos de fraudes, indica-se o incidente com requerimento de prestação de informações e tomada de diligências sobre o assunto, inclusive notificando a empresa.
33. Vê-se, portanto, a gravidade dos fatos narrados. Por essas razões, se expõem os motivos de direito à seguir, urgindo para a cooperação interinstitucional, de modo a garantir, no mínimo, efetividade nas investigações e responsabilização dos responsáveis e contenção dos danos.

II. DA COMPETÊNCIA DAS DIVERSAS AUTORIDADES E DA NECESSIDADE DE COOPERAÇÃO INSTITUCIONAL

34. A abrangência e complexidade do caso exige que todas as autoridades competentes se articulem de modo a garantir eficiência, rapidez e eficácia nas investigações e responsabilização pelos danos causados. A dimensão deste vazamento de dados atinge a todos os brasileiros e demanda das autoridades equivalente atuação coordenada. Nesse sentido, cabe destacar as autoridades competentes e os mandamentos legais para articulação interinstitucional.
35. **Autoridade Nacional de Proteção de Dados (ANPD)**. A despeito da aplicação de sanções da ANPD ter sido adiada para 01º de agosto de 2021, todos os artigos referentes ao exercício de suas funções já estão em vigor desde dezembro de 2018. A ANPD tem a competência de investigar por meio de processo administrativo, fiscalizar, determinar auditoria para averiguar os vazamentos de dados aqui tratados, conforme estabelece o art. 55-J da LGPD:

²² <https://link.estadao.com.br/noticias/cultura-digital,vazamento-de-220-milhoes-de-cpfs-pode-ser-o-mais-lesivo-do-brasil-diz-especialista,70003592780>

²³ <https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml?origin=folha>

²⁴ <https://www.cisoadvisor.com.br/hacker-poe-a-venda-na-dark-web-270-milhoes-de-registros-da-dataprev/>

Art. 55-J. Compete à ANPD:

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (...)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (...)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (...)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

36. Assim, a ANPD pode atuar tecnicamente para apurar violações à LGPD, determinar a realização de auditorias, orientar medidas para responsabilização e minimização de danos, por meio, por exemplo, da formatação de plano de contingência apto à reparação de danos às pessoas vítimas do vazamento. Além disso, deve a Autoridade comunicar os órgãos de controle o descumprimento pela administração pública do disposto na Lei de Dados.
37. A LGPD também estabelece competência para a ANPD articular-se com outras autoridades reguladoras. Frente à impossibilidade de aplicação de sanções e o fato de que a ANPD ainda se encontra em fase de estruturação, essa interlocução se torna ainda mais precípua. Nesse sentido, é competência da ANPD **“articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação”** (art. 55-J, XXIII da LGPD).
38. A LGPD ainda impõe o dever de coordenação entre autoridades e órgãos competentes para garantir eficiência nos setores regulados:

Art. 55-J, § 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

Art. 55-K. [...] “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.”

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante)

39. **Sistema Nacional de Defesa do Consumidor (SNDC).** A LGPD destaca a conexão com o direito do consumidor: tendo a defesa do consumidor como um de seus fundamentos (art. 2º, VI); ao garantir o direito de peticionar em relação aos seus dados contra o controlador perante organismos de defesa do consumidor (art. 18, §8º).
40. Nesse sentido, são aplicáveis também as normas de Direito do Consumidor, nomeadamente o **Código de Defesa do Consumidor (Lei 8.078/1990, CDC)**. Por se tratar de dados provenientes de relações de consumo, como dados cadastrais utilizados para exercício de serviço público, ou pontuação de crédito e demais informações financeiras que ficam sob a guarda de cadastro de consumidores (mesmo que ainda não comprovada a origem precisa), **é nítido que os vazamentos envolvem relações de consumo e atraem, por consequência, a aplicação do CDC.**
41. Tal lei é de aplicação difusa pelo Judiciário e pelos Procons, mas tem sua aplicação promovida e harmonizada nacionalmente pela **Secretaria Nacional do Consumidor (Senacon)**, vinculada ao Ministério da Justiça e Segurança Pública. Assim, cabe à Senacon, em coordenação do SNDC:

Lei. 8.078/90

Art. 106 (...)

II - receber, analisar, avaliar e encaminhar consultas, denúncias ou sugestões apresentadas por entidades representativas ou pessoas jurídicas de direito público ou privado;

VI - representar ao Ministério Público competente para fins de adoção de medidas processuais no âmbito de suas atribuições;

VII - levar ao conhecimento dos órgãos competentes as infrações de ordem administrativa que violem os interesses difusos, coletivos, ou individuais dos consumidores;

Parágrafo único. Para a consecução de seus objetivos, o Departamento Nacional de Defesa do Consumidor poderá solicitar o concurso de órgãos e entidades de notória especialização técnico-científica.

42. Em 26/01/2021, a Senacon instaurou procedimento de averiguação preliminar com notificação à Serasa Experian, suspeita de estar envolvida no vazamento. Outro integrante do SNDC, o Procon-SP, também já se debruça sobre o assunto.
43. Para além da aplicação de seus dispositivos gerais, aplicam-se sanções administrativas dispostas no CDC (art. 56), dentre as quais incluem multa, que pode chegar a R\$10 milhões, suspensão do fornecimento do produto e/ou serviço, suspensão temporária da atividade, revogação da concessão ou permissão de uso, interdição total ou parcial, intervenção administrativa e imposição de contrapropaganda, além da previsão de reparação integral para os consumidores lesados, em cumprimento ao princípio constitucional do acesso à justiça (art. 5º, XXXV, CF).
44. A proteção a direitos difusos, observáveis no âmbito da proteção de dados enquanto direito individual e coletivo, também é função primordial do **Ministério Público** (art. 128, I, “a” c/c 129, III, CF/1988) e a LC n. 75/1993 dispõe sobre a competência do Ministério Público Federal (e, conseqüentemente, da Justiça Federal) e sua atribuição de promover a responsabilidade de do fornecedor de produtos e serviços por atos ilegais que tenham cometido, conforme art. 6º, incisos VII, alíneas “a” e “c”; XIII; XIV, alíneas “c” e “e”; XX.
45. **Polícia Federal**. Ademais, cabe à ANPD comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (art. 55-J XXI). Assim, considerando a provável ocorrência dos crimes de quebra de sigilo financeiro (art. 10 da LC 105/2001) e de violação de sigilo funcional (art. 325 §2º do CP), urge-se a participação da Polícia Federal para fins de investigação da origem do vazamento de dados, semelhante do ocorrido recentemente na operação Data Leaks, que investiga vazamento de dados do INSS²⁵.
46. **Banco Central do Brasil (BCB)**. Dada a suspeita de que o vazamento de dados tenha sido proveniente de birô de crédito, o BCB também deve ser envolvido nas investigações, tanto pelo fato de terem sido vazados dados bancários, como histórico de cheque, quanto

²⁵ PF e MPF deflagram a 2ª fase da Operação Data Leak. Disponível em:
<http://www.pf.gov.br/agencia/noticias/2019/02/pf-e-mpf-deflagram-a-2a-fase-da-operacao-data-leak>

pelo fato noticiado acerca de aumento de fraudes bancárias.

47. Sobre esse último ponto, em consonância com a Lei do Cadastro Positivo, **art. 12, §3º e 5º, LCP**, a **Resolução Bacen nº 4.737/2019**, art. 14, determina infrações à regulamentação do CMN sujeitam o gestor ao cancelamento do seu registro junto ao BCB, “*considerando as circunstâncias de cada caso concreto e o contexto dos fatos*”, mediante processo administrativo próprio e de garantia do devido processo legal, conforme descrito na Lei nº 9.784/1999.
48. Não é demais pontuar que o BCB deve verificar se todos os requisitos técnicos de segurança da informação dos birôs de crédito foram cumpridos, conforme art. 6º, inc. II, da **Resolução Bacen 4.737/2019** e art. 2º, inc. II e III, do **Decreto nº 9.936/2019**. Cabe verificar se o gestor de banco adotou as medidas necessárias para a preservação do sigilo das informações, mantendo os sistemas de guarda e acesso com requisitos de segurança que protejam as informações de acesso não autorizado, conforme Decreto nº 9.936/19, art. 10, II e III.
49. **Caixa Econômica Federal.** Diante das notícias que demonstram que os cidadãos já estão sendo vítimas de fraude, principalmente com a retirada indevida do FGTS do trabalhador, mediante a utilização dos dados vazados para acesso aos aplicativos, é necessário a CEF fazer parte dos encaminhamentos, tendo vista que é o órgão gestor do FGTS e responsável pelo aplicativo que tem sido objeto de fraude (art. 4º e 7º, incisos, Lei 8.036/1990).
50. A cooperação institucional entre as autoridades competentes elencadas deve ser coordenada primordialmente pela ANPD que é o órgão central de interpretação e aplicação da LGPD, inclusive com a criação de um **Comitê de Crise**, que permita o tratamento adequado desse enorme incidente que envolve uma enorme quantidade de dados, de pessoas atingidas e de instituições (públicas e privadas), que devem estar em contato para solucionar o quanto antes os diversos problemas, cessar a violação dos direitos e ressarcir aqueles que sofrerem danos.
51. A cooperação interinstitucional, aqui suscitada e incentivada, visa à melhor apuração dos fatos, identificação dos responsáveis, apuração dos danos (e de seu nexos de causalidade) para eventual punição pelos ilícitos perpetrados.

III. DA VIOLAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS E AO CÓDIGO DE DEFESA DO CONSUMIDOR: INOBSERVÂNCIA DOS PRINCÍPIOS DA SEGURANÇA E PREVENÇÃO E DE DIREITOS BÁSICOS DO CONSUMIDOR

a. Grave violação do dever de segurança no fornecimento de serviços

52. A proteção de dados pessoais é um direito decorrente dos direitos fundamentais à vida privada e intimidade, conforme definido no artigo 5º, *caput* e inciso X, ambos da Constituição Federal.
53. A Lei Geral de Proteção de Dados descreve, no artigo 6º, os seguintes princípios:
- 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;
54. A segurança é direito básico do consumidor, como afirmado pelo artigo 6º, inciso I, do CDC. Ainda, sobre a segurança dos serviços colocados no mercado de consumo, versa o mesmo diploma legal:
- Art. 8º produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito.
55. A ausência de medidas técnicas e administrativas aptas a proteger os dados, somada à ausência de medidas capazes de prevenir a ocorrência desse dano, gerou um cenário de descaso com relação aos cidadãos.
56. O resultado foi a vulnerabilidade de dados de milhões de cidadãos brasileiros, que hoje ficam expostos a quaisquer possibilidades de práticas ilícitas e maliciosas de terceiros sob posse dessas informações. Os requisitos legais - o respeito ao princípio da prevenção e à segurança como direito básico dos cidadãos - não foram observados, ficando assim evidente a violação cometida.
57. A vulnerabilidade é pressuposto das relações de consumo (art. 4º, inciso I, CDC). No presente caso, ganha especial relevo pela exposição de dados ter ocorrido em plena pandemia, momento de instabilidade econômica em que as pessoas já passam por inúmeras dificuldades.
58. É enorme o risco de utilização desses dados para fraudes. Tem sido crescentes os casos

em que pessoas têm o seu CPF reiteradamente utilizado de maneira ilegal por terceiros. Tais práticas fraudulentas ocorrem justamente devido a vazamentos como esse e, não raras vezes, o problema não ocorre apenas uma vez, sendo que em muitos casos medidas judiciais são necessárias.

59. O vazamento dos dados também possibilita ataques fraudulentos que, comumente, se utilizam de informações deixadas expostas como maneira de “capturar” uma pessoa e enganá-la, o que vem aumentando exponencialmente no país²⁶. Chamada de *phishing*, essa prática simula uma situação real - um e-mail com uma promoção ou com um boleto falso referente a uma dívida existente, por exemplo - e leva cidadãos a compartilharem informações confidenciais como senhas e número de cartões de crédito, ou a realizar pagamentos indevidos.
60. O nível de detalhamento dos dados vazados coloca os consumidores em situação de risco exacerbada, não somente em relação a golpes financeiros, mas também com a possibilidade de dados comportamentais serem utilizados para fins desconhecidos e ilegítimos, desde uso para manipulação eleitoral, a perseguições políticas ou discriminações.
61. Ainda, considerando a natureza do fluxo informacional, em muitos casos, a reparação de danos é inviável, visto que, uma vez vazada, perde-se o controle sobre a informação pessoal.
62. É inegável, portanto, a ocorrência de danos à vida privada e à intimidade das pessoas que tiveram seus dados pessoais expostos, sendo necessária a investigação dos fatos narrados e consequente responsabilização da empresa envolvida.

b. Violação do dever de informar e ausência de comunicação à ANPD

63. Além da violação do dever de segurança e prevenção previstos no CDC e na LGPD, o consumidor tem violado seu direito à informação, uma vez que o agente de tratamento responsável pela base de dados não assumiu a origem do vazamento e, conseqüentemente, não notificou os titulares acerca do incidente. Tampouco houve campanha de informação acerca dos danos ocorridos, dos riscos existentes para o consumidor e das medidas que podem ser adotadas.
64. Nesse sentido, viola-se o direito do consumidor de informação adequada e clara sobre os

²⁶ Fantástico. Mais de 60 milhões de brasileiros já sofreram com fraude financeira na internet, diz pesquisa. <https://g1.globo.com/fantastico/noticia/2021/01/31/mais-de-60-milhoes-de-brasileiros-ja-sofreram-com-fraude-financeira-na-internet-diz-pesquisa.ghtml>

riscos apresentados pelo serviço (art. 6º, III), bem como os deveres de comunicação estabelecidos na LGPD:

Art. 48. **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.

§ 1º A comunicação será feita **em prazo razoável**, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

c. Necessária reparação dos danos sofridos pelos cidadãos

65. Em suma, considerando a nítida violação aos direitos do consumidor-cidadão de segurança e informação e a incontestada ocorrência de danos materiais e morais de natureza individual e coletiva, faz-se necessária a adoção imediata e urgente, por parte das autoridades competentes, de medidas capazes de (i) investigar as origens e causas do vazamento; e (ii) reparar e minimizar os danos causados, conforme pedidos elencados no tópico a seguir.
66. Ressaltamos que devem ser ressarcidos todos os danos individuais e coletivos, materiais e morais, que os cidadãos venham a sofrer (art. 42, §3º, LGPD). É dever do Estado propiciar ao cidadão, no mínimo, informações de como proceder com relação à documentação e produção probatória sobre os danos sofridos, também para cumprir o dever de facilitação da defesa do consumidor (art. 6º, inc. VIII, CDC).

IV. Pedidos

67. Como conclusão, o Idec entende que é de extrema urgência a adoção de uma cooperação interinstitucional entre os órgãos aqui oficiados. Para tanto, desde já requer que sejam criados instrumentos para dar ampla informação aos consumidores sobre os principais acontecimentos decorrentes do incidente aqui narrado, assim como quais medidas de segurança e quais outros direitos a população afetada possui, sem prejuízo da criação de

16

um canal centralizado para que os consumidores possam relatar casos de fraude que ocorreram dentro do período de vazamento.

68. A instauração e publicização das informações sobre os procedimentos e/ou inquéritos nos respectivos órgãos para apuração da origem e dos responsáveis pelo vazamento, caso já não tenham sido instaurados. Ressaltamos que a publicização dos atos processuais referentes a esse vazamento é de interesse público.
69. É necessário que sejam tomadas fortes medidas de segurança em toda a cadeia de tratamento de dados que deu origem ao vazamento, para que essa situação não volte a ocorrer. A apresentação de execução de um plano de contingência para reparar e minimizar os danos causados pelo vazamento, com a destinação de recursos para eventuais danos sofridos pelos consumidores é uma medida imperiosa.
70. Diante do exposto e frente à urgência do vazamento, que tem potencial de ser o mais grave da história, o **Instituto Brasileiro de Defesa do Consumidor** requer, em suma²⁷:
- (i) identificar se a base comercializada foi obtida de agentes de tratamento de dados que possuem dever de cumprimento da LGPD;
 - (ii) **realizar auditoria** para identificar se o incidente é originário de invasão de sistemas da Serasa Experian ou de outros birôs de crédito, com a verificação se há dados vazados que não estão presentes na base de dados do birô e seus terceirizados, bem como se as informações financeiras conferem com as informações específicas da metodologia de cada birô (ex: pontuação de crédito e classificação dos consumidores), por meio de auditoria prevista na LGPD, art. 55-J, inc. XVI;
 - (iii) aplicar imediatamente as regras previstas no capítulo de **segurança e boas práticas** previsto na LGPD, em especial os artigos relacionados à elaboração de **Plano de Resposta a Incidente de Segurança** e comunicação com ANPD;
 - (iv) construir um **Plano de Resposta ao Incidente de Segurança** que deverá dar especial ênfase aos riscos e danos relevantes aos titulares, incluindo as possibilidades de golpes de engenharia social, roubo de identidade, fraudes lesivas e, se possível, diminuição da pontuação do risco de crédito;
 - (v) determinar a **estruturação de um plano para atendimento permanente às pessoas afetadas, por parte dos responsáveis pelo incidente**. Esse plano deve incluir, não exaustivamente, a disponibilização de (a) canal de atendimento facilitado (via Whatsapp,

²⁷ As recomendações dos itens i a vi foram inspiradas no documento produzido pela **Associação Data Privacy Brasil de Pesquisa**, Comunicado 001/2021 Produzido em 25.01.2021, assim como nas entrevistas dadas pelos professores Bruno Bioni (<https://link.estadao.com.br/noticias/cultura-digital,vazamento-de-220-milhoes-de-cpfs-pode-ser-o-mais-lesivo-do-brasil-diz-especialista,70003592780>) e Rafael Zanatta (<https://tecnoblog.net/406175/tecnocast-177-o-grande-vazamento-de-dados-do-brasil/>).

Instagram, Facebook e página própria) para confirmação de dados vazados e esclarecimento de dúvidas, (b) materiais de instrução sobre como prevenir golpes de engenharia social com base nos dados, e (c) soluções de monitoramento de CPF, por um período crítico de tempo, de forma gratuita;

(vi) as medidas adotadas para mitigação de riscos através de página *web* própria devem utilizar formato aberto para permitir a verificação permanente por terceiros da segurança conferida e, em conformidade à diretriz da atuação do poder público no desenvolvimento da internet no Brasil (art. 24, V, Lei nº 12.965/2014);

(vii) garantir a implementação de um plano de resposta ao incidente estruturado e eficiente através do uso de recursos emergenciais do Fundo de Direitos Difusos. Os recursos utilizados devem ser devidamente restituídos após a identificação e responsabilização do agente de tratamento envolvido;

(viii) determinar a cooperação institucional entre a ANPD, Banco Central e o Sistema Nacional de Defesa do Consumidor para a defesa de toda a coletividade afetada, tendo em vista que se trata de um incidente de segurança que envolve relação de consumo e o score de crédito (LGPD, art. 55-J, §4º);

(ix) considerando que há vazamento de dados do score de crédito e outros dados bancários do consumidor, deve o Banco Central abrir processo administrativo e participar da articulação interinstitucional para fins de fiscalização e penalização de instituições financeiras e birôs de crédito;

1) À Autoridade Nacional de Proteção de Dados:

- a) Publicação imediata de site/portal público específico com orientações gerais aos cidadãos sobre os dados vazados, abrindo um canal de informação e orientação completa sobre os vazamentos e demais incidentes de segurança;
- b) A publicização dos atos processuais referentes a esse vazamento, de interesse público;
- c) Priorizar o item sobre “Comunicação de incidentes e especificação do prazo de notificação”, conforme disposto em sua agenda regulatória, recém-publicada, especialmente a adoção de parâmetros para resposta a incidentes e remediação (art. 50, §2º, LGPD);
- d) Conhecida a origem dos vazamentos, determinar, ao agente de tratamento, a ampla divulgação do fato em meios de comunicação e a adoção de medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2º, LGPD);

- e) Permitir a participação das associações de consumidores e posterior publicação dos relatórios para possibilitar a reparação na forma coletiva dos danos sofridos, nos termos do art. 42, §3º, LGPD.

2) Ao Ministério da Justiça e Segurança Pública:

- a) O exercício de orientação, coordenação e supervisão dos órgãos e entidades da administração federal na área de sua competência de "IV - defesa da ordem econômica nacional e dos direitos do consumidor", nos termos do art. 87, parágrafo único, inciso I da Constituição Federal e art. 1º, inciso IV, do Decreto nº 9.662/2019.

3) À Secretaria Nacional do Consumidor:

- a) Garantir a efetiva prevenção e reparação de danos patrimoniais e morais aos consumidores (art. 6º, VI, CDC), com a aplicação de multa ao agente de tratamento responsável (art. 56, I, CDC), que deve ser direcionada ao Fundo de Direitos Difusos em prol da proteção dos consumidores, sem prejuízo de outras sanções civis e penais;
- b) Articular junto com o SNDC, órgãos federais, estaduais, do Distrito Federal e municipais e as entidades privadas de defesa do consumidor, medidas de prevenção e de informação ao consumidor acerca dos vazamentos de dados (art. 106, inc. I, CDC), prestando informação clara e adequada e orientação ao consumidor-cidadão (art. 106, inc. III e IV, CDC), além de permitir a reparação dos danos sofridos (art. 6º, inc. VIII, CDC); e
- c) Constatada a negligência ou omissão do agente de tratamento em garantir as medidas de segurança de dados adequadas, determinar medidas necessárias e adequadas para o caso, inclusive podendo determinar a suspensão de fornecimento do serviço (art. 56, VI e 58, CDC).

4) À Polícia Federal:

- a) Apurar as possíveis infrações e responsabilidades quanto aos casos narrados, em especial em relação ao sigilo bancário (art. 10 da LC 105/2001) e ao sigilo funcional (art. 325 §2º do CP), por haver repercussões interestaduais das infrações (art. 144, § 1º, I e IV, CF/88);

- b) A publicização dos atos e inquéritos referentes a esse vazamento, de interesse público;

5) Ao Ministério Público Federal:

- a) Instaurar inquérito civil para realização das investigações, em coordenação com demais autoridades competentes (art. 7º, I, LC 75/93);
- b) Requisitar e acompanhar diligências investigatórias e a instauração de inquérito policial (art. 7º, I, LC 75/93);
- c) Exaurida a fase investigatória, promover ação civil pública para a proteção dos interesses difusos e coletivos e dos consumidores (art. 6º, IV, c, LC 75/93) para a responsabilização dos agentes de tratamento envolvidos (art. 13, LC 75/93).

6) Ao Banco Central:

- a) Peça informações à ANPD e aos birôs de crédito sobre o vazamento de dados bancários e do *score* de crédito dos consumidores, determinando a realização de auditoria e abertura de processo administrativo, para fins de cumprimento do art. 18, e parágrafos, do Decreto 9.636/2018;
- b) Determine às instituições financeiras que sejam intensificadas as medidas de segurança dos dados dos consumidores e que relatórios de fraudes sejam encaminhados periodicamente ao BCB e à ANPD.

7) Ao Congresso Nacional:

- a) Abertura de Comissão Parlamentar Mista de Inquérito (CPMI) destinada a investigar os vazamentos de dados aqui tratados por prazo certo e com poderes de investigação próprios das autoridades judiciais (CF, art. 58, § 3º; RCCN, art. 21; RICD, arts. 35 a 37; RISF, arts. 145 a 153);
- b) Realização de audiência pública com a participação reguladores (Banco Central, ANPD, Senacon), dos birôs de crédito com atuação no país, com a Receita Federal, a empresa Telefônica S.A. e demais suspeitos de serem responsáveis pela origem do vazamento, garantida a participação da sociedade civil;
- c) Criação, por Ato Conjunto dos Presidentes do Senado Federal e da Câmara dos Deputados, de uma "Comissão Mista de Proteção de Dados", tendo em vista o forte impacto desses assuntos aos cidadãos e que possuem especificidade própria,

transcendendo as comissões do consumidor e de tecnologia e perpassando as competências de ambas as Casas;

8) À Caixa Econômica Federal:

- a) Revisão de suas práticas de segurança, principalmente dos aplicativos ligados ao FGTS, prestar esclarecimentos à sociedade e atender adequadamente às demandas dos consumidores que foram vítimas de fraude.

71. Por fim, a entidade noticiante também requer:

- a. Qualquer que seja a análise procedida, seja feito exame das condutas noticiadas à luz de toda a legislação acima mencionada, inclusive, se for o caso, apuração de responsabilidades à luz da CF/1988, assim como da Lei nº 8.429/1992.
- b. Qualquer que seja a análise procedida da(s) jurisdicionada(s), que a mesma seja realizada não só à luz do exame de conformidade, mas também sob a ótica do desempenho/eficiência (art. 37, caput, CF/1988).
- c. Que as diligências a serem adotadas no âmbito das autoridades, para além das vias investigativas, sejam acompanhadas da adoção de todas as medidas urgentes quanto bastem para obstar os prejuízos imediatos e gravíssimos experimentados pelos brasileiros.
- d. Sua habilitação como interessado em eventual procedimento que vier a ser instaurado, requerendo a intimação dos resultados desta promoção para as providências de estilo.
- e. Que seja a entidade subscritora comunicada de seu encaminhamento/resultado, fundamentadamente.

São Paulo, 03 de fevereiro de 2021.

Teresa Liporace
Coordenadora Executiva

Diogo Moyses Rodrigues
Coord. Programa de Direitos Digitais

Juliana Oms

Michel Roberto Oliveira de Souza

OAB/SP 442.657

OAB/SP 323.983

Christian Tárík Printes

Bárbara Prado Simão

OAB/SP 316.680

OAB/SP 428.335

Camila Leite Contri

Pesquisadora do Programa de Direitos Digitais