INSTITUTO BRASILEIRO DE DEFESA DA PROTEÇÃO DE DADOS PESSOAIS, COMPLIANCE E SEGURANÇA DA INFORMAÇÃO – SIGILO

EXMO. SR. DR. JUIZ FEDERAL DE UMA DAS VARAS CÍVEIS DE SÃO PAULO-SP.

INSTITUTO BRASILEIRO DE DEFESA DA PROTEÇÃO DE DADOS PESSOAIS, COMPLIANCE E SEGURANÇA DA INFORMAÇÃO - SIGILO, pessoa jurídica de direito privado, inscrita no CNPJ nº 32.574.046/0001-00, com sede na Avenida Angélica n. 2632, cj. 63, Consolação, CEP 01228-200, São Paulo-SP, por seus advogados, vem, respeitosamente perante V.Exa., propor a seguinte

AÇÃO CIVIL PÚBLICA C.C. INDENIZAÇÃO POR PERDAS E DANOS MORAIS E MATERIAIS, com pedido de TUTELA DE URGÊNCIA

com fundamento no art. 5º, inc. X, XXVII e XXIX, da CF de 1988, nos arts. 6º, 7º, 9º, 15, 16, 18, 19, 22, 41, 42, 43, 46, 47, 48, 51, 52 e 53, da LGPD, nos arts. 6º, incs. III, IV, VI e VIII, 42, parágrafo único, e 43, §§ 2º e 3º, e 101, inc, I, do Código de Defesa do Consumidor e art. 1 e 7º do Marco Civil da Internet, LACP (Lei n. 7.347/1985) arts. 1º e 2º, dentre outros, contra **SERASA EXPERIAN S.A.**, pessoa jurídica, inscrita no CNPJ/MF sob o n. 62.173.620/0001-80, com sede na Rua Antônio Carlos n. 434, CEP 01309-010, Cerqueira César, São Paulo SP, e da **UNIÃO FEDERAL** (**AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS - ANPD)**, com sede na Praça dos Três Poderes, Anexo I, Ala B, sala 101, Brasília-DF, pelas motivações fáticas e fundamentos legais que passa a expor:

1 - PRELIMINARMENTE

1.1. DA LEGITIMIDADE DO AUTOR

O **INSTITUTO SIGILO** é associação sem fins lucrativos, fundada há mais de 1 (um), que detém, entre outros objetivos listados em seu Estatuto, abaixo transcrito:

> Art. 1º O INSTITUTO BRASILEIRO DE DEFESA DA PROTEÇÃO DE DADOS PESSOAIS, COMPLIANCE E SEGURANÇA DA INFORMAÇÃO SIGILO, doravante denominada SIGILO, é uma associação de direito privado, sem fins lucrativos e com fins educacionais e sociais de âmbito nacional, **cujo objetivo é a defesa da proteção de dados pessoais, da segurança da informação, das práticas de compliance, dos direitos fundamentais digitais, bem como a inclusão digital, mediante a representação e defesa dos direitos dos usuários, presentes e futuros, e prestadores de serviços de acesso e aplicações de Internet, em todas as instâncias que se fizerem necessárias**. [Grifou-se].

Como se vê, um dos objetivos do referido instituto é a defesa da proteção de dados dos consumidores, bem como a proteção dos direitos fundamentais digitais.

Além disso, o art. 5° da Lei n. 7.347/85, determina que é legitimada ativa a associação que:

> Art. 5º Têm legitimidade para propor a ação principal e a ação cautelar:
> (...) V – **a associação que, concomitantemente**:
> a) **esteja constituída há pelo menos 1 (um) ano nos termos da lei civil**;
> b) **inclua, entre suas finalidades institucionais, a proteção** ao patrimônio público e social, ao meio ambiente, **ao consumidor**, à ordem econômica, à livre concorrência, aos direitos de grupos raciais, étnicos ou religiosos ou ao patrimônio artístico, estético, histórico, turístico e paisagístico.

O Código de Defesa do Consumidor também estabelece que o direito dos consumidores poderá ser realizado de forma coletiva.

> **Art. 81**. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo.
> Parágrafo único. A defesa coletiva será exercida quando se tratar de:
> I – interesses ou direitos difusos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato;
> II – interesses ou direitos coletivos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base;
> III – interesses ou direitos individuais homogêneos, assim entendidos os decorrentes de origem comum.

A legislação em comento estabeleceu, também, os legitimados para propor ação em defesa dos consumidores.

> Art. 82. Para os fins do art. 81, parágrafo único, são legitimados concorrentemente:
> (...)
> IV – **as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos por este código, dispensada a autorização assemblear**. – Grifou-se

Diante disso, o presente instituto é legitimado para propor ações em nome dos consumidores que possam ter seus direitos violados com relação ao uso indiscriminado de seus dados por terceiros.

Por fim, restará demonstrado que a situação apresentada na presente demanda se trata de direitos individuais homogêneos, uma vez que a instituição financeira **RÉ SERASA** acessa inúmeros dados de consumidores para oferecimento de serviços e produtos.

Diante disso, além de restarem demonstrados as finalidades institucionais do **AUTOR**, bem como a pertinência do objeto da presente ação, resta configurado o requisito da sua legitimidade.

2 – DOS FATOS

O AUTOR SIGILO, na condição de associação sem fins lucrativos, que trabalha em defesa da proteção de dados pessoais dos **TITULARES DE DADOS**, teve notícia, que, em **janeiro de 2021**, houve um gigante vazamento de dados atribuídos à **RÉ SERASA**.

Tal fato foi noticiado por inúmeras reportagens e publicações, o que engloba, mas não se limita, a seguinte matéria do portal **TECNOBLOG** relatando que a **SERASA** permitiu o acesso indevido a dados pessoais dos **TITULARES DE DADOS**, fora das finalidades que se propõe a realizar, no que obtiveram as informações de endereço residencial dos usuários, dados de compra, CPF, cartão de crédito, dentre outras.

tecnoblog

Início » Antivírus e Segurança » Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava

Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava

Vazamento inclui CPF, foto de rosto, endereço, telefone, e-mail, score de crédito, salário e mais; Serasa nega ser fonte dos dados

Por Felipe Ventura
22/01/2021 às 14:10

Esta semana, surgiu a notícia de um **vazamento** enorme que expôs o CPF de mais de 220 milhões de brasileiros. O **Tecnoblog** descobriu que o caso é mais grave: esse conjunto de dados pessoais, oferecido de graça em um fórum de internet, está associado a uma base ainda maior que inclui foto de rosto, endereço, telefone, e-mail, score de crédito, salário, renda e muito mais. O arquivo parece estar associado à Serasa Experian, mas a empresa nega ser a fonte.

Além disso, na citada reportagem[1], a própria **SERASA EXPERIAN S/A** admite a existência e extensão do problema:

> **O arquivo de 14 GB possui dados de 223,74 milhões de CPFs distintos, e aparentemente foi compilado em agosto de 2019. Ele está disponível na internet aberta, não na dark web: o link até foi indexado pela busca do Google. O número de pessoas afetadas é maior do que a população brasileira porque a base de dados também inclui falecidos.** [com nossos destaques de estilo].

[1] VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. **Tecnoblog**. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/amp/. Acesso em 8 fev. 2021.

No entanto, apesar de toda uma gama de indícios que apontam para a base de dados mantida pela empresa, a SERASA não admitiu que a falha tenha sido por ela ocasionada[2], tampouco entrou em contato com os **TITULARES** sobre como foram acessados os seus dados, quais dados foram levados, quais os mecanismos de segurança aplicados e quais as medidas de mitigação de riscos foram aplicadas, insistindo de que não há falha de segurança advinda de sua base de dados[3].

Como se vê, Exa., praticamente todos os dados dos **TITULARES** brasileiros, vivos e mortos, foram expostos no incidente mencionado, o que poderá ocasionar em inúmeras fraudes praticadas por terceiros mal-intencionados que detenham essas informações.

Contudo, conforme noticiado, foi possível explorar diversos dados pessoais dos Contudo Exa., conforme noticiado, foi possível explorar diversos dados pessoais dos **TITULARES**, além de outra **vulnerabilidade** que permitiria a terceiros o acesso a informações detalhadas sobre cartões utilizados pelos usuários como forma de pagamento, bem como prints de salários, entre outros dados que causem exposição danosa.

Como advertiu o advogado Omar KAMINSKI, um dos mais respeitados especialistas sobre o tema no Brasil, se referiu ao evento como catastrófico:

---

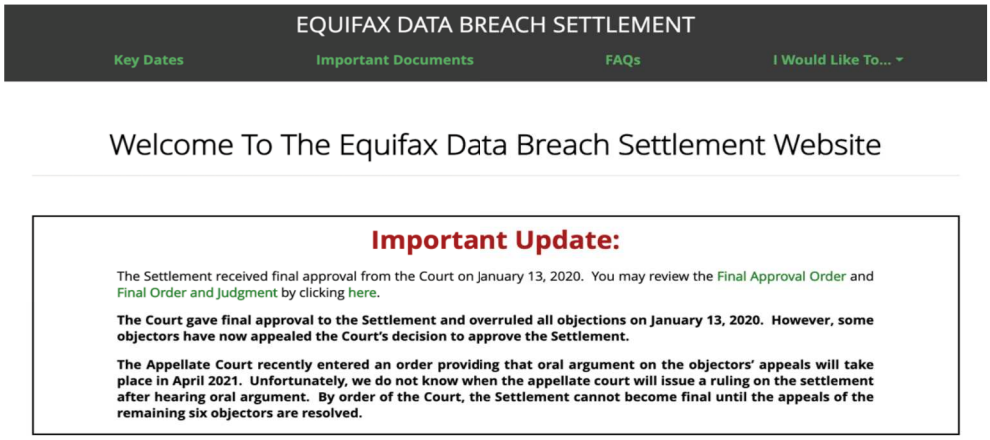
2 A reportagem do TECNOBLOG trouxe a posição do SERASA: “Em comunicado ao Tecnoblog, a Serasa Experian diz: ‘estamos cientes de alegações de terceiros sobre dados disponibilizados na dark web; conduzimos uma investigação e neste momento não vemos nada que indique que a Serasa seja a fonte’”. Conforme URL acima referido.

3 Nota do Serasa acerca do vazamento presente em reportagem da CNN Brasil: “Fizemos uma investigação aprofundada que indica que não há correspondência entre os campos das pastas disponíveis na web com os campos de nossos sistemas onde o Score Serasa é carregado, nem com o Mosaic. Além disso, os dados que vimos incluem elementos que nem mesmo temos em nossos sistemas e os dados que alegam ser atribuídos à Serasa não correspondem aos dados em nossos arquivos”.

> **Não se pode mais tolerar esse tipo de ocorrência como se fosse normal ou aceitável. Não é, nem pode ser. Se a desculpa era a ausência de uma lei específica, *habemus legem*.**[4] [Destacamos].

Com razão, KAMINSKI compara o vazamento ocorrido no Brasil ao que aconteceu nos Estados Unidos em 2017, quando os dados da empresa de gestão de crédito **Equifax**, portanto, com atuação análoga à SERASA, foram vazados e comprometeram a privacidade de 147 milhões de consumidores, entre EUA, Canadá e Reino Unido.

Em 2019, a empresa celebrou um acordo com a Comissão Federal de Comércio (FTC), autoridade de defesa dos consumidores, e com os Estados, para o pagamento de cerca de 700 milhões de dólares (R$ 3,7 bilhões) e a responsabilidade da própria empresa montar uma central de atendimento para os lesados, pelo período de 4 (quatro) anos.[5]



Fonte: https://www.equifaxbreachsettlement.com/

[4] SANTOS, Rafa. **Vazamento de dados é grave e seu impacto será sentido por anos, dizem especialistas**. Consultor Jurídico. São Paulo, 1 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-01/vazamento-dados-grave-impacto-sentido-anos. Acesso em: 8 fev. 2021.

Assim, é evidente a **falha de segurança da informação** nos servidores utilizados pela **RÉ** para armazenar e processar, tanto os dados de seus usuários como de suas transações realizadas, o que poderá ocasionar em inúmeras fraudes por terceiros mal intencionados que tiverem acesso indevido a tais dados, especialmente para práticas maliciosas como "roubo de identidade" e as fraudes mais diversas.

Destaca-se ainda que, embora a **RÉ SERASA** aparentemente terceirize seus serviços de hospedagem e armazenamento, é sua responsabilidade fiscalizar a regular prestação do serviço de forma a evitar que ocorram incidentes como os aqui demonstrados, já que de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 ou "LGPD") a Serasa tem responsabilidade solidária com seus agentes de tratamento de dados pessoais parceiros[6].

Mesmo a **SERASA** negando veementemente o não vazamento de sua base, o arquivo exposto possui essa configuração, tal como apontam as matérias jornalísticas e relatórios de consultoria que seguem em anexo, sendo tal o vínculo entre as bases vazadas e a empresa RÉ uma menção obrigatória nas fontes das reportagens, com destaque para a empresa líder de proteção de dados e segurança digital que primeiro reportou o incidente - a PSafe[7], além de sites especializados, como CISO Advisor[8] e Security Report[9].

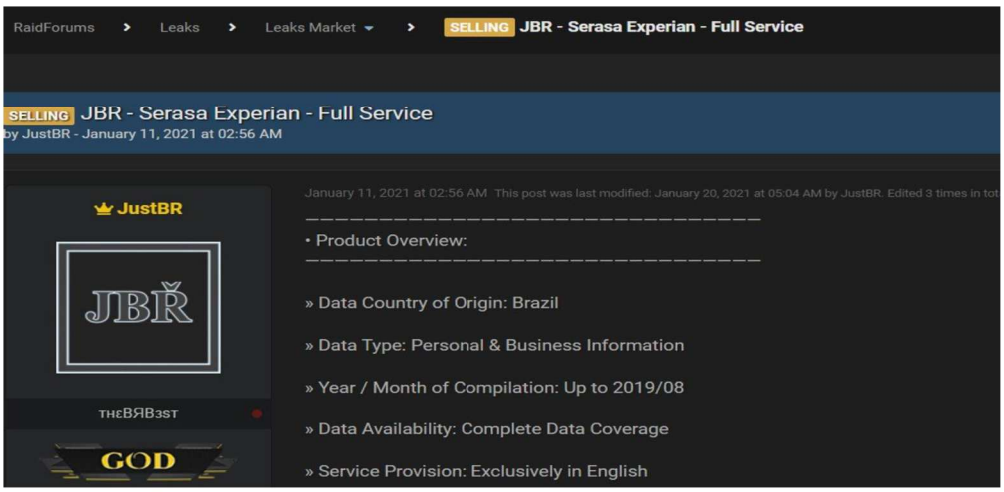
---

[6] Art. 42, § 1º, incisos I e II da LGPD.
[7] Conforme noticiado amplamente, foi o "dfndr lab", laboratório de pesquisa de segurança da PSafe (https://www.psafe.com) que identificou o vazamento no dia 20.01.2021. Cf. ARBULU, Rafael. Disponível em: Vazamento de banco de dados expõe CPF de quase toda a população do Brasil. **Olhar Digital.** Disponível em: https://olhardigital.com.br/2021/01/20/seguranca/vazamento-de-banco-de-dados-expoe-cpf-de-quase-toda-a-populacao-do-brasil/.
[8] https://www.cisoadvisor.com.br/.
[9] https://www.securityreport.com.br/.

Tem-se que o mais representativo acervo de dados é intitulado 'Serasa Experian', e existem alguns indícios de que estes dados podem estar relacionados à empresa:

- uma das bases traz dados do **Mosaic, serviço da Serasa Experian que classifica os consumidores em 11 grupos e 40 segmentos, a fim de fazer anúncios segmentados e prospecção de clientes**;
- **outras duas bases possuem informações sobre modelos de afinidade e propensão, algo que também é oferecido pela Serasa, a chance de que uma pessoa tem de comprar determinado produto ou serviço como seguro, previdência privada, cartão de crédito, jogos, viagens, artigos de luxo, entre outros**;
- há ainda uma lista de **scores de crédito, produto pelo qual a Serasa é mais conhecida**.

De fato, é possível perceber num "print screen" obtido pela PSafe que "**o arquivo principal é intitulado SERASA EXPERIAN**", conforme matéria da Época:



Fonte: **Revista Época.** Disponível em: https://epoca.globo.com/brasil/hacker-rouba-dados-de-223-milhoes-de-brasileiros-vende-na-dark-web-24851406. Acesso em 8 fev. 2021.

Na mesma matéria (em anexo), consta, ainda, a seguinte informação:

> De acordo com a PSafe, **o hacker alegou ter copiado os dados de um bureau de crédito.** Em um fórum na internet, há um banco de dados de brasileiros que foi colocado à venda em 11 de janeiro. **Conforme a descrição no site, as informações comercializadas teriam sido roubadas da Serasa Experian.** A empresa nega. [Destacamos].

Em face disto, Exa., o **AUTOR SIGILO**, que luta contra a **banalização dos vazamentos de dados** dos **TITULARES**, que a **RÉ SERASA**, bem como outras empresas de cadastros positivos e negativos, permitem o acesso indevido a dados de seus associados e de toda a sociedade brasileira, sem a possibilidade efetiva de intervenção e questionamentos, vê-se impelido a buscar a **total transparência** sobre os fatos e eventos incontestes aqui narrados e perguntar:

a) Quais dados mantidos pela **RÉ SERASA EXPERIAN** foram vazados?;

b) Quais as medidas de segurança da informação foram aplicadas antes e depois do incidente?;

c) Quais as medidas técnicas apresentadas para a mitigação dos riscos?;

d) Os dados foram recuperados? Existem riscos para os **TITULARES**?;

e) O(s) responsáveis pelo incidente obtiveram acesso aos cartões de débito e de crédito dos **TITULARES**?;

f) Os **TITULARES** foram comunicados? Existe comprovante da comunicação?

Contudo, **até o presente momento**, os **RÉUS**, em seus *sites* ou através da imprensa, não divulgaram o tamanho, a extensão e a gravidade do vazamento em questão. Muito menos apresentaram as **medidas de segurança** aplicadas para conter o incidente.

A nota de esclarecimento na reportagem, que desmente as argumentações apresentadas, é vaga e imprecisa, o que indica **falta de transparência** e contradição com as políticas da ré **SERASA**. Também não provou que comunicou a todos os **TITULARES** sobre essas questões, as quais está obrigada por lei, vide LGPD e Marco Civil da Internet (Lei n. 12.965/2014 ou "MCI") a comunicar.

Ultimamente, Exa., os **TITULARES** possuem um sentimento de total **despertencimento** dos seus dados pessoais. Eles são utilizados por estas empresas para maximizarem seus lucros com estes dados sem terem de prestar informações algumas ou disponibilizar quaisquer canais à disposição para retificar, corrigir ou modificá-las.

Diante disso, em que pese a empresa responsável pelos serviços de armazenamento dos dados dos usuários e processamento das transações por eles realizados, é evidente a omissão da **SERASA** perante o seu dever de fiscalizar, exigir e apontar eventuais falhas de segurança existentes nos serviços prestados.

Por outro lado, Exa., deve-se destacar a omissão irresponsável, até o presente momento, da ré **UNIÃO**, conquanto possui um órgão especializado dentro da administração pública direta federal - a recém criada **ANPD**, integrante da Presidência da República e que possui atribuições relacionadas à proteção de dados pessoais e da privacidade e, sobretudo, o dever de realizar a fiscalização do cumprimento da LGPD.

Nesse sentido, a **UNIÃO,** omitindo-se do seu dever legal, vem apresentando atuação irrelevante e completamente alheia a esse gigante vazamento, o que é ilegal e coloca os **TITULARES DE DADOS** em situação de **hipervulnerabilidade**. Em que pese se intitular AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, até o que se viu é que se trata de entidade puramente decorativa, sem qualquer relevância prática.

Portanto, é nítida a sua posição como conivente pelo incidente de segurança noticiado, conquanto seu silêncio eloquente faz crer que nada se poderia fazer em relação a um evento catastrófico.

Até onde pôde ser constatado, tanto a **SERASA EXPERIAN** quanto a **ANPD** não demonstraram, inequivocamente, terem realizado todos os esforços razoáveis para evitar a ocorrência do evento, bem como mitigar os efeitos nefastos que poderão ser sentidos por um longo período, pela população inteira de um país e, ainda, as organizações também afetadas.

Demais disso, a inexistência de um plano de contingência e medidas consistentes para minimizar todo o potencial lesivo desse incidente, a ausência de transparência sobre esses procedimentos e, sobretudo, a falta de qualquer pronunciamento da administração pública direita federal, por seu órgão especializado - "**Autoridade Nacional de Proteção de Dados**", reclama a adoção de provimento judicial urgente, no sentido de fazer cumprir a legislação sob ataque.

Em relação à referida Autoridade, é bem verdade que emitiu uma nota, em que se limitou apenas a afirmar que está realizando uma apuração técnica:

> A ANPD está apurando tecnicamente informações sobre o caso e atuará de maneira cooperativa com os órgãos de investigação competentes para **apurar a origem; a forma em que se deu o possível vazamento; as medidas de contenção e de mitigação adotadas em um plano de contingência; as possíveis consequências e os danos causados pela violação**. Concluída esta etapa, a ANPD sugerirá as medidas cabíveis, previstas na Lei Geral de Proteção de Dados (LGPD), para promover, com os demais órgãos competentes, **a responsabilização e a punição dos envolvidos.** [com nossos destaques de estilo].

No entanto, o simplório e inócuo comunicado só foi divulgado após toda a imprensa nacional e diversos especialistas alertarem para a monumental extensão do vazamento, destacando-se aí que diversas autoridades nacionais foram vítimas do incidente, dentre as quais todos os ministros do Supremo Tribunal Federal, e os chefes dos demais poderes, incluindo o Presidente da República, como noticiou o Consultor Jurídico, do dia 02.02.2021[10]:

> **Os dados dos 11 ministros do Supremo Tribunal Federal estão à venda na internet, após o megavazamento de dados de 223 milhões de CPFs, além de dados cadastrais e informações econômicas, fiscais, previdenciárias, perfis em redes sociais, escore de crédito e fotografia pessoal.**
>
> A empresa de segurança Shyhunt analisou, a pedido do Estadão, alguns dos arquivos disponibilizados por criminosos na internet, mas não foi possível identificar a identidade ou o número de pessoas envolvidas no vazamento. **O arquivo analisado é considerado um "catálogo" das informações em poder do hacker — assim, não é possível saber se ele de fato tem essas informações, apenas que anunciou que elas estão à venda**.

[10] CONSULTOR JURÍDICO. **Vazamento do fim do mundo: após megavazamento, dados de ministros do Supremo são postos à venda**. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2021-fev-02/megavazamento-dados-ministros-stf-sao-postos-venda. Acesso em 8 fev. 2021.

> **O hacker está oferecendo informações em 37 categorias**: básico simples, básico completo, e-mail, telefone, endereço, **Mosaic (um serviço oferecido pelo Serasa),** ocupação, **score de crédito**, registro geral, título de eleitor, escolaridade, empresarial, Receita Federal, classe social, estado civil, emprego, afinidade, modelo analítico, poder aquisitivo, fotos de rostos, servidores públicos, cheques sem fundos, devedores, Bolsa Família, universitários, conselhos, domicílios, vínculos, LinkedIn, salário, renda, óbitos, IRPF, INSS, FGTS, CNS, NIS e PIS. Segundo o catálogo, a maioria das informações são referentes ao ano de 2019, mas há bases de 2017, 2018 e 2020 no pacote. A categoria 'fotos de rostos' também inclui arquivos entre 2012 e 2020.", detalha a reportagem do *Estadão*. (...) **Os hackers ainda estão oferecendo dados do presidente da República, Jair Bolsonaro; do agora ex-presidente da Câmara dos Deputados, Rodrigo Maia; e do ex-presidente do Senado, Davi Alcolumbre**. [Destaques nossos]

Como se verá a seguir, inúmeras outras matérias e opiniões de especialistas apontam para o imenso prejuízo que esse único evento pode causar para toda a população, sendo que cada cidadão brasileiro afetado pelo vazamento, enquanto titular de dados pessoais, será atormentado por anos com os efeitos nefastos que agora se expõe.

Com a realização de auditorias necessárias, pelas autoridades competentes, incluindo-se, em especial a **ANPD**, conquanto ente responsável, em nome da segundada demandada (UNIÃO), para zelar pelo cumprimento da LGPD, restará devidamente comprovada a responsabilidade da primeira demandada no episódio.

Portanto, a omissão e a falta de responsabilização de entidades diretamente ligadas com a provável origem deste evento, demanda imediata resposta por parte do Poder Judiciário nacional, como forma de mitigar os efeitos nefastos que provavelmente os titulares de dados enfrentarão ao longo dos próximos anos.

3 – FUNDAMENTOS JURÍDICOS

Com efeito, a discussão acerca da proteção dos dados pessoais dos usuários da internet não é recente, ainda que no âmbito nacional tenha-se iniciado mais tardiamente em relação a outros países.

Embora nos últimos anos a discussão sobre o tema tenha se tornado central no meio jurídico, principalmente após a promulgação do Regulamento Geral de Proteção de Dados da União Europeia (a denominada "GDPR")[11], a legislação nacional já dispunha de mecanismos legais, ainda que não totalmente eficazes, que traziam princípios e regras a serem adotadas de forma a garantir níveis de proteção adequadas aos titulares dos dados, bem como responsabilizassem agentes em razão de incidentes que comprometessem os dados dos **TITULARES**.

3.1. O QUE ESTÁ EM JOGO: ESTADO-DA-ARTE EM MATÉRIA DE MEDIAÇÃO JUDICIAL POR VIOLAÇÕES DE DADOS PESSOAIS COMO O CASO VERTENTE

Excelência, diante dos fatos concretos e inquestionáveis, os titulares de dados, neste ato representado pelo AUTOR, têm à sua frente uma batalha homérica em face da **SERASA EXPERIAN**, que é uma empresa multinacional, usufruindo dos

[11] Trata-se do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que revogou a Diretiva 95/1946 e entrou em vigor na data suprarreferida. O título do documento em inglês corresponde à sigla GDPR (*General Data Protection Regulation*), mais popular no campo de estudos do fenômeno proteção de dados.

dados pessoais de milhões de brasileiros sem quaisquer objeções ou confrontações.

A **SIGILO**, em nome não só de seus associados, mas da sociedade brasileira, visa defender a proteção legal e constitucional dos direitos de cada um dos titulares de dados, sobremaneira na tentativa de evitar a continuidade do descalabro que, ao fim e ao cabo, se articula diretamente com o *core business* da empresa demanda, que lucra somas bilionárias com práticas nem sempre louváveis.

Além de dados pessoais constantes em fichas de cadastro, hábitos de consumo, linhas de crédito e o micro-comportamento dos usuários são os dados que as empresas buscam desenfreadamente para entender a jornada de consumo dos seus potenciais consumidores em um cruzamento de informações que já têm em sua própria base, construída a partir dos dados coletados de seus consumidores.

Yuval HARARI, em *Homo Deus,* fala na ascensão de uma nova religião ou de uma nova divindade, para a qual entregamos nossas vidas – o "*dataísmo",* a crença absoluta na direção da sociedade a partir de dados.[12]

Na mesma senda, a advertência de Shoshana ZUBOFF, aclamada pesquisadora da Universidade de Harvard, de que a sociedade se encontra "aprisionada" no que denominou de *capitalismo de vigilância* ("*surveillance capitalismo"*), segundo o qual o fenômeno de grandes acervos informacionais ("*Big Data"*) não é simplesmente uma ferramenta tecnológica ou uma metodologia, mas

[12] HARARI, Yuval Noah. **Homo Deus: uma breve história do amanhã**. Trad. Paulo Geiger. Rio de Janeiro: Companhia das Letras, 2016, p. 321-322.

uma ditadura comportamental imposta pelas grandes corporações[13] - as mesmas que adquirem as informações de grandes bancos de dados sob o pretexto de tratamento legítimo para fins de "proteção de crédito".

Na conjunção do art. 5º, incisos X e XII, da Constituição da República, verifica-se que os negócios da **RÉ SERASA** e a reiterada inobservância do presumível dever de cuidado com os **TITULARES**, em todos os seus âmbitos, **ferem** a **inviolabilidade de dados**, a **privacidade**, a **intimidade**, a **vida privada** deles, colocando em risco a sociedade brasileira.

Assim como ocorreu com o Caso EQUIFAX, é possível reconhecer que a responsabilidade da SERASA decorre do fato da empresa ter se omitido de tomar todas as medidas razoáveis necessárias para prevenir atividades que pudessem resultar na violação da legislação que ora se evidencia.

Tratando-se de um fenômeno recente, a hiperconectividade digital tem gerado infinitos benefícios a todo e qualquer cidadão que passa a se utilizar da "infovia" ou da "tecnoesfera". O fato, sem a intenção de estender demasiado questões socioeconômicas de fundo, vivemos a era da expansão global das TICS e do Big Data, na qual dados passam a ser o novo petróleo. O reverso disso são os riscos cibernéticos e ameaças crescentes como os incidentes de segurança específicos que comprometem a privacidade e os dados pessoais, como o caso vertente.

---

[13] ZUBOFF, Shoshana. **Big other: surveillance capitalism and the prospects of an information civilization.** Journal of Information Technology, Cambridge, n. 30, p. 75-89, 2015.

Diante desse cenário, novas leis de privacidade em vigor ao redor do mundo atribuem a empresas e às autoridades de supervisão, como a recente *California Consumer Privacy Act,* aprovada em 2020. Mas mesmo quando inexistem tais leis ou órgãos de fiscalização específicos, é cada vez mais frequente o reconhecimento de que empresas e governos possuir o princípio denominado "*reasonable duty of care",* literalmente, o razoável **dever de cuidado**, com base em estruturas legais existentes, como regras basilares de responsabilidade civil e leis de defesa do consumidor.

Cada vez mais, os consumidores também fizeram algumas incursões significativas em ações por negligência contra empresas que passaram por eventos cibernéticos. Em 28 de janeiro de 2019, a Corte do Distrito Norte da Geórgia (EUA) emitiu uma decisão na ***Ação Coletiva da Equifax (Consolidated Consumer Class Action)***, permitindo que as reivindicações das vítimas da Equifax fossem atendidas.[14]

O Tribunal rejeitou os argumentos da empresa - que, diga-se de passagem, desenvolve atividade empresarial análoga à da **SERASA EXPERIAN**, de que os danos experimentados pelos titulares de dados deveriam ser atribuídos aos hackers e poderiam ter sido causados por violações de dados em outras empresas.

No entanto, a Corte Distrital observou que **permitir que as empresas "confiem em outras violações de dados para derrotar uma conexão causal" criaria um incentivo perverso para as empresas: desde que ocorram violações**

[14] GESSER, Avi; e ROBLES, David. The Rise of Cyber Negligence Claims: Plaintiffs Find Receptive Judges by Going Back to Basics. **NYU Law's Program on Corporate Compliance and Enforcement**. Disponível em: https://wp.nyu.edu/compliance_enforcement/2019/03/06/the-rise-of-cyber-negligence-claims-plaintiffs-find-receptive-judges-by-going-back-to-basics/. Acesso em: 8 fev. 2021.

de dados suficientes, empresas individuais nunca seriam consideradas responsáveis.

O Tribunal concluiu que, devido ao risco previsível de violação de dados, a Equifax devia aos consumidores o dever legal independente de tomar medidas razoáveis para proteger suas informações pessoais sob a custódia da Equifax. Ao fazê-lo, o Tribunal concluiu que a doutrina da necessária **perda econômica** não era um obstáculo à reparação dos consumidores porque a Equifax tinha um dever independente de salvaguardar informações pessoais.

Ao concluir que a Equifax tinha um dever independente de cuidado que existe no contexto de violações de dados, a Corte tornou as reivindicações de negligência uma opção mais viável para os reclamantes de violação de dados. Essa mudança de interpretação culminou com o histórico acordo celebrado com a Federal Trade Comission dos EUA e outros estados.[15]

Da mesma forma, em novembro de 2018, a Suprema Corte da Pensilvânia decidiu no processo DITTMAN V. UPMC que um empregador tem o dever de direito comum de usar o cuidado razoável para proteger as informações pessoais dos funcionários. O Tribunal considerou que a doutrina de perda econômica da Pensilvânia permite a reparação de "danos puramente pecuniários" em reivindicações de negligência por violação de dados, desde que o demandante

[15] EXAME ONLINE, 22 jul. 2021. Disponível em: https://exame.com/negocios/equifax-pagara-ate-us-700-milhoes-por-vazamento-de-dados-pessoais/.

possa estabelecer a violação do réu de um dever legal decorrente da lei comum que é independente de qualquer dever assumido nos termos do contrato.[16]

Esse caso envolveu a violação da rede do Centro Médico da Universidade de Pittsburgh, que resultou no roubo de informações de milhares de funcionários, incluindo números do Seguro Social, datas de nascimento, informações fiscais e dados de contas bancárias.

Ao longo das últimas semanas, pode-se perceber que a empresa não demonstrou qualquer empenho para atender ao primado do razoável dever de cuidado, conquanto as hipóteses autorizativas de tratamento de dados pessoais não são uma cláusula aberta para que a vida das pessoas sejam devassadas, com o comprometimento, inclusive de dados sensíveis, incluindo-se aí os de crianças e adolescentes.

Deixar a ré **SERASA EXPERIAN** impune seria o mesmo que conceder status de permissivo legal para as más práticas verificadas nas rotinas da empresa, sobremaneira com implicações ilícitas. Por outro lado, impor sanções cíveis como ora pretendido, com base na legislação em pleno vigor no Brasil, é medida que se impõe e que representa nítida evolução em relação ao atual estágio civilizatório da sociedade algorítmica.

É preciso ter em mente o que está em jogo: valores fundamentais do constitucionalismo tais como a privacidade, a liberdade de expressão, a isonomia e princípio democrático, apenas para ficar em alguns. E o próprio direito à proteção de dados pessoais passa, nessa quadra, a ostentar status constitucional, na medida

[16] SUPREME COURT OF PENNSYLVANIA. [J-20-2018]. Disponível em: https://cases.justia.com/pennsylvania/supreme-court/2018-43-wap-2017.pdf?ts=1542811231.

em que o STF passou a enuncia-lo sob a égide do princípio do *direito à autodeterminação informativa*, na trilha do clássico conceito erigido pela Corte Constitucional, na *Sentença da Lei do Censo* (BVerfGE 65, 1, *"Volkszählung"*). [17]

Referido princípio só restou cristalizado em nosso território após a primeira grande controvérsia envolvendo a LGPD, em meio à pandemia da Covid-19, por ocasião do julgamento pelo STF da Medida Cautelar na Ação Direta de Inconstitucionalidade 6387.[18]

Trata-se de decisão em que o Plenário do STF referendou medida liminar anteriormente concedia pela Min. Rosa Weber em face de pedido do Conselho Federal da Ordem dos Advogados do Brasil para sustar os efeitos da Medida Provisória 954, de 2020, que concedia ao Poder Executivo, por intermédio da Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), autarquia federal, o direito de obter de todas as operadoras de telefonia móvel e fixa "relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas". Cumpre destacar que, paralelamente, à ADI proposta pela OAB Nacional, diversos partidos políticos também se socorreram do STF para igual propósito.

---

[17] RUARO, Regina Linden; e RODRIGUEZ, Daniel Piñeiro. Nada a esconder? O direito à proteção de dados frente a medidas de segurança pública e intervenção estatal. **Portal de e-Governo, Inclusão Digital e sociedade do conhecimento.** Disponível em: http://www.egov.ufsc.br/portal/conteudo/nada-esconder-o-direito-à-proteção-de-dados-frente-medidas-de-segurança-pública-e-intervenç. Para uma análise detalhada do caso, cf. MARTINS, Leonardo. (org.) **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244.

[18] STF, ADI 6387 MC-REF / DF, Relatora: Min. Rosa Weber, 7 mai, 2020.

No voto conjunto das ADIs 6.389, 6.390, 6.393, 6.388 e 6.387, para fins de referendo na medida cautelar na ADI 6.387/DF, o Min. Gilmar Mendes (STF) plasmou a explícita enunciação do *direito à autodeterminação informativa* como núcleo jusfundamental do "***direito à proteção de dados***", consoante exprime em sua ampla fundamentação:

> (...) a discussão travada nesta ADI testa as possibilidades e os limites da **proteção constitucional do direito à privacidade** (art. 5o, inciso X) frente aos riscos desencadeados pelo constante avanço tecnológico que caracteriza a nossa sociedade da informação. (...) **O direito fundamental à proteção de dados pessoais** nos contornos aqui assinalados não assume natureza absoluta, mas, como qualquer outro direito fundamental, admite flexibilizações, traduzidas na possibilidade concreta de uso e tratamento desses dados para a realização de finalidades de interesse público legitimamente protegidas pelo ordenamento jurídico. No caso em tela, contudo, fazendo incidir os parâmetros de tutela do **direito à autodeterminação informacional**, verifica-se que a Medida Provisória 954/2020 é altamente deficitária na fixação de salvaguardas mínimas para a garantia da privacidade dos usuários de serviços de telefonia no Brasil. (...) Como destacado acima, a doutrina e a própria legislação aplicável impõem que a **autodeterminação** só possa ser afastada por um dever de justificação minudente e exaustivo das finalidades atribuídas ao tratamento de dados. No caso em tela, há uma enorme dificuldade de se extrair do texto normativo um contorno mínimo de segurança sobre a finalidade do tratamento de dados que é simplesmente referenciado com o objetivo de "produção estatística oficial".[19] [Destaquei].

[19] STF, ADI 6387 MC-REF/DF, Relatora: Min. Rosa Weber, 7 mai, 2020.

O direito à privacidade, como se percebe, ecoa como dimensão do direito à personalidade, sendo o **direito à proteção de dados pessoais**, uma dimensão à parte. Seria um reducionismo identificar a proteção de dados como espécie do gênero privacidade, portanto. Prova disso é a própria relevância que temos aos institutos associados à noção de *proteção de dados* ou *privacidade de dados*.

Assim, o objeto da presente causa não é apenas possível como está sobejamente demonstrada nas provas aqui trazidas, que **os réus foram brutalmente negligentes em relação aos direitos dos TITULARES**. Como será demonstrado a seguir, já existem precedentes jurisprudenciais que acenam para a possibilidade de responsabilização objetiva e solidária de organizações como a empresa demandada, bem como a ocorrência do dano moral *in re ipsa,* como no caso em tela.

3.2. DA RESPONSABILIDADE OBJETIVA E SOLIDÁRIA DA RÉ SERASA EXPERIAN POR TODA A CADEIA DE TRATAMENTO DE DADOS DOS TITULARES

Apenas em respeito à arte da argumentação, Excelência, ainda que as alegações da **RÉ SERASA EXPERIAN** fossem verdadeiras, vale dizer, que os dados não teriam saído de servidores ou de quaisquer estabelecimentos dela, em razão do sistema protetivo de dados que cercam todos os tratamentos pela referida empresa, dessume-se sua responsabilidade com base na tese da responsabilidade solidária em razão de sua atividade econômica.

Afinal, cabe questionar: que procedimentos foram adotados pela empresa para apresentar tal conclusão de que "não teria sido a origem do vazamento"? E se

tivesse sido confirmada como tal, quais seriam as medidas de contenção e mitigação dos danos? Não resta claro qual seria ou deveria ser a resposta ao incidente, o que descortina a fragilidade da governança da multinacional, de que seu *accountability* é praticamente inexistente e, sobretudo, que seu compliance é deficitário.

Aliás, a política específica de conformidade à Lei Geral de Proteção de Dados é evidentemente uma preocupação secundária da Empresa, que sequer indica seu Encarregado de Proteção de Dados, em flagrante violação à Lei 13.709/2018, como será exposto adiante.

Com efeito, os direitos dos **TITULARES DE DADOS** são de caráter personalíssimo, ou seja, estão diretamente conectados com a dignidade humana de cada um deles. Assim, quaisquer vazamentos ou tratamentos ilegais atingem aos **TITULARES DE DADOS** de forma única, indisponível e inalienável e, coletivamente, desfere um golpe à sociedade que se vê desprotegida pelos agentes de tratamento, no caso a **SERASA EXPERIAN**, de serviços com alto risco de segurança.

Por ser um direito personalíssimo, os **TITULARES DE DADOS** têm o direito de perseguir os seus dados em qualquer lugar e a qualquer tempo e os agentes de tratamento têm o dever de retirar da internet ou de qualquer outro lugar os dados pessoais obtidos ilegalmente de suas bases e seus tratamentos.

Com a devida vênia, Exa., a ré **SERASA**, por mais que alegue que os seus ambientes de tratamento não ocasionaram o incidente sob exame, pelo contexto dos dados vazados, é evidente que são dados obtidos de serviços que ela oferece de maneira única e indistinta.

Ou seja, mesmo que hipoteticamente as informações não tenham vazados dos seus bancos de dados, estas foram violadas de bancos de dados de parceiros com quem a **SERASA EXPERIAN** compartilha tais dados pessoais, ainda a fazendo responsável pelo acontecido de acordo com o Art. 42, § 1º, incisos I e II da LGPD.

Diante disso, a empresa Ré tem o dever objetivo de cuidar e de aplicar as melhores práticas de segurança da informação aos dados que coletou dos **TITULARES DE DADOS** com consentimento ou não, conforme o art. 46 da LGPD.

Portanto, em qualquer cenário, a ré **SERASA EXPERIAN** responde objetivamente pelos dados vazados, pois, direta ou indiretamente, concorreu para a ilegalidade e não aplicou as melhores práticas no desenvolvimento dos seus serviços, demonstrando descaso com o episódio, quando deveria realizar todos os esforços necessários para mitigar os deletérios efeitos do vazamento.

3.3. DA APLICAÇÃO DO MARCO CIVIL DA INTERNET AO PRESENTE CASO

Nesse contexto, a Lei 12.965/14 (Marco Civil da Internet) disciplinou, entre outros princípios, a proteção à privacidade, a proteção dos dados dos seus titulares, bem como a responsabilização dos agentes em caso de incidentes. Confira-se:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> (...)
> **II - proteção da privacidade;**
> **III - proteção dos dados pessoais, na forma da lei;**
> (...)
> **VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;**

Além disso, a referida legislação ainda assegurou aos seus **TITULARES** o direito à inviolabilidade da intimidade e da vida privada e o não fornecimento de seus dados à terceiros.

Tal aspecto merece transcrição, *in litteris*:

> Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> **I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;**
>
> **II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;**
>
> **III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;**
>
> (...) VI - informações claras e completas constantes dos contratos de prestação de serviços, **com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade**;
>
> **VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;**
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

Com efeito, Exa., o incidente relatado na presente demanda violou as principais garantias previstas aos **TITULARES** na legislação supramencionada, uma vez que, conforme informado, a exposição dos dados abrangia diversos dados pessoais dos **TITULARES**, bem como históricos de compras, dados da previdência, de renda, receita federal, endereços de *e-mail* e até possibilidade acesso aos dados dos cartões de crédito e de débito.

Nesse contexto, destaque-se a **quantidade exagerada de dados pessoais** obtidos pela **RÉ SERASA** dos **TITULARES**, o que implica no aumento dos riscos de exposição no caso de ocorrência de eventuais incidentes de segurança da informação, o que acabou ocorrendo.

Diante disso, é imperioso destacar o dispositivo do art. 13, § 2º do Decreto 8.771/16 (que regulamentou a Lei 12.965/2014), o qual determina que as aplicações de internet devam reter a menor quantidade de dados pessoais possíveis justamente para mitigar os riscos de exposição em eventual incidente de segurança. Confira-se:

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
> (...)
> § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, **os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais**, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos.

Nessas circunstâncias, **além da RÉ SERASA não assegurar que os dados pessoais dos seus usuários**, sob sua guarda e responsabilidade, não fossem expostos por terceiros não autorizados, ainda exigia diversos dados pessoais que, em um primeiro momento, não aparentam ser essenciais para o regular fornecimento de seus serviços.

Em razão da evidente previsibilidade quanto a ocorrência de incidentes de segurança da informação, em razão da alta informatização dos negócios, é imprescindível que as empresas sigam protocolos de segurança para mitigar riscos de seus processos, bem como proteger os dados de seus consumidores, principalmente.

Portanto, as empresas de aplicações de internet, no qual se enquadra a **RÉ SERASA EXPERIAN**, **devem reter a menor quantidade de dados pessoais possível para reduzir os riscos de exposição em caso de incidentes**, o que, aparentemente não ocorreu no presente caso.

Além disso, o Marco Civil da Internet é cristalino ao exigir que o armazenamento dos dados pessoais dos usuários de aplicações de internet deve atender a preservação da vida privada e da intimidade dos **TITULARES**.

> **Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.**

Ademais, embora a falha relatada tenha sido encontrada, o dispositivo do art. 11 da Lei n. 12.965/14 define que qualquer operação de coleta, armazenamento e guarda dos dados pessoais, desde que um desses atos ocorra em território nacional, deverá ser respeitada a legislação nacional, o que não ocorreu.

> Art. 11. **Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.**
>
> § 1º **O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.**
>
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. [Com nossos destaques].

Portanto, Vossa Excelência, como se percebe, a **SERASA EXPERIAN**, em um primeiro momento, deixou de cumprir com sua obrigação de resguardar os dados dos **TITULARES**, ao permitir que os dados desses fossem eventualmente expostos em um nítido incidente de segurança da informação.

3.4. DA VIOLAÇÃO DA PRIVACIDADE

Com efeito, a exposição dos dados pessoais dos usuários da **RÉ SERASA EXPERIAN,** em razão de um incidente de segurança da informação, implicou em evidente **violação da vida privada dos TITULARES**.

Nesse sentido, o art. 21 do Código Civil preceitua:

> Art. 21. **A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.**

Assim, resta evidente, Exa., que o vazamento de dados ocorridos nos sistemas de utilizados pela **RÉ SERASA**, bem como a ausência de medidas necessárias para o combate a tal violação, configuram sua patente responsabilidade civil em razão dos riscos que poderão sobrevier aos consumidores.

Neste sentido, cabe a lição de Maria Helena Diniz, referente ao dispositivo legal supracitado:

> **O direito à privacidade da pessoa contém interesses jurídicos, por isso seu titular pode impedir ou fazer cessar invasão em sua esfera íntima usando para sua defesa: mandado de injunção, habeas data, habeas corpus, mandado de segurança, cautelares inominadas e ação de responsabilidade civil por dano moral e patrimonial.** [grifo nosso]

Como dito, embora a **RÉ SERASA** tenha alegado que o incidente relatado tenha sido solucionado, o que deverá ser apurado, é patente **a exposição dos dados** dos **TITULARES**, uma vez que os próprios pesquisadores de segurança tiveram acesso a esses dados, sendo possível seu acesso, também, por terceiros inescrupulosos.

Como bem ressalta Walter CAPANEMA, um dos maiores pesadelos da modernidade consiste no "vazamento de dados, normalmente por falhas de segurança. São relatados, todos os dias, diversos casos, desde abrangendo dados bancários, *logins* e senhas do Netflix, redes sociais e biométricos.

O dano poderá ser potencializado com o posterior uso dos dados pessoais por criminosos, para a criação de identidades falsas, exploração de *logins* e acesso aos dados das vítimas."[20]

Já é consabido amplamente que centenas de consumidores já buscaram informações junto à RÉ **SERASA EXPERIAN** acerca do comprometimento de seus dados pessoais, sendo as mesmas desatendidas, como praxe. Assim, nos termos do Capítulo III da LGPD, o **não-atendimento dos direitos dos titulares** poderá ensejar, a princípio, a configuração de um dano moral, sendo possível, inclusive, cumulá-lo com um dano patrimonial, caso a impossibilidade de exercício do direito tenha trazido lucro cessante ou dano emergente.

[20] CAPANEMA, Walter A. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Jurídicos da Escola Paulista da Magistratura. São Paulo, a. 21, n. 53, p. 163-170, jan-mar 2020.

3.5. DA APLICAÇÃO DA LGPD: NÃO-ATENDIMENTO A DIVERSOS PRECEITOS DA LEGISLAÇÃO DE REGÊNCIA

Além de todos os problemas apresentados no incidente de segurança da informação em questão, conforme o art. 48, § 1°, da LGPD, a **RÉ SERASA** deveria ter, num breve espaço de tempo, comunicado os titulares de que cumpriu com as seguintes determinações:

> 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.**

Contudo, tal prática exigida por lei ainda não foi realizada, o que traz enormes prejuízos aos direitos dos **TITULARES**, tais como previstos em lei e na política de privacidade da **RÉ SERASA**.

Diante disso, requer o **SIGILO** que sejam esclarecidos os pontos determinados em lei e que ainda não foram cumpridos, sob pena das medidas legais e judiciais cabíveis.

Somando-se a isso, o **SIGILO**, ao tentar buscar informações no *site* da **RÉ SERASA**, verificou **o não cumprimento do art. 41 da LGPD**, que determina a indicação de um **ENCARREGADO DE PROTEÇÃO DE DADOS (EPD), conforme comprovam os documentos juntados.**

Em face dessas ilegalidades, requer o AUTOR que a **RÉ SERASA** seja condenada por suas práticas ilegais e abusivas, que ferem os direitos dos **TITULARES** e que não estão em conformidade com a LGPD.

Desse modo, o **AUTOR**, no exercício de suas atribuições institucionais, verificou, Exa., o efetivo descumprimento por parte da **RÉ SERASA dos arts. 18, 19, 41, 46, 47, 48 e 49 da LGPD**, bem como as leis do Marco Civil da Internet e do Código de Defesa do Consumidor, devendo a mesma ser condenada em todas as sanções cíveis e penais cabíveis.

3.6. DO DEVER DE INDENIZAR OS TITULARES PELOS DANOS CAUSADOS

O Poder Judiciário nacional é pacífico quanto à possibilidade de consumidores possuírem o direito à indenização em episódios que impliquem no menoscabo do direito à privacidade, como casos de vazamento de dados pessoais. Confira-se:

> RESPONSABILIDADE CIVIL Dano material Contrato de telefonia móvel Troca fraudulenta do "chip". Aplicação do Código de Defesa do Consumidor. Vazamento de informações e realização de operações espúrias decorrentes do sistema de segurança falho da ré. Fato incontroverso. Responsabilidade objetiva. Danos comprovados - Recurso da ré improvido. Recurso adesivo da autora provido.

> **RESPONSABILIDADE CIVIL Dano moral Inúmeros os transtornos decorrentes da fraude - Autora que foi envolvida numa situação a que não deu causa, tendo que resolver as pendências Indenização devida. Fixação do valor em R$ 10.000,00 (dez mil reais). Recurso da ré improvido. Recurso adesivo da autora provido.** (TJSP, Ap. Cível n. 1006791-98.2019.8.26.0196, 23ª Câm. Dir. Privado, Rel. Des. J. B. Franco de Godoi, julgado em 19.05.2020) – grifo nosso
>
> TELEFONIA - CONSUMIDORES VÍTIMAS DE ROUBO DENTRO DA PRÓPRIA RESIDÊNCIA - CRIMINOSOS QUE TIVERAM ACESSO A INFORMAÇÕES EXCLUSIVAS DA EMPRESA DE TELEFONIA - FALHA NA PRESTAÇÃO DE SERVIÇOS EVIDENCIADA - RESPONSABILIDADE OBJETIVA DA CONCESSIONÁRIA - INTELIGÊNCIA DO ARTIGO 14 DO CDC - RISCO DA ATIVIDADE - DANOS MORAIS CONFIGURADOS - QUANTUM BEM FIXADO - RECURSO IMPROVIDO. **"A prestadora de serviços assume o risco pelas fraudes perpetradas contra seus clientes, especialmente se os meliantes lograram ter acesso a informações exclusivas da empresa"**. (TJSP; Apelação Cível 1010245-20.2017.8.26.0564; Relator (a): Renato Sartorelli; Órgão Julgador: 26ª Câmara de Direito Privado; Foro de São Bernardo do Campo - 9ª Vara Cível; Data do Julgamento: 19/09/2019; Data de Registro: 19/09/2019) – grifo nosso

D. Julgador, à vista de toda a carga motivacional da pretensão de reparação aqui deduzido, relevante trazer à baila, mais uma vez, a lição de W. CAPANEMA[21]:

> A responsabilidade surge do exercício da atividade de proteção de dados que viole a "**legislação de proteção de dados**". Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Deve-se aqui fazer uma analogia com o conceito de "legislação tributária" do art. 96 do CTN, para incluir não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades. Mas a responsabilidade civil na LGPD não surge apenas da violação do microssistema jurídico de proteção de dados. É preciso interpretar o

[21] CAPANEMA, Walter A. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Jurídicos da Escola Paulista da Magistratura. São Paulo, a. 21, n. 53, p. 163-170, jan-mar 2020.

art. 42, *caput* em conjunto com o art. 44, parágrafo único, que assim dispõe:

"Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano".

O art. 46, por sua vez, estabelece que os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas visando a proteção de dados pessoais. Tais normas podem ser editadas, inclusive, pela ANPD.

Pela complexidade da atividade de segurança da informação, devem ser considera- das apenas aquelas medidas previstas em padrões devidamente reconhecidos, como as denominadas normas ISO. Dessa forma, é possível identificar duas situações de responsabilidade civil na LGPD:

a) violação de normas **jurídicas**, do microssistema de proteção de dados;

b) violação de normas **técnicas**, voltadas à segurança e proteção de dados pessoais.

E, evidentemente, só caracterizará a responsabilidade civil, se a violação de norma jurídica ou técnica ocasionar dano material ou moral a um titular ou a uma coletividade.

Por seu turno, o art. 944 do Código Civil dispõe que "A indenização mede-se pela extensão do dano". E a extensão de um dano relativo à proteção de dados poderá levar em consideração os seguintes critérios:

- a quantidade de dados pessoais afetados;
- a natureza dos dados pessoais afetados: o vazamento de dados pessoais
- sensíveis, por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos;
- a reincidência da conduta;

- a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados;
- a ausência de notificação dos usuários da ocorrência do incidente;
- a comprovada utilização dos dados pessoais vazados de titulares por terceiros.

Os precedentes são explícitos quanto à caracterização do dano moral em situações como a presente, *in litteris*:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; **(ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente.** 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. **5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são**

> **assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade.** 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. **Hipótese em que se configura o dano moral in re ipsa**. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. [Com nossos destaques].

Frise-se que não está em causa aqui o reconhecimento do dano moral *in re ipsa*, como já decidido em outras ocasiões pela mesma Corte Superior (cf. STJ, RESP 1.758.799-MG, em anexo), mas a aplicabilidade da própria legislação específica, diante da ocorrência de violação expressa aos direitos de personalidade, inserindo-se aí a privacidade e os dados pessoais em si.

Pois bem. Na primeira sentença proferida após a vigência parcial da LGPD[22], reconheceu-se o dever legal de empresa do setor da construção civil e, assim, condenou a empresa a:

> se abster de repassar ou conceder a terceiros, a título gratuito ou oneroso, **dados pessoais, financeiros ou sensíveis titularizados pelo autor**, sob pena de multa de R$ 300,00 (trezentos reais) por contato indevido; b) condenar a ré ao pagamento de **indenização a título de dano moral** no importe de R$ 10.000,00 (dez mil reais), atualizado pela tabela prática do TJSP desde a data da publicação desta sentença e acrescido de juros moratórios de 1% (um por cento) ao mês a contar da data do trânsito em julgado.

Mesmo antes da vigência da Lei de Proteção de Dados, o Judiciário nacional já estava aferrado ao bom combate das violações de direitos subjetivos relacionados à privacidade, como no aresto a seguir:

> DIREITO DO CONSUMIDOR. FALHA NA PRESTAÇÃO DE SERVIÇOS. SEGURANÇA DA INFORMAÇÃO. ANUNCIO EM SITE DE CLASSIFICADOS ONLINE. PÁGINA DE ACOMPANHANTES. DANOS MORAIS. VALOR DA INDENIZAÇÃO. 1. Na forma do art. 46 da Lei 9.099/1995, a ementa serve de acórdão. Recurso próprio, regular e tempestivo. 2. Falha na prestação de serviços. Nas relações de consumo, responde o fornecedor objetivamente por eventuais danos causados ao consumidor decorrentes de falha na prestação dos serviços, na forma do art. 14 do Código de Defesa do Consumidor. Ainda, em seu §1º, "O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar[...]". Caracteriza falha na prestação de serviços a disponibilização de anúncio em site de classificados online sem a verificação da autenticidade e identidade do anunciante, a fim de evitar possíveis fraudes, principalmente em anúncios de acompanhantes onde a pessoa que está oferecendo seus serviços não costuma divulgar seus dados pessoais como, no caso, o nome completo. 3. **Responsabilidade civil. Dano Moral. O dano causado à autora é evidente, considerando que seu nome, sobrenomes e telefones, inclusive profissional, de atividade**

[22] TJSP. Processo n. 1080233-94.2019.8.26.0100. Data do julgado: 29 de setembro de 2020.

> **completamente distinta, foram disponibilizados em site de classificados online, como anúncio de acompanhante. A autora demonstra que seus dados pessoais foram expostos e que foi atingida em seus atributos da personalidade, de modo que é cabível indenização por danos morais.** De outra parte, não resta caracterizada a culpa exclusiva de terceiro a romper o nexo causal, pois foi a inadequada prestação de serviços da ré, sem os cuidados que a especificidade requer, que permitiu a indevida veiculação de anúncio que atingiu a intimidade e a imagem da autora, de modo que resta caracterizada a sua responsabilidade pelo ilícito. **4. Valor da indenização. O valor fixado na sentença para a indenização (R$10.000,00) cumpre com adequação as funções preventivas e compensatórias da condenação.** Sentença que se confirma pelos seus próprios fundamentos. 5. Litigância de má-fé. A omissão da ré na produção de provas em seu favor não caracteriza litigância de má-fé. Antes revela o simples desinteresse na defesa, que é sancionada com as consequências decorrentes do ônus imposto pela Lei. Recurso a que se dá parcial provimento para afastar a condenação por litigância de má-fé. 6. Recurso conhecido, e provido, em parte. Custas processuais e honorários advocatícios, fixados em 10% do valor da condenação, pelo recorrente vencido. (TJDFT, Acórdão n. 971472, Relator Juiz AISTON HENRIQUE DE SOUSA, 2ª Turma, Data de Julgamento: 5/10/2016, Publicado no DJe: 13/10/2016).

Diante do exposto, Exa., o **AUTOR** vem requerer a responsabilização da **SERASA EXPERIAN** pelos transtornos causados aos **TITULARES**, bem como pelos possíveis riscos de fraude que a exposição dos dados poderá ocasionar.

Nesse sentido, requer a fixação da indenização por danos morais em favor de cada um dos **TITULARES** de dados pessoais afetados com as práticas ilícitas da **SERASA EXPERIAN**, no montante individual de R$ 15.000,00 (quinze mil reais), conforme parâmetros legais, doutrinários e jurisprudenciais acima referidos.

Requer, ainda, seja condenada a empresa **SERASA EXPERIAN** ao pagamento de indenização por danos morais em *quantum* não inferior a R$ 200.000.000,00 (duzentos milhões de reais), com fulcro no art. 6°, VI do Código de

Defesa do Consumidor, montante que deverá ser revertido ao Fundo de Defesa de Direitos Difusos, estabelecido pelo art. 13 da Lei n. 7.347/85.

3.7. DO DEVER LEGAL DA RÉ UNIÃO (ANPD)

D. Julgador, diversamente do que se poderia pensar de soslaio em relação a sua suposta autonomia funcional, **a Autoridade Nacional de Proteção de Dados (ANPD)** é órgão regulatório e criada por decreto do Poder Executivo e atrelado à Presidência da República incumbido de zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. No entanto, trata-se de um ente despersonalizado, razão pela qual atrai a legitimidade passiva da ré **UNIÃO**.

O dever legal da União decorre exatamente da previsão do art. 55-A da LGPD, introduzido após promulgação da Lei n. 13.853/2019, da estruturação da ANPD para cumprir a missão institucional projetada no novo marco protetivo dos titulares de dados.

A rigor, a legislação de regência trouxe a **Estrutura Regimental e Quadro Demonstrativo dos Cargos** aprovados mediante publicação do Decreto n. 10.474/2020, no qual constam, em seu ANEXO I, as competências inerentes à ANPD.

Tais competências, apesar de comporem um rol bastante extenso, são fundamentais para o bom desenvolvimento, andamento e funcionamento da ANPD, posto que seu funcionamento estar diretamente associado à proteção de dados pessoais.

Indubitavelmente há que se reconhecer um poder paternalístico de cuidado que deve ser observado à **ANPD** tal qual ocorre, via de regra, com os *Procons* em relação à defesa do consumidor, considerando-se a hipossuficiência dos titulares de dados em relação aos agentes de tratamento, nos termos da lei.

Sendo assim, resta cristalina a falha da ANPD na situação explicitada, falha esta baseada não em uma ação errônea, mas em uma gravíssima omissão.

A ré **UNIÃO**, a partir do momento que institui e vincula à Presidência da República um órgão que possui como atribuição fundamental a fiscalização da LGPD, não há como se conceber que essa mesma entidade se mantenha inoperante diante de uma violação sem precedentes à legislação.

Merece destacar o que dispõe o aludido Decreto 10.474/2020 acerca da competência da ANPD, como forma de explicitar o dever jurídico ora caracterizado:

> Art. 2º Compete à ANPD:
>
> (...)
>
> IV - **fiscalizar** e **aplicar sanções** na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> (...)
>
> XVI - **realizar auditorias** ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com observância ao disposto no inciso II, **sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento**, incluído o Poder Público;

Vossa Excelência, até o momento da propositura da presente ação não se viu nenhuma medida técnica relevante que correspondesse, por mais prematuro que fosse o estágio procedimental, a um plano de contigência, com a avaliação da extensão dos danos presumíveis, formas de mitigação da exposição de dados pessoais ocasionada pelo incidente e o imperioso dever de responsabilização dos agentes criminosos que concorreram para o evento.

Nesse horizonte, plenamente cabível transpor para o presente caso a noção extraída do Direito Penal para caracterizar a criminosa omissão dos envolvidos como típica inobservância ao **dever de cuidado**. Conforme o art. 55-J da LGPD, compete à **ANPD** "zelar pela proteção dos dados pessoais, nos termos da legislação". Zelar é a ação de cuidar e tomar conta da proteção de dados. Em outras palavras, a LGPD exige da **UNIÃO** uma **ação positiva** para a aplicação da lei, em que o silêncio omissivo é proibido e ilícito.

Assim como é a maciça opinião dos especialistas em segurança de dados quanto à responsabilização da SERASA EXPERIAN, também pode se dizer que é ponto pacífico que a ANPD não tem atuado minimamente para exercer o seu dever legal de fiscalização, conforme já requestado pelo CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL, por meio de Ofício (ANEXO) dirigido àquele ente supervisor, no qual destaca:

> O ocorrido submete praticamente toda a população brasileira a um cenário de grave risco pessoal e irreparável violação à privacidade e precisa ser investigado a fundo pelas autoridades competentes, em particular por essa agência (...)

Ao passo em que a **ANPD** claudica em relação à tomada de decisões que possam contemporizar a gravidade do incidente, o Procon-SP e a Secretaria Nacional do Consumidor (SENACON) já intimaram a RÉ SERASA EXPERIAN para prestar esclarecimentos, o que reforça ainda mais a patente inoperância da AUTORIDADE.

Enquanto as consequências do vazamento vão se agravando, dia após dia, conforme amplamente veiculado, o Diretor-Presidente da ANPD está mais preocupado em conceder entrevistas e evangelizar o campo simbólico de proteção:

AgênciaBrasil

Geral

Autoridade Nacional alerta para a proteção de dados

Hoje se comemora o Dia Internacional da Privacidade de Dados

Publicado em 28/01/2021 - 16:56 Por Agência Brasil - Brasília

Na data em que se celebra o Dia Internacional da Privacidade de Dados, o diretor-presidente da Autoridade Nacional de Proteção de Dados (ANPD), Waldemar Gonçalves, alerta para a conscientização da sociedade em relação ao tema. Para ele, a riqueza da atualidade é a proteção de informações pessoais e a Autoridade Nacional de Proteção de Dados tem papel essencial na defesa dos dados de brasileiros.

"No século 21, hoje, os dados são o novo petróleo. Exatamente porque a empresa viu quão preciosos esses dados [são]. Com desenvolvimento tecnológico, inteligência artificial, a coisa hoje é de uma velocidade muito rápida. Quando faço uma pesquisa na internet e olho um determinado produto, poucos segundos depois começa a surgir 'do nada' uma série de ofertas daquele produto. São empresas que comercializam essas informações e passam a ser extremamente valiosas. Esse é o nosso foco, essa proteção de dados. Até a criação da autoridade, ele não tinha a quem recorrer de forma mais pontual", disse Gonçalves em entrevista ao programa *Brasil em Pauta*, que vai ao ar às 22h no domingo (31), na **TV Brasil**.

Relacionadas

Política

Ministério cria Comitê Gestor de Proteção de Dados Pessoais

Fonte: Agência Brasil [EBC]. https://agenciabrasil.ebc.com.br/geral/noticia/2021-01/autoridade-nacional-alerta-para-protecao-de-dados. Acesso em 8 fev. 2021.

E na Agenda do mesmo Diretor-Presidente, disponibilizado na página institucional da ANPD, nunca se observa registro de compromissos oficiais, como se percebe em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/agenda-de-autoridades/agenda-do-diretor-presidente-waldemar-goncalves-ortunho-junior.

Ora, Douto Julgador, no caso Equifax acima referido, a postura adotada pela administração pública dos EUA, nos âmbitos federal e estadual, foi decisiva para que a empresa envolvida fosse devidamente responsabilizada. Mesmo diante da ausência de legislação específica em vigor (a Lei da Califórnia ainda cumpre o período de vacância) e da inexistência de órgão específico que fiscalize o cumprimento dos direitos dos titulares (como a **ANPD**).

Na recém divulgada a agenda regulatória para 2021 e 2022, a Diretoria da **ANPD assinalou que o prazo para o início do processo regulatório de direitos dos titulares de dados pessoais ficou para o segundo semestre de 2022** (!), em que pese a LGPD estar em pleno vigor e prever esses direitos, ao passo em que a PEC 17/2019, que inclui o direito fundamental à proteção de dados no art. 5º da CRFB, pende de aprovação na Câmara dos Deputados, já o tendo sido no Senado Federal[23].

A negligência da **ANPD** motiva a adoção de medidas particulares direcionadas à **UNIÃO**, no sentido de obriga-la a uma ação sistematizada e aderente à legislação de regência, com procedimentos estruturados que representem possibilidades técnicas e legais de mitigação dos riscos e dos danos

[23] https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757.

ocasionados pela ação comissiva da **SERASA**, seja por meio da referida AUTORIDADE NACIONAL ou qualquer órgão de accountability que promane os atos administrativos esperados em situações como a presente, com o efetivo exercício do regular poder polícia do Estado e o uso de mecanismos de *Direito Administrativo Sancionador*.

Portanto, são **deveres legais** da ré **UNIÃO,** para os fins buscados na presente Ação Civil Pública:

(i) a notificação da ré **SERASA EXPERIAN**, com a requisição de providências legais e tecnológicas, para que os TITULARES sejam resguardados e protegidos dos riscos existentes na violação dos seus dados;

(ii) a realização de **auditoria técnica, a ser conduzida pela ANPD,** para constatar a desastrosa falha de segurança sob exame; e

(iii) a realização de toda e qualquer medida administrativa necessária à apuração de atos ilícitos porventura cometidos pela Autoridade, com ou sem participação de agentes públicos, com fiel observância à LGPD, CDC, Lei Geral de Telecomunicações, Marco Civil da Internet, Lei Anticorrupção Empresarial, entre outras bases legais.

4 – DO PEDIDO DE TUTELA LIMINAR DE URGÊNCIA

O art. 300 do Código de Processo Civil preconiza a possibilidade de concessão de tutela de urgência quando presentes elementos que evidenciem a

probabilidade do direito e o perigo de dano ou o risco ao resultado útil do processo.

A probabilidade do direito foi demonstrada na medida em que a empresa SERASA EXPERIAN se omitiu no dever de comunicação aos titulares e às autoridades da gravidade do incidente sob análise, em que pese processar informações específicas dos titulares de dados, em categorias relacionadas ao "score" de crédito, o que concorreu diretamente - em primeira e/ou última análise, para a exposição sem precedentes de dados pessoais e a comercialização indiscriminada de informações privadas.

De igual sorte, quedou-se silente sobre as características do evento ilícito sob apuração e que tipo de respostas tem oferecido ao incidente, com o intuito de mitigar riscos e danos prováveis. Nesse particular, à vista da extensão de prejuízos que podem afetar milhões de consumidores, espera-se que a EMPRESA RÉ adote um plano de contingência que inclua mecanismos de eliminação das bases de dados que supostamente vazaram de seus servidores, aplicando-se recursos técnicos que só a **SERASA EXPERIAN** detém, em razão de ser a responsável pelo tratamento de diversas categorias informacionais presentes nos acervos vazados.

Com efeito, o perigo de dano está configurado na manutenção da circulação, com comercialização ou não, dos dados pessoais de milhões de titulares, que permanecem sujeitos a danos aos direitos à sua intimidade e privacidade, conquanto estão vulneráveis a diversas fraudes e ilícitos, como "roubo de identidade", à guisa de exemplo, redundando num risco cibernético de grande elevado potencial lesivo.

Imagine, Excelência, se os dados biométricos de um titular são apropriados por criminosos, dispostos a pagar a quantia exigida pelos detentores dessa base de dados que foi extraída da empresa RÉ, para praticarem outros ilícitos.

Por estes motivos, requer a SIGILO, forte no que dispõe o referido art. 300 do CPC, c/c art. 84, § 3º a 5º, do CDC, o deferimento de tutela de urgência para:

(i) compelir a RÉ SERASA EXPERIAN a comunicar a todos os TITULARES que tiveram os dados expostos sobre o incidente relatado por meio de cartas com aviso de recebimento (AR), sob pena de multa diária de R$ 10.000,00 (dez mil reais);

(ii) determinar que a RÉ SERASA EXPERIAN divulgue, no prazo de 48 (quarenta e oito) horas, em suas redes e mídias de comunicação, quais foram os incidentes de segurança da informação ocorridos e quais os planos para solucionar o eventuais riscos aos seus consumidores, tal como determina o art. 48 da LGPD, sob pena de multa diária no montante de R$ 10.000,00 (dez mil reais); e

(iii) obrigar a RÉ SERASA EXPERIAN a adotar medidas técnicas que importem na eliminação dos dados vazados da internet ou outra providência prática equivalente, a fim de que cessem os prejuízos aos TITULARES, sob pena de multa diária de R$ 10.000,00 (dez mil reais) em caso de descumprimento.

Por fim, requer a **SIGILO**, seja liminarmente imposto à **UNIÃO** a realização de auditoria sobre o vazamento em questão, bem como a comunicação a todos os

TITULARES sobre o vazamento ocorrido, sob pena de multa diária de R$ 10.000,00 (dez mil reais) em caso de descumprimento.

5 – DOS PEDIDOS

Diante de todo o exposto, Exa., vem o **AUTOR** requerer a este D. Juízo a citação da **RÉ SERASA EXPERIAN**, para que, ciente de tudo, abstenha-se das atitudes abusivas e paguem indenização por danos materiais e morais dentro dos valores abaixo delimitados, e em não respondendo, que se aplique a pena de confissão e de revelia, conforme o art. 344 do CPC, concedendo-se liminarmente a **TUTELA DE URGÊNCIA,** *inaudita altera pars*, dos itens "a" a "d", nos termos do art. 300, do CPC c/c art. 84, § 3º a 5º, do Código de Defesa do Consumidor para:

a) **liminarmente**, que a **RÉ SERASA EXPERIAN** comunique a todos os **TITULARES** que tiveram os dados expostos sobre o incidente relatado por meio de cartas com aviso de recebimento (AR), sob pena de multa diária de **R$ 10.000,00** (dez mil reais);

b) **liminarmente**, que seja determinada à **RÉ SERASA EXPERIAN** a divulgação, no prazo de **48 (quarenta e oito) horas**, em suas redes e mídias de comunicação, quais foram os incidentes de segurança da informação ocorridos e quais os planos para solucionar o eventuais riscos aos seus consumidores, tal como determina o **art. 48 da LGPD**, sob pena de multa diária de **R$ 10.000,00 (dez mil reais)**;

c) ainda **liminarmente**, que seja determinada à **RÉ SERASA EXPERIAN** a aplicação das medidas técnicas e tecnológicas necessárias para retirar os dados vazados da internet, a fim de que cessem os prejuízos aos **TITULARES**, sob pena de multa diária de **R$ 10.000,00 (dez mil reais)** em caso de descumprimento;

d) também em caráter liminar *inaudita altera pars*, que seja determinada à **UNIÃO** a realização de auditoria sobre o vazamento em questão, bem como a comunicação a todos os **TITULARES** sobre o vazamento ocorrido, sob pena de multa diária de **R$ 10.000,00 (dez mil reais)**, em caso de descumprimento;

e) a condenação definitiva da **RÉ SERASA EXPERIAN,** em razão de sua conduta ilícita que culminou com a exposição dos dados de milhões de consumidores, dentre os quais seus usuários, com base no que determinam **os arts. 12, incs. II e III, do Marco Civil da Internet, e arts. 42, 51 e 52 da LGPD**;

f) a condenação definitiva da **RÉ SERASA** na obrigação de fazer para que aplique medidas técnicas e tecnológicas necessárias para retirar os eventuais dados vazados da internet, a fim de que cessem os prejuízos aos **TITULARES, pelo período a ser indicado em perícia técnica a ser instaurada, a critério desse r. Juízo**;

g) a condenação definitiva da **RÉ SERASA** ao pagamento de indenização por danos morais, em razão do vazamento massivo de dados pessoais, no importe de **R$ 15.000,00 (quinze mil reais)**, para cada um dos **TITULARES**;

h) a condenação definitiva da **RÉ SERASA** ao pagamento, a título de danos morais coletivos, com fulcro no art. 6º, VI do Código de Defesa do Consumidor, em valor não inferior a **R$ 200.000.000,00 (duzentos milhões de reais)**, a ser revertido ao Fundo de Defesa de Direitos Difusos estabelecido pelo art. 13 da Lei n. 7.347/1985;

i) a intimação do Ministério Público Federal, com fulcro nos arts. 5º, §1º da Lei n. 7.347/85 e art. 92 do Código de Defesa do Consumidor;

j) a publicação de edital no órgão oficial com fulcro no art. 94 do Código de Defesa do Consumidor;

k) o regular processamento da presente demanda independentemente do recolhimento de eventuais custas processuais pelo **AUTOR**, conforme previsão expressa dos arts. 18 da Lei n. 7.347/85 e 87 do Código de Defesa do Consumidor;

l) que, ao final, sejam julgados PROCEDENTES todos os pedidos acima veiculados, com a condenação do pagamento das custas processuais, juros de multa, correção monetária e honorários advocatícios, em seu valor máximo, como medida de equidade e correção.

Protesta por todos os meios de prova em direito admitidos e que se façam necessários para o deslinde da questão, especialmente pelo depoimento pessoal do representante dos **RÉUS**, sob pena de confissão, juntada de novos documentos, oitiva de testemunhas, dentre outros necessários ao deslinde da questão.

Sob pena de nulidade, requer sejam as INTIMAÇÕES alusivas ao presente feito dirigidas EXCLUSIVAMENTE aos advogados **Gustavo Rabay Guerra**, inscrito na OAB/PB sob n. 16080-B, e **Marina Lacerda Cunha Lima**, inscrito na OAB/PB sob n. 15769, ambos com endereço profissional à R. Nevinha Cavalcanti, 398, Miramar, João Pessoa-PB. E, ainda, sejam anotados os seguintes endereços eletrônicos para recebimento de comunicações processuais: contato@rpcl.adv.br, gustavo@rpcl.adv.br e marina@rpcl.adv.br.

Por fim, em respeito ao art. 3º do Código de Processo Civil, o **SIGILO** informa que possui interesse na realização de audiência de conciliação.

Os subscritores da presente ação civil pública declaram que todas as cópias são fiéis aos originais e que poderão apresentá-los oportunamente, por solicitação deste Juízo.

Dá-se a causa o valor de R$ 200.000.000,00 (duzentos milhões de reais).

Termos em que, D. R. e A., com todos os documentos inclusos, j.

Pede deferimento.

São Paulo-SP, 11 de fevereiro de 2021.

GUSTAVO RABAY GUERRA
Advogado - OAB-PB 16080-B

MARINA CUNHA LIMA
Advogada - OAB-PB 15769

RÔMULO PALITOT BRAGA
Advogado - OAB/PB 8.635

Documento Assinado eletronicamente de acordo com os termos da Lei 11.419/2006.