FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

KLARA NINA VIEIRA DE SIQUEIRA

A APLICAÇÃO DA RESPONSABILIDADE CIVIL À LUZ DA LGPD: UM ESTUDO SOBRE O VAZAMENTO DE DADOS PESSOAIS PELO INSS

VITÓRIA
2023

KLARA NINA VIEIRA DE SIQUEIRA

A APLICAÇÃO DA RESPONSABILIDADE CIVIL À LUZ DA LGPD: UM ESTUDO SOBRE O VAZAMENTO DE DADOS PESSOAIS PELO INSS

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Direito da Faculdade de Direito de Vitória, como requisito parcial para obtenção do grau de bacharel em Direito.
Orientador: Prof. Dr. José Luís Bolzan de Morais

VITÓRIA
2023

AGRADECIMENTOS

No filme “Na Natureza Selvagem”, de Sean Penn, aprendi que “a felicidade só é real quando compartilhada”. Hoje me encontro feliz ao concluir mais uma etapa importante da minha graduação, e gostaria de dividir esse sentimento e agradecer a todos que estiveram comigo durante essa caminhada.

Agradeço à Faculdade de Direito de Vitória e aos docentes que contribuíram para o meu aprendizado. Em especial, agradeço ao meu orientador José Luís Bolzan de Morais pela paciência, dedicação e por todo conhecimento transmitido ao longo dos encontros do Grupo de Pesquisa e das orientações.

Sou grata aos meus pais, pelo amor incondicional e pelos esforços sem medidas para me ajudar a alcançar meus sonhos. Sem o apoio deles eu não conseguiria chegar até aqui.

Agradeço aos meus amigos e primos, pela amizade e companheirismo demonstrado ao longo dessa trajetória.

Sobretudo, agradeço a Deus, que me manteve firme até aqui e permitiu que eu encontrasse essas pessoas durante minha caminhada.

RESUMO

A presente pesquisa tem por objetivo adentrar o tema da proteção de dados pessoais, em especial, quando o agente tratador de dados é o próprio Poder Público, de modo a analisar como a jurisprudência aplica a responsabilidade civil em caso de tratamento inadequado de dados. Nesse sentido, o artigo é organizado em três etapas, sendo a primeira voltada a explicar a ampla geração e o tratamento de dados na era digital, bem como o valor econômico crescente e os usos possíveis dessas informações.Em um segundo momento, aborda-se a evolução legislativa no que tange à proteção de dados no Brasil, até atingir a Lei Geral de Proteção de Dados, de modo a garantir os direitos fundamentais à privacidade e à autodeterminação informativa.Nesse mesmo capítulo, discute-se a lacuna deixada pela LGPD quanto ao regime de responsabilidade civil que deve incidir sobre casos de vazamento ou tratamento ilícito de dados pessoais. Aponta-se, assim, a ausência de previsão expressa da LGPD quanto à aplicação de responsabilidade subjetiva ou objetiva. Por fim, de modo a discutir a atuação do Poder Público como agente tratador de dados, recorre-se ao exemplo do Instituto Nacional do Seguro Social (INSS), demonstrando como se dão a coleta e o tratamento de informações pela Autarquia, bem como evidenciando a existência de vazamento e comercialização de dados pessoais com terceiros, sem o consentimento dos titulares. Diante do exposto, demonstra-se como a jurisprudência atua perante os casos de vazamentos de dados pelo INSS, bem como de que modo a LGPD vem sendo aplicada, em especial quanto ao regime de responsabilidade civil.

PALAVRAS CHAVES: dados pessoais, vazamento de dados, INSS, responsabilidade civil, LGPD, jurisprudência.

ABSTRACT

The present research aims to delve into the topic of personal data protection, especially when the data controller is the State itself, in order to analyze how jurisprudence applies civil liability in cases of inadequate data processing. In this regard, the article is organized into three stages, with the first one focused on explaining the extensive generation and processing of data in the digital age, as well as the increasing economic value and potential uses of this information. In a second moment, the legislative evolution regarding data protection in Brazil is addressed, leading to the General Data Protection Law (LGPD), in order to ensure fundamental rights to privacy and informational self-determination. In this same chapter, it is discussed the gap left by the LGPD regarding the regime of civil liability that should apply to data breaches or unlawful processing of personal data. It is pointed out that the LGPD does not provide an explicit provision for the application of subjective or objective liability. Finally, in order to discuss the State's role as a data controller, the example of the National Institute of Social Security (INSS) is used, demonstrating how the collection and processing of information by the autarchy occurs, as well as highlighting the existence of data leaks and the commercialization of personal data with third parties without the consent of the data subjects. In light of the above, it is shown how jurisprudence deals with data breaches by INSS, as well as how the LGPD is being applied, especially with regard to the regime of civil liability.

KEYWORDS: personal data, data leakage, INSS, civil liability, LGPD, jurisprudence.

SUMÁRIO

1 INTRODUÇÃO 6

2 O TRATAMENTO DE DADOS PESSOAIS E OS DIREITOS FUNDAMENTAIS 8
2.1 A CONSTITUIÇÃO E O VALOR ECONÔMICO DOS BANCOS DE DADOS 10

3 A EVOLUÇÃO LEGISLATIVA EM MATÉRIA DE PROTEÇÃO DE DADOS 14
3.1 A RESPONSABILIDADE CIVIL NO CONTEXTO DE VAZAMENTO DE DADOS 16
3.2 A RESPONSABILIDADE CIVIL DO ESTADO PELO VAZAMENTO DE DADOS 19

4. O VAZAMENTO DE DADOS PESSOAIS PELO INSS 24
4.1 JULGAMENTOS DE CASOS DE VAZAMENTO DE DADOS PELO INSS 28

5. CONSIDERAÇÕES FINAIS 32

REFERÊNCIAS 35

1 INTRODUÇÃO

A criação da internet durante a Guerra Fria foi um dos grandes marcos da humanidade, tendo em vista que seu acesso e sua expansão permitiram a ampla circulação de informações, diminuindo a distância entre as pessoas.

Apesar dos benefícios proporcionados pelo universo digital, a internet também dificulta o controle quanto à geração, coleta e tratamento de dados pessoais, estando tais informações sujeitas às mais diversas finalidades.

Além disso, casos de vazamento e compartilhamento de dados pessoais, sem o consentimento dos titulares dos dados, tornaram-se cada vez mais comuns, tornando-se um obstáculo à proteção dos direitos fundamentais à intimidade e à autodeterminação informativa no contexto brasileiro.

Nesse sentido, o presente trabalho visa a abordar a questão da proteção de dados pessoais, sobretudo quando o agente tratador de dados é o próprio Poder Público, bem como, analisar o regime de responsabilidade civil adotado para aqueles que permitem a exposição indevida de tais informações.

Dessa forma, se aborda, inicialmente, como o avanço da internet possibilitou que os dados pessoais se tornassem uma verdadeira moeda de troca, dotados de valor econômico, sendo utilizados para os mais diversos fins, como a publicidade, a política, o controle de determinadas condutas, dentre diversos outros usos possíveis na sociedade digital.

Posteriormente, analisa-se a evolução legislativa no ordenamento jurídico brasileiro quanto à proteção de dados pessoais, desde o Código de Defesa do Consumidor – o primeiro diploma legal a abordar o tema de forma direta – demonstrando de que modo se atingiu o patamar de proteção atual, principalmente por meio da Lei Geral de Proteção de Dados (LGPD).

Em seguida, aborda-se o que dispõe a LGPD quanto ao tema da responsabilização civil pelo tratamento inadequado de dados pessoais, frisando a ausência de previsão

expressa quanto à existência de responsabilidade civil objetiva ou subjetiva, o que provoca uma dificuldade prática na aplicação da norma a ser suprida pelo Poder Judiciário.

O texto aborda a dicotomia do assunto em relação as empresas privadas e pessoas físicas, como também traz a discussão de como esse sistema de responsabilidade é adotado quando o Estado é o acusado de permitir essa exposição das informações.

Valendo-se do exemplo do Instituto Nacional do Seguro Social, o presente estudo demonstra como se dá a coleta e o tratamento de dados pela autarquia, bem como expõe as denúncias e alguns dos casos de vazamento e compartilhamento de dados sem o consentimento dos titulares.

Por fim, a partir de pesquisa jurisprudencial, demonstra-se como o Poder Judiciário atua quanto instado a se manifestar sobre o tema, em especial, de que forma aplica a responsabilidade civil perante a regulamentação da Lei Geral de Proteção de Dados.

2 O TRATAMENTO DE DADOS PESSOAIS E OS DIREITOS FUNDAMENTAIS

A produção e o intercâmbio de informações pessoais são intrínsecos às relações humanas. Tais dados possibilitam a identificação do indivíduo, a exemplo de nome, idade, raça, orientação sexual, religião, impressão digital, dentre tantas outras características que se enquadram no conceito de dados pessoais à luz do entendimento legal e doutrinário predominante.

Ao longo dos anos, com a evolução da sociedade, esses dados tomaram forma e importância que até então não possuíam, decorrente da era da informação e do advento do universo digital. Assim, “a computação produz dados como subproduto. Usando tecnologias digitais, ou por meio de tecnologias digitais que usam você”. (VÉLIZ, 2021, p. 55). Desse modo, é possível compreender que os dados pessoais são frutos da existência humana, e, além disso, produtos da era da tecnologia.

Perante esse cenário no qual os dados tornaram-se produtos, a humanidade passou a vivenciar paradigmas que antes não existiam, a exemplo do vazamento e do controle de informações pessoais. Nesse sentido, destaca-se a influência do tratamento de dados nas relações entre os sujeitos e destes com a estrutura econômica, inclusive internacionalmente, possibilitando negociações e interações a partir de dados disponíveis na internet (CAMPOS, A., 2022)

Portanto, percebe-se que, com o passar dos anos, os dados pessoais passaram a ser mais que mera expressão da identidade humana e tornaram-se um produto capaz de construir e moldar a opinião daqueles que consomem conteúdos presentes nas redes sociais, como *marketing* e propagandas contidas nos canais de comunicação, de modo a invadir e rechaçar o direito fundamental à privacidade.

O direito à privacidade é um direito fundamental garantido no artigo 5º, inciso X, da Constituição Federal de 1988 (BRASIL, 2023a) que “conduz à pretensão do indivíduo de não ser o foco da observação de terceiros, de não ter seus assuntos e informações pessoais e características particulares expostas a terceiros ou ao público em geral” (MENDES; BRANCO, 2020, p. 288).

À vista disso, o direito à privacidade é essencial para que cada indivíduo exerça sua liberdade na esfera privada, bem como, em matéria de dados pessoais, para que tenha suas informações protegidas em face de terceiros.

Assim, apesar de a Constituição Federal – e especialmente o direito à privacidade – ter se consolidado em momento anterior ao advento das tecnologias digitais, deve-se reconhecer sua incidência sobre as relações jurídicas firmadas virtualmente. Nesse sentido:

> A nossa Constituição não tem previsão expressa de sua aplicação no mundo virtual, todavia, há de se reconhecer a eficácia dos direitos fundamentais em relações jurídicas constituídas on line (FREIRE JÚNIOR, 2014, p. 31).

No entanto, apesar do reconhecimento do direito fundamental à privacidade, sabe-se que, em decorrência da referida evolução dos meios de comunicação, os dados pessoais passaram a ser utilizados de forma lesiva aos próprios titulares, dentre outros fatores, em virtude da ausência de uma proteção sólida a essas informações.

Para além da violação ao direito à privacidade, o tratamento e a manipulação inadequada de dados pessoais ferem o direito à livre autodeterminação informativa, o qual Sarlet (2020) considera como o fundamento legal mais direto para o direito à proteção de informações pessoais.

Esse direito, extraível do princípio da dignidade humana, diz respeito à prerrogativa do titular de dados pessoais para definir a extensão e as formas de uso conferidas a estes. Em outras palavras, preserva o controle do indivíduo sobre suas próprias informações.

Apesar do direito à livre autodeterminação informativa, fato é que, em um contexto de sociedade da informação, resta cada vez mais difícil garantir o controle dos indivíduos sobre os dados pessoais em circulação na internet. Nesse sentido:

> [...] os indivíduos têm suas vidas, cada vez mais “transparentes”, uma vez que as informações sobre eles são, constantemente, produzidas e utilizadas – tanto pelos poderes públicos quanto pelos privados. Essa dupla transparência significa, na realidade, uma relação de (in)visibilidade extremamente desigual, de modo que se conhecem cada vez menos as maneiras como os próprios dados são coletados e quais sentidos são

> atribuídos àqueles dados (MENEZES NETO; BOLZAN DE MORAIS, 2018, p. 234).

Nesse contexto, os dados pessoais se tornaram cada vez mais vulneráveis aos anseios do mercado e das instituições, sendo constantemente armazenados e processados por instituições públicas e privadas, compondo bancos de dados sem que os titulares dessas informações possuam conhecimento ou consintam com o tratamento e compartilhamento dos dados pessoais (SILVA, 2021, p. 97).

Em igual perspectiva, Machado (2014, p. 345), ao abordar a dicotomia entre privacidade e desenvolvimento tecnológico, esclarece que:

> Sabe-se que o desenvolvimento tecnológico trouxe muitos benefícios para a sociedade, como o uso da Internet, a rapidez na comunicação, a socialização das informações e outros; entretanto, as novas dimensões da coleta e do tratamento de informações pessoais provocaram um apelo à privacidade. O debate acerca da privacidade não se restringe mais ao tema clássico da defesa da esfera privada contra as invasões externas, isto porque tal discussão evoluiu qualitativamente, o que nos faz considerar que os problemas da privacidade no âmbito da infraestrutura da informação representam um dos componentes mais importantes atualmente.

Por esse contexto, bem como pelos problemas decorrentes dele, principalmente a lesão aos direitos à privacidade e à livre autodeterminação informativa, demonstra-se a urgência ao tratar do assunto sob uma perspectiva jurídica.

Isso porque, embora o aumento exponencial da geração e do tratamento de dados pessoais seja resultado inevitável à sociedade digital, é importante recordar que os direitos fundamentais não podem ser suprimidos em detrimento do avanço da tecnologia.

2.1 A CONSTITUIÇÃO E O VALOR ECONÔMICO DOS BANCOS DE DADOS

Abordar o tratamento de dados pessoais e suas implicações jurídicas demanda discutir, também, as questões que envolvem os bancos de dados, que se caracterizam como coleções organizadas de informações estruturadas dos titulares, armazenadas digitalmente por instituições públicas ou privadas. Quanto ao tema, Doneda (2011, p. 92) destaca o banco de dados como sendo:

> Um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que

> procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações.

Denuncia-se, portanto, o caráter utilitarista da coleta de dados, voltada a extrair o maior lucro ou retorno possível a partir das informações reunidas. Os dados pessoais coletados e compilados por empresas privadas e instituições públicas podem ser usados das mais inimagináveis formas. Nesse sentido:

> Utilizando mecanismos de data mining, big data e de análises preditivas, os códigos de computadores classificam dados para os mais variados propósitos: desde a criação de perfis sobre qual a melhor estratégia de marketing a ser adotada com um consumidor específico, até a análise de informações que levam um sistema a categorizar alguém como potencial terrorista (MENEZES NETO; BOLZAN DE MORAIS, 2018, p. 237).

Dessa maneira, é possível entender que os bancos de dados são constituídos a partir de informações pessoais, sensíveis ou não, selecionadas com uma finalidade específica. Em outras palavras, há uma lógica por trás da coleta de dados, com o objetivo de se obter um resultado a respeito de determinado campo de pesquisa, seja ele no consumo, na política, na economia, na segurança pública, dentre outros.

Nesse sentido, ao se abordar a coleta de dados realizada cotidianamente na sociedade moderna, Véliz (2021, p. 25) elenca que esta ocorre de maneira natural sem que o cidadão perceba que está sendo vigiado e tendo seus dados mais íntimos coletados por uma rede de pessoas interessadas em suas informações, por motivos diversos. Senão vejamos:

> Ao pegar seu telefone logo pela manhã, você está informando a grande quantidade de bisbilhoteiros - o fabricante do seu smartphone, todos aqueles aplicativos que você instalou em seu telefone e a sua empresa de telefonia móvel, bem como as agências de inteligência, caso você seja uma pessoa “interessante” - a que horas você acorda, onde você tem dormido e com quem (assumindo que a pessoa com quem você divide a cama também mantém o telefone perto dela).

Assim sendo, compreende-se que a coleta de dados pessoais ocorre de maneira cotidiana e inevitável nos dias atuais, afinal, basta utilizar um *smartphone, notebook* ou outro dispositivo eletrônico conectado à internet para que tal geração e armazenamento de dados se operem.

Ocorre que essa coleta de dados é geradora de grandes problemas, tendo em vista que o seu tratamento equivocado ou a ausência da segurança adequada, por vezes,

acaba resultando em vazamento dessas informações, seja pela atuação de hackers, pela venda, pela disponibilização, dentre outros meios.

Exemplo disso foi o ataque hacker de ampla repercussão sofrido pelo sistema do Ministério da Saúde em 2021, ocasião na qual o perito em crimes digitais Wanderson Castilho afirmou que o Brasil é um dos países do mundo com maior dificuldade em matéria de segurança no armazenamento de informações pessoais (COSTA, 2021).

Além disso, outra problemática que decorre tanto da coleta quanto do vazamento desses dados pessoais é a finalidade para a qual estes acabam sendo utilizados, uma vez que, por meio dessas informações pessoais, sensíveis ou não, consegue-se obter controle sobre determinados sujeitos.

Isso porque estes dados possibilitam que empresas e instituições públicas mapeiem características relevantes dos sujeitos, como preferências políticas, histórico de consumo e classe socioeconômica, podendo utilizar desses dados para moldar e influenciar os titulares dos dados pessoais.

Importante frisar que as possíveis consequências do rápido avanço tecnológico em relação ao direito dos usuários é tema que há muito se discute. Ruy Rosado de Aguiar, ainda nos anos 90 já destacava a necessidade de proteção de dados pessoais pelo ordenamento jurídico:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. (BRASIL, 1995)

Nessa mesma perspectiva, no ano de 2017, a revista *The Economist* publicou uma reportagem intitulada, em tradução livre, “O recurso mais valioso do mundo não é mais petróleo, e sim, dados”, a qual versava sobre a forma como as empresas de tecnologia empregam os dados de modo a torná-los uma das principais moedas do mercado (*THE WORLD’S*, 2017).

Isto é, para além da coleta e do controle dessas informações, os bancos de dados são utilizados como uma “moeda de troca” no mercado atual, ou seja, o proprietário do banco de dados o comercializa com quem se interesse em dar um fim específico às informações registradas.

A situação narrada faz parte do conceito de *Big Data*, que se define como “um conjunto de tecnologias, processos e práticas que permitem às empresas analisarem dados a que não tinham acesso e tomar decisões ou mesmo gerenciar atividades de forma muito mais eficiente” (TAURION, 2013, p. 28).

Resta claro, dessa forma, que a problemática dos bancos de dados é muito maior que aparenta ser, tendo em vista que, além de serem constituídos, muitas vezes, de forma velada e sem o consentimento do titular dos dados, ainda são utilizados como mercadoria no mundo digital, com a finalidade de moldar e influenciar o comportamento dessas pessoas, que têm seus dados tratados de forma ilícita, causando graves danos à privacidade e à autodeterminação informativa dos indivíduos.

3 A EVOLUÇÃO LEGISLATIVA EM MATÉRIA DE PROTEÇÃO DE DADOS

Elaborada em um cenário de Guerra Fria, a internet das coisas foi projetada com o intuito de promover e facilitar a comunicação entre laboratórios em caso de bombardeios. Apesar disso, em 1992, criou-se a "*World Web*", expandindo-se o acesso a tal tecnologia de maneira gradual, até atingir os patamares globais percebidos atualmente (DIZARD JUNIOR, 2000).

Conforme o acesso à internet se expandiu, a aproximação dos usuários ao conteúdo que ela proporciona permitiu que os dados e informações pessoais desses fossem coletados e tratados por quem tivesse interesse. Nesse cenário, a evolução da tecnologia e, em consequência, da sociedade digital, exigiu que o universo jurídico se adaptasse a essa realidade, haja vista o valor crescente atribuído a esses dados (GONÇALVES, A., 2019).

Por outro lado, o direito à proteção de dados pessoais teve sua gênese na Alemanha pós Segunda Guerra, marcada pela necessidade de construir hospitais e registrar as informações pessoais de feridos em larga escala, além de compartilhá-las com outros órgãos e departamentos (CAMPOS, R., 2022).

Nesse contexto, em razão da preocupação com os direitos à intimidade e à privacidade dos pacientes, surgiu a Lei de Proteção de Dados Pessoais do Estado Alemão de Hesse, em 1970 (OLIVEIRA, 2022, p. 28).

De início, a norma foi direcionada apenas à proteção de dados no âmbito da administração pública, entretanto, em 1976, a proteção se tornou matéria de lei federal, destinada tanto aos entes públicos como ao setor privado, de forma ampla.

A criação de uma lei voltada à proteção de dados pessoais acabou por repercutir e influenciar toda a Europa, a qual passou a discutir o assunto e, anos depois, adotou a Diretiva nº 95/46/CE do Parlamento Europeu, a qual deu início à *General Data Protection Regulation* (GDPR ou RGPD),que motivou outros países – como o Brasil – a criarem normas referentes ao assunto (DÖHMANN, 2020).

No Brasil, a regulamentação da privacidade e da proteção de dados, apesar da influência europeia, se deu por outros caminhos. O direito à privacidade, garantido no artigo 5º, inciso X, da Constituição Federal de 1988, ou, ainda, o *habeas data,* remédio constitucional utilizado para garantir o acesso a informações pessoais sob a posse de instituições públicas, surgiram em reação ao período de Ditadura Militar, entre 1964 e 1985, tendo em vista a expressiva supressão de direitos e a violação à proteção de dados pessoais (CAMPOS, R., 2022).

No ano de 1990, por meio dos artigos 43 e 44 do Código de Defesa do Consumidor (BRASIL, 2021), houve a primeira menção direta à proteção de dados pessoais no ordenamento jurídico brasileiro, ainda de forma incipiente. Tais dispositivos motivaram a elaboração da Lei 12.414/2011, denominada Lei do Cadastro Positivo, a qual:

> [...] foi a primeira normativa brasileira concebida a partir de conceitos e de uma sistemática comum à tradição de proteção de dados, que já estava consolidada em outros países. É possível observar a presença de conceitos como o de dados sensíveis e outros, bem como de alguns dos princípios mais importantes de proteção de dados, entre os quais os da finalidade, transparência, minimização e segurança, entre outros (DONEDA, 2020, p. 33).

Em 2014, por sua vez, foi criada a Lei nº 12.965/2014, denominada Marco Civil da Internet, com a pretensão de regulamentar os direitos e deveres dos usuários da internet no Brasil. Nesse sentido:

> O objetivo principal desse instrumento normativo é a segurança jurídica dos usuários da rede mundial de computadores, tanto os internautas comuns, quando os provedores que franqueiam o acesso às páginas digitais, os comerciantes que se utilizam da plataforma e a própria Administração Pública (PINHEIRO; BONNA, 2020, p. 372).

O referido regramento trouxe, além de princípios e direitos atinentes ao meio digital, ferramentas práticas necessárias para assegurar o respeito às normas. Todavia, apesar de sua complexidade, a Lei 12.965/2014 ainda não abordava precisamente a proteção de dados físicos ou digitais, de forma que se restringia apenas a regulamentar o uso da internet no Brasil.

Diante disso, após a promoção do RGPD europeu, foi promulgada a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (BRASIL, 2022a) – que “dispõe sobre tratamento de dados de pessoas naturais, tanto por meio físico, quanto por

meio digital, reconhecendo a finalidade da tutela desses dados/informações para a proteção de direitos” (MULHOLLAND, 2018, p. 162).

Isso ocorreu em razão da clara necessidade de criação de uma norma que, de modo geral, abordasse o tema da proteção de dados, haja vista a ocorrência de diversos casos de vazamento de informações pessoais anteriores à regulamentação (SOUZA; PADRÃO, 2019, p. 214).

Desse modo, diante do cenário existente em uma sociedade moderna, na qual os dados pessoais se tornaram espécie de moeda de troca, a criação de uma norma que regulamentasse a proteção de informações pessoais se fez, e ainda se faz, extremamente necessária.

Pelo exposto, possível verificar que o debate quanto à proteção de dados pessoais já perdura há décadas, embora as inovações tecnológicas cada vez mais aceleradas amplifiquem sua urgência. Desse modo, o ordenamento jurídico brasileiro buscou, de diversas formas, proteger o direito à privacidade de seus cidadãos.

A proteção de dados vem evoluindo constantemente, desde a primeira menção direta no Código de Defesa do Consumidor até se atingir a atual redação da LGPD, que, de modo mais abrangente, prevê não apenas os conceitos de dados pessoais – sensíveis ou não – e as formas de tratamento de dados, como também a responsabilização pela divulgação não autorizada ou pelo vazamento dessas informações.

3.1 A RESPONSABILIDADE CIVIL NO CONTEXTO DE VAZAMENTO DE DADOS

A Lei Geral de Proteção de Dados traz, em sua redação, uma sessão exclusiva para abordar a responsabilidade civil e o ressarcimento pelos danos gerados ao titular dos dados em razão do vazamento ou tratamento ilegal.

A responsabilidade civil é conceituada como “a reparação de danos injustos resultantes da violação de um dever geral de cuidado” (ROSENVALD; FARIAS;

NETTO, 2019, p. 185). Isto é, a obrigação de reparar quando um dano a outrem for causado.

O Direito Civil subdivide a responsabilidade civil em duas espécies: a responsabilidade objetiva – na qual não se analisa a culpa do agente – e a responsabilidade subjetiva – na qual a culpa determina se há responsabilidade. Nesse sentido:

> Na responsabilidade objetiva prescinde-se totalmente da prova da culpa. Ela é reconhecida, como mencionado, independentemente de culpa. Basta, assim, que haja relação de causalidade entre a ação e o dano. [...] Diz-se, pois, ser "subjetiva" a responsabilidade quando se esteia na ideia de culpa. A prova da culpa do agente passa a ser pressuposto necessário do dano indenizável. Nessa concepção, a responsabilidade do causador do dano somente se configura se agiu com dolo ou culpa (GONÇALVES, C., 2023, p. 21).

Apesar dessa diferenciação quanto às espécies de responsabilidade civil, a Lei Geral de Proteção de Dados não aborda de forma expressa qual a modalidade a ser aplicada em caso de violação de dados pessoais. Dessa forma, entende-se que cabe à interpretação jurídica sanar essas lacunas, de modo a balizar a aplicação da responsabilidade civil em matéria de proteção de dados:

> [...] a LGPD não foi extremamente feliz no desenho das normas atinentes à responsabilidade civil. Há falhas e omissões que podem e precisam ser sanadas pelo intérprete, em busca de um regime de responsabilidade civil que se afigure, a um só tempo, coerente e eficaz (SCHREIBER, 2020, p. 331).

Diante da incerteza contida no texto legal, mais precisamente nos artigos 42 a 44 da LGPD, surgem duas correntes que discutem esse assunto. A corrente que defende a responsabilidade civil objetiva em caso de tratamento irregular de dados entende que, por ser este o sistema adotado no Código de Defesa do Consumidor, será também o que rege a Lei Geral de Proteção de Dados, uma vez que o CDC é uma das maiores influências à elaboração da LGPD (GUEDES, 2019, p. 171).

Prova disso é a semelhança evidente entre os artigos 43, caput, da LGPD e 12, §3º, do Código de Defesa do Consumidor:

> Artigo 43. Os agentes de tratamento só não serão responsabilizados quando provarem: (BRASIL, 2022a)
>
> Artigo 12. [...]

> § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: (BRASIL, 2021)

Desse modo, a corrente mencionada interpreta que o artigo 43 da LGPD diz respeito a um regime de responsabilidade civil objetiva, ou seja, independentemente de culpa, ressalvadas as hipóteses dos incisos.

Entendem os precursores dessa corrente que a responsabilização civil daquele que realiza o tratamento irregular de dados pessoais, gerando dano ao titular, deve ocorrer da seguinte maneira:

> Nestes termos, as condições de imputação de responsabilidade do controlador e do operador pelos danos decorrentes do tratamento indevido dos dados serão: a) a identificação de uma violação às normas que disciplinam o tratamento de dados pessoais; e b) a existência de um dano patrimonial ou extrapatrimonial (moral) ao titular dos dados. Para a imputação de responsabilidade de ambos não se exigirá a demonstração de dolo ou culpa (é responsabilidade objetiva) (MIRAGEM, 2019, p. 27).

Sendo assim, estes que defendem a aplicação da responsabilidade civil objetiva buscam demonstrar que isso se dá em virtude da semelhança com o CDC – que, como dito, adota o regime da responsabilidade objetiva – bem como argumentam que a finalidade da Lei Geral de Proteção de Dados é mitigar os casos de vazamento e de tratamento inadequado de dados, gerenciando o “risco intrínseco aos titulares” (MENDES, DONEDA, 2018, p. 473).

Por outro lado, aqueles que defendem a aplicação da responsabilidade subjetiva em matéria de proteção de dados argumentam que é necessária a análise da culpa, tendo em vista o sistema de obrigações e deveres dos agentes de tratamento abordados no texto da LGPD, como o disposto nos artigos 37, 39, 42 e 46 da norma.

Para essa corrente, antes de se responsabilizar o agente de tratamento de dados, deve-se analisar se este observou aos requisitos legais, bem como se houve culpa ou dolo, para, então, determinar se há responsabilidade civil e, consequentemente, o dever de reparar os danos.

Nesse sentido, Bruno (2019, p. 323) esclarece que “é possível sustentar que a regra geral da Lei é a da responsabilidade civil subjetiva, no qual o elemento da culpa deverá ser demonstrado". Como argumento central para tal entendimento, defende-

se que a lei não poderia criar uma série de métodos e cuidados a serem seguidos pelo tratador de dados e, depois, não analisar se tais disposições foram cumpridas – ou seja, se existiu culpa ou dolo – para fins de responsabilização civil.

Para essa corrente, criar um *standard* de comportamento a ser seguido pelo agente de tratamento de dados e, ao final, aplicar a responsabilidade subjetiva, seria desprovido de lógica e representaria uma confissão de ineficácia das normas impostas pela Lei Geral de Proteção de Dados (GUEDES, 2019).

Diante de tal dicotomia, observa-se que a aplicação da responsabilidade civil nos casos de vazamento de dados torna-se ainda mais complexa, haja vista que a própria lei não trata do assunto de maneira clara e objetiva.

Sendo assim, cabe aos tribunais pátrios analisar os casos dessa natureza, de modo a debater, criar e consolidar um entendimento quanto ao regime de responsabilidade civil aplicável à proteção de dados pessoais, uniformizando o tratamento quanto ao assunto, em respeito ao artigo 926 do Código de Processo Civil (BRASIL, 2023b) e em observância ao princípio da segurança jurídica.

Devidamente demonstrada a ausência de consenso quanto à modalidade de responsabilidade civil aplicável em caso de vazamento ou tratamento inadequado de dados pessoais, cumpre, a seguir, apresentar as peculiaridades da LGPD quando o agente tratador de dados é o Poder Público.

3.2 A RESPONSABILIDADE CIVIL DO ESTADO PELO VAZAMENTO DE DADOS

A Lei Geral de Proteção de Dados destinou seu capítulo IV ao tratamento de dados pessoais pelo Poder Público, em seus artigos 23 a 32. Explica, assim, como o tratamento de dados deve ser realizado pelo Estado, prevendo normas para a manipulação e segurança adequada dessas informações.

Importa destacar que, para a LGPD, o tratamento diferenciado disposto no capítulo IV não se aplica às empresas públicas e às sociedades de economia mista que atuam no mercado de concorrência. Veja-se:

> Artigo 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no artigo 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
> Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo (BRASIL, 2022a).

Outro aspecto importante que consta no capítulo IV da Lei Geral de Proteção de Dados é a responsabilidade civil aplicada à Administração Pública quando estiver na posição de agente tratadora de dados pessoais, em caso de vazamento ou compartilhamento de informações.

Apesar de abordar a responsabilidade civil, cumpre destacar que a lei, assim como na responsabilidade civil das empresas privadas, não traz de forma expressa, em seu texto, qual o regime de responsabilização adotado. Todavia, no caso de responsabilização da Administração Pública, deve-se observar o que dispõe o artigo 37, §6º, da Constituição da República:

> Artigo 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
> [...]
> § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa (BRASIL, 2023a).

Nesse sentido a Constituição Federal de 1988 expõe, de maneira clara, que a responsabilidade da Administração Pública pelos danos causados é objetiva, assegurado o direito de regresso contra o responsável em caso de dolo ou culpa. Trata-se de responsabilidade extracontratual do Estado, a qual se conceitua do seguinte modo:

> Pode-se, portanto, dizer que a responsabilidade extracontratual do Estado corresponde à obrigação de reparar danos causados a terceiros em decorrência de comportamentos comissivos ou omissivos, materiais ou jurídicos, lícitos ou ilícitos, imputáveis aos agentes públicos (DI PIETRO, 2022, p. 843).

Nessa perspectiva, importa diferenciar quando se adota a responsabilidade objetiva e quando se adota, excepcionalmente, a responsabilidade subjetiva em caso de dano provocado pelo Estado em sentido amplo. Assim, compreendendo a responsabilidade objetiva como aquela que dispensa a análise de culpa, pode-se

afirmar que o Estado responderá dessa forma sempre que causar danos patrimoniais ou morais a terceiros, por atos comissivos, ressalvadas as excludentes de responsabilidade.

O regime acima expressa a teoria do risco administrativo, pelo qual há responsabilidade objetiva do Estado pelos atos comissivos praticados por seus agentes. Em síntese:

> Registra-se na jurisprudência e na doutrina, o que repercutiu em legislações nesse sentido, a adoção paulatina da teoria do risco, que deixa de lado a indagação acerca da culpa (elemento subjetivo) e se concentra no fato de que as atividades estatais envolvem riscos. [...]
> A responsabilização decorrente de risco também é chamada de responsabilidade objetiva do Estado, em contraposição à subjetiva. A ideia presente na responsabilização objetiva do Estado, que não mais pressupõe a conduta culposa (NOHARA, 2023, p. 766)

Sem a pretensão de esgotar o tema, importante ressaltar, para os fins desse artigo, que a teoria do risco administrativo admite excludentes e atenuantes de responsabilidade. Assim, caso o ente público comprove a ocorrência de força maior, caso fortuito, fato de terceiro ou culpa exclusiva da vítima, será isento de responsabilidade, enquanto se comprovar culpa concorrente da vítima ou de terceiros, poderá atenuá-la.

Por outro lado, em caso de omissão pelo Poder Público que provoque dano a terceiro, a doutrina e a jurisprudência reconhecem a incidência da teoria da culpa do serviço público, segundo a qual deve o Estado responder sob o regime da responsabilidade civil subjetiva em caso de omissão lesiva.

Segundo essa teoria, também conhecida como teoria da culpa anônima do serviço público, o Estado responderá pelos danos causados por omissão lesiva desde que o serviço público seja defeituoso (funcione mal ou não funcione) ou funcione atrasado (DI PIETRO, 2022).

Assim, nesses casos, a condenação do Estado demanda provar que a omissão lesiva representa atuação em desconformidade com seu dever legal ou descaso que legitime o dever de reparar o dano.

Contudo, sobre a responsabilização desmedida do ente público, que “nem toda conduta omissiva retrata um desleixo do Estado em cumprir um dever legal; se assim for, não se configurará a responsabilidade estatal” (CARVALHO FILHO, 2022, p. 514). Isto é, deve-se analisar se houve culpa pelo Estado, de modo a caracterizar sua responsabilidade pelo dano causado.

Uma das formas de apurar se houve desleixo do Estado em cumprir um dever legal é analisar se houve, no tratamento de dados, desrespeito aos princípios constitucionais a serem observados pela Administração Pública (art. 37, caput, CR/88), bem como aos princípios e às demais regras que regem a Lei Geral de Proteção de Dados, a exemplo:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (BRASIL, 2022a).

Além destes, o artigo 6º da Lei Geral de Proteção de Dados ainda prevê o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas como princípios a serem observados no tratamento de dados pessoais.

Nesse sentido, cabe a aplicação de responsabilidade objetiva ao Estado em caso de conduta comissiva danosa, ressalvadas as excludentes de responsabilidade, bem como de responsabilidade subjetiva quando a omissão do Poder Público representar desleixo em desempenhar seu dever legal, provocando danos a terceiros.

Cumpre ressaltar, por fim, que, nos termos da segunda parte do artigo 37, §6º, da Constituição Federal, é assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa. Dessa forma, enquanto a responsabilidade do Estado pode ser objetiva ou subjetiva, a depender da conduta lesiva, o direito de regresso em

face do agente público apenas é devido em caso de dolo ou culpa deste, ou seja, aplica-se a responsabilidade subjetiva ao agente público. Confira-se:

> Ao dizer que o Estado pode exercer seu direito de regresso contra o agente responsável nos casos de culpa ou dolo, a Constituição vinculou as partes à teoria da responsabilidade subjetiva ou com culpa. Significa dizer que o Estado só pode ressarcir-se do montante com que indenizou o lesado se comprovar a atuação culposa de seu agente, o que, aliás, constitui a regra geral no direito privado.
> [...]
> Estão presentes, desse modo, no preceito constitucional, dois tipos de responsabilidade civil: a do Estado, sujeito à responsabilidade objetiva, e a do agente estatal, sob o qual incide a responsabilidade subjetiva ou com culpa (CARVALHO FILHO, 2022, p. 508).

Devidamente abordado o regime de responsabilidade civil aplicável às condutas estatais, bem como as possibilidades de excludentes de responsabilidade e de direito de regresso em face do agente público, cabe destacar que tal regime também se aplica em matéria de proteção de dados pessoais.

Restam esclarecidas, portanto, as maneiras de responsabilização do Poder Público em caso de violação de dados pessoais, devendo o Estado se atentar às regras contidas na Lei Geral de Proteção de Dados, em especial no artigo 6º e no capítulo IV, bem como aos princípios constitucionais contidos no artigo 37 da Constituição Federal, evitando danos aos titulares e, consequentemente, sua responsabilização, seja sob o regime da responsabilidade objetiva ou subjetiva.

Diante desse esclarecimento, se faz necessário, ainda, avaliar como o Poder Judiciário vem processando e julgando, na prática, o vazamento e o tratamento inadequado de dados pessoais pelas repartições públicas. Para tal, se recorre ao caso do Instituto Nacional do Seguro Social, com diversos indícios de vazamento de dados ao longo dos últimos anos, causando danos morais e materiais aos titulares de dados pessoais.

4. O VAZAMENTO DE DADOS PESSOAIS PELO INSS

O Instituto Nacional do Seguro Social (INSS) é uma instituição pública criada para atender as necessidades sociais e previdenciárias de seus contribuintes, garantindo, por exemplo, os direitos dos segurados do Regime Geral de Previdência Social.

Para além de suas competências administrativas, tais quais conceder benefícios previdenciários, o INSS também possui competência para administrar e operacionalizar o Cadastro Nacional de Informações Sociais (CNIS), conforme dispõe o artigo 3º, inciso I, do Decreto nº 10.047/2019 (BRASIL, 2019).

No sítio eletrônico oficial do Governo Federal (EMITIR..., 2023), conceitua-se o CNIS como “o documento que informa todos os seus vínculos, remunerações e contribuições previdenciárias”. Assim, de modo a viabilizar a organização das informações do beneficiário pelo CNIS, é imprescindível a coleta e o tratamento de dados pessoais.

A partir disso, tem-se que o INSS, ao longo das décadas, constituiu um vasto banco de dados, abastecido pelas informações pessoais de milhares de brasileiros. Essa coleta de dados pessoais, sensíveis ou não, pela autarquia é realizada por meio do cadastro dos segurados, presencial ou virtualmente, junto ao sistema do INSS.

Destaca-se o fato de que, uma vez que estas informações são utilizadas para a execução de serviço público, os titulares dos dados – mesmo que sensíveis – não precisam consentir com o seu tratamento, como dispõe o artigo 11, inciso II, da LGPD, em suas alíneas “a” e “b”. Confira-se na íntegra:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> [...]
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (BRASIL, 2022a).

Além desse meio de coleta de dados pessoais, o INSS possui acesso a documentos emitidos ou armazenados por outras instituições públicas, por meio de um sistema

de integração e intercâmbio de dados pessoais que facilita a obtenção de informações de seus beneficiários.

A título de exemplo, existe a integração entre os sistemas do INSS, do Centro de Referência da Assistência Social – responsável pela manutenção e atualização do Cadastro Único – e do e-Social, que unifica a prestação das informações referentes à escrituração das obrigações fiscais, previdenciárias e trabalhistas dos cidadãos.

Assim posto, as informações coletadas são utilizadas para compor o documento intitulado “Extrato CNIS” que, conforme informado pelo Governo Federal, “consolida e agrupa as informações das diversas fontes de informação, sendo que esse processo leva em conta a vigência das fontes que alimentam o CNIS, para efeitos de cálculo de prevalência entre as fontes” (A LGPD..., 2021).

O banco de dados do INSS é tratado pela Dataprev, que é “uma empresa pública vinculada ao Ministério da Gestão e Inovação em Serviços Públicos, com personalidade jurídica de direito privado, patrimônio próprio e autonomia administrativa e financeira” (SOLUÇÕES..., 2023), criada pela Lei Federal nº 6.125/1974.

A Dataprev é uma empresa do ramo da tecnologia que gerencia e aperfeiçoa o banco de dados do INSS. Assim, tem por objetivo viabilizar tecnologias de informação na área da assistência social e da previdência, prestando serviço de tratamento de informações e atividades correlatas.

Desse modo, é possível compreender que esta empresa realiza o tratamento dos dados dos cadastrados e beneficiários do INSS, portanto, à luz do que dispõe o artigo 5º, incisos VI e VII, da Lei Geral de Proteção de Dados, o INSS se trata do controlador desses dados pessoais, enquanto a Dataprev é a operadora dessas informações.

Sendo assim, em caso de vazamento ou de qualquer outra violação referente a esses dados pessoais, é cabível a responsabilização de ambas. Apesar das imposições da LGPD para assegurar a proteção aos dados pessoais armazenados

pelo INSS, os vazamentos de dados pela autarquia não sofreram a redução esperada, ocorrendo, ainda, de forma recorrente.

Isso se confirma pelo fato de que, nos últimos anos, foram diversos os casos de vazamento de dados dos segurados da previdência social, sendo essas informações utilizadas para alimentar bancos de dados de instituições financeiras, por exemplo.

Assim, empresas privadas que tiveram acesso aos dados pessoais dos beneficiários do INSS passaram a realizar propostas abusivas, de maneira antiética e ilegal, àqueles que recebem ou que receberão benefícios previdenciários, em especial, os idosos, que estão mais suscetíveis a serem convencidos por golpes e propostas de tal natureza.

Veja trecho de reportagem do Instituto Brasileiro de Defesa do Consumidor em denúncia a esse tipo de situação (GOLPE..., 2019):

> Novos beneficiários estão sendo assediados insistentemente por telefone ou nas agências por bancos e financeiras que passam a oferecer o empréstimo antes mesmo de o INSS notificar a pessoa que ela conseguiu o benefício.
>
> No crédito consignado, como as parcelas são descontadas diretamente do salário ou da aposentadoria, a renda fica comprometida antes mesmo de o dinheiro chegar à conta do consumidor. O resultado? Facilidade para realizar empréstimos e muita dificuldade para pagar as parcelas, levando muitos ao superendividamento.

Percebe-se, desse modo, como a problemática do vazamento de dados provoca uma repercussão social negativa, principalmente em relação à população mais vulnerável, como idosos e população de baixa renda. Diante desse cenário, após diversas denúncias, a situação chegou ao plenário da Câmara dos Deputados:

> Alerta à Comissão de Defesa dos Direitos da Pessoa Idosa:
>
> Em março de 2019, o Idec contatou a Deputada Federal Lídice da Mata, Presidente da Comissão de Defesa dos Direitos da Pessoa Idosa (CIDOSO), da Câmara dos Deputados, manifestando grande preocupação com os aspectos regulatórios que favorecem a abordagem abusiva dos consumidores e com o vazamento criminoso de dados dos beneficiários do INSS, em que requisitava a tomada de medidas pela Comissão. Em abril, a deputada presidente da Comissão encaminhou dois requerimentos:
>
> Requerimento 17/2019 solitica informações no sentido de esclarecer a Comissão quanto às denúncias sobre os abusos na oferta e concessão de

> empréstimos consignados, principalmente para aposentados e demais beneficiários do INSS;
>
> Requerimento 18/2019 requer a realização de Audiência Pública, em conjunto com a Comissão de Defesa do Consumidor, com a finalidade de debater os abusos na oferta e concessão de empréstimos consignados, principalmente para aposentados e demais beneficiários do INSS (GOLPE..., 2019).

No intuito de identificar a origem dos numerosos vazamentos de dados pessoais do banco de dados do Instituto Nacional do Seguro Social, iniciou-se, em 2018, investigação denominada “Operação *Data Leak*”, inicialmente no estado do Mato Grosso e, posteriormente, se expandindo para outros estados, apurando os crimes de vazamento e receptação ilícita de dados sigilosos, corrupção, lavagem de dinheiro, dentre outros.

A Polícia Federal, a partir de denúncias e evidências coletadas, passou a suspeitar que os atos ilícitos visando ao vazamento de informações envolveriam servidores do INSS e da Dataprev – empresa responsável pelo armazenamento e tratamento de dados dos cadastrados no sistema da autarquia previdenciária – estimando-se que as informações estariam sendo cedidas mediante pagamentos na ordem dos milhões de reais (OPERAÇÃO..., 2018).

Dentre as consequências práticas da operação, foram instaurados procedimentos investigativos e ações judiciais contra os suspeitos de favorecimento do esquema de vazamento de dados, além de cumpridos diversos mandados de busca e apreensão e de prisão.

Uma operação desta magnitude apenas reforça a gravidade da atual situação de vazamento de informações sigilosas do banco de dados do INSS, afetando a milhares de brasileiros, o que demonstra, no mínimo, a ausência da implementação adequada das cautelas e das medidas de segurança previstas na Lei Geral de Proteção de Dados.

Cumpre, nesse momento, mapear as decisões dos tribunais regionais e das cortes superiores quanto ao tema, de modo a verificar de que maneira a responsabilidade civil do Poder Público vem sendo considerada em matéria de proteção de dados.

4.1 JULGAMENTOS DE CASOS DE VAZAMENTO DE DADOS PELO INSS

O cenário de vazamento e tratamento inadequado de dados pessoais, amplificado pela sociedade digital e sua constante evolução, é relativamente recente, ainda não existindo um entendimento jurisprudencial consolidado sobre a matéria, o que torna essencial fomentar debates visando à criação de teses em torno do tema.

Conforme abordado, a legislação brasileira evoluiu, ao longo dos anos, a fim de abarcar a proteção aos dados pessoais, regulamentando a coleta e o tratamento dessas informações. Apesar disso, ainda restam lacunas a respeito do regime de responsabilidade civil aplicado pela LGPD aos agentes tratadores de dados.

Quanto ao tema da responsabilidade civil em matéria de proteção de dados, ainda não há um consenso na jurisprudência brasileira quanto à incidência de responsabilidade subjetiva ou objetiva. Os tribunais, ao processarem e julgarem estes casos, formulam teorias e entendimentos diversos, inexistindo, até então, uniformidade no tratamento da matéria, em especial, quanto ao regime de responsabilidade aplicável (BRANCO, 2021).

Em relação aos casos que envolvem o INSS como agente tratador de dados, aborda-se, inicialmente, o julgamento do Recurso Inominado Cível nº 5000086-03.2021.4.03.6345, pelo Tribunal Regional Federal da 3ª Região (BRASIL, 2022b).

No caso, a requerente ajuizou ação de indenização por danos morais em face do INSS, sob o fundamento de que, depois do deferimento do benefício previdenciário de pensão por morte, em junho de 2021, teria recebido diversas ligações e mensagens de bancos e outras empresas do ramo financeiro oferecendo empréstimos e benefícios de crédito.

Em primeiro grau, o pedido da autora foi julgado procedente, todavia, o INSS recorreu da sentença, alegando a ausência de conduta que acarretasse dano moral. Ademais, a autarquia alegou que deveria ser aplicada a responsabilidade civil subjetiva e que, consequentemente, a culpa do réu deveria ser demonstrada pela autora, extraindo tal entendimento do artigo 42 da LGPD.

Por sua vez, o tribunal regional negou provimento ao Recurso Inominado interposto pelo INSS, entendendo que houve dano moral suportado pela autora, bem como que as provas acostadas aos autos seriam suficientes para demonstrar que os danos sofridos extrapolam o mero dissabor cotidiano.

No julgamento do recurso, o Ministro Relator entendeu, em seu voto, pela aplicação da responsabilidade objetiva, tendo em vista o disposto no artigo 37, §6º, da Constituição Federal, e que não restam dúvidas que, tratando-se de ente estatal, a responsabilidade da civil adotada pela LGPD é a objetiva. De modo que caberia interpretação quando a responsabilidade subjetiva apenas para empresas privadas ou pessoas físicas.

O Tribunal concluiu, nesse sentido, que houve o compartilhamento ilegal dos dados pessoais da parte recorrida por ato lesivo do INSS, tendo em vista que este deveria ter adotado medidas de segurança a fim de evitar situações como essa.

Em caso semelhante, o Tribunal Regional Federal da 4ª Região (TRF-4) julgou a Apelação Cível nº 5042071-61.2016.4.04.7100/RS, referente a processo originário no qual o requerente pleiteava a condenação do INSS ao pagamento de danos morais (BRASIL, 2022c).

Em suma, o autor requereu administrativamente, em 2015, o benefício previdenciário de aposentadoria por tempo de contribuição, entretanto, depois de concedido, requereu o seu cancelamento por não concordar com o valor apurado pela autarquia.

Em 2016, o autor pleiteou novamente a concessão do benefício de aposentadoria, entretanto, não obteve êxito, pelo fato de o seu benefício anterior, com valor inferior, não ter sido desativado mesmo após o requerimento administrativo.

Na ocasião do tratamento de dados pessoais do titular pelo INSS, terceiros de má-fé obtiveram as informações do autor, contraindo empréstimos junto a instituições bancárias em seu nome.

Diante disso, o sujeito lesado ajuizou ação requerendo a concessão do benefício de aposentadoria e a indenização por danos morais, em decorrência da conduta ilícita do INSS, sendo julgada a ação procedente apenas quanto ao pedido de concessão do benefício previdenciário.

Inconformado com a sentença, o autor interpôs Recurso de Apelação, alegando certa omissão do juízo de primeira instância ao analisar o pedido de indenização por danos morais pelo vazamento de seus dados pessoais, alegando falha no serviço e dever de reparar.

No julgamento do recurso, o voto vencedor, do ministro relator Francisco Donizete Gomes, defendeu a aplicação de responsabilidade objetiva ao INSS pelos danos causados, uma vez que, se tratando de entidade pública, é dispensada a análise de culpa, nos termos do artigo 37, §6º, da Constituição Federal, sendo este mais um caso de reconhecimento de responsabilidade objetiva em caso de vazamento de dados pelo Poder Público.

Outro caso que se ressalta, para os fins dessa pesquisa, é o julgamento da Apelação Cível nº 5001738-29.2019.4.04.7111/RS, referente a pleito indenizatório pelo vazamento de dados pelo INSS, no qual o autor requereu a aplicação do regime da responsabilidade objetiva, com fundamento na Constituição Federal (BRASIL, 2022d).

Os sucessores processuais da requerente originária alegaram que esta passou a receber inúmeras ligações de instituições financeiras logo após a concessão do benefício de aposentadoria, até a data de seu falecimento, ultrapassando o razoável. Eles alegaram que as informações obtidas por terceiros foram vazadas do banco de dados do INSS, o que ensejaria indenização por danos morais.

Todavia, o TRF-4 negou provimento ao recurso interposto, por considerar que as alegações autorais não teriam sido comprovadas. Entendeu o tribunal que não estariam provados nos autos o ato ilícito do INSS, o dano moral sofrido e o nexo causal entre os dois. De acordo com o voto, os dados poderiam ter sido compartilhados por qualquer sujeito, não necessariamente o INSS.

Assim, desconsiderando a hipossuficiência técnica e o ônus de difícil desincumbência para o recorrente, o TRF-4 entendeu que seria dever deste comprovar a ocorrência de ato ilícito pelo INSS e o dano moral sofrido, o que impossibilitou a incidência de responsabilidade civil.

Pelo exposto, é possível verificar que, ainda que não haja jurisprudência pacífica quanto ao regime de responsabilidade civil aplicável em caso de vazamento ou tratamento inadequado de dados, os tribunais tendem a entender pela incidência de responsabilidade objetiva quando o agente tratador de dados é o Poder Público, nos termos do artigo 37, §6º, da Constituição Federal.

Do mesmo modo, observa-se que as decisões proferidas em um mesmo tribunal podem divergir, como é o caso do TRF-4. Isso se afirma pelo fato de que, enquanto uma turma aplicou a responsabilidade objetiva e julgou procedentes os pedidos autorais, aplicando a responsabilidade objetiva, outra turma sequer entrou no mérito da responsabilidade, uma vez que impôs ao autor o ônus de comprovar que suas informações pessoas haviam sido divulgadas pela autarquia.

Tudo isso demonstra a necessidade de os tribunais firmarem uma jurisprudência sólida a respeito do tema, a fim de evitar, por exemplo, que os autores tenham seus pedidos negados em decorrência da dificuldade probatória em caso de vazamento de dados, devido à notória hipossuficiência técnica da qual padecem.

As decisões a respeito desse tema ainda são relativamente recentes, sendo que diversas das ações indenizatórias sequer tiveram decisão de mérito em primeira instância. Entretanto, é possível analisar a tendência de julgamento dos tribunais em caso de vazamento de dados envolvendo o INSS, a qual aponta para a aplicação da responsabilidade objetiva, afastando-se a tese do INSS de ausência de responsabilidade pela não comprovação da culpa.

5. CONSIDERAÇÕES FINAIS

O presente trabalho pretendeu analisar de que forma ocorrem a coleta e o tratamento de dados pessoais pelo INSS, acarretando, em diversos casos, o vazamento dessas informações sigilosas. Além disso, a pesquisa demonstra como se posiciona a jurisprudência quanto ao tema da responsabilidade civil em matéria de proteção de dados quando o agente tratador é o próprio Poder Público.

Divide-se o estudo em três etapas. Inicialmente, é feita uma análise geral de como os dados pessoais deixaram de ser apenas expressão da identidade dos sujeitos para se tornarem verdadeiras moedas de troca no mercado atual, dotados de valor econômico crescente.

Dessa forma, buscou-se demonstrar como a coleta e o tratamento de informações pessoais por terceiros, bem como a comercialização desses dados, é fenômeno cotidiano da sociedade digital. Assim, faz-se importante definir o que se entende por “banco de dados”, conceituado como coleções organizadas de informações estruturadas dos titulares, armazenadas digitalmente por instituições públicas ou privadas.

Na segunda etapa, são abordados os direitos à privacidade e à autodeterminação informativa, tendo em vista que a proteção de dados é extraível desses direitos fundamentais. Se aponta a constante violação de direitos do cidadão na era digital, ao ter seus dados coletados, tratados e comercializados sem o seu consentimento.

Além disso, houve a preocupação de discutir a legislação que trata da proteção de dados e o seu avanço ao longo dos anos, para garantir uma proteção cada vez mais abrangente ao titular das informações. Para tanto, remete-se ao surgimento de normas jurídicas para proteger os cidadãos, diante da vulnerabilidade das informações disponibilizadas na rede.

Nesse sentido, é realizada a análise da evolução legislativa em um panorama internacional, a começar pelas normas europeias, que inauguraram a regulação do tema, influenciando os debates quanto à proteção de dados no Brasil.

Para tanto, destacou-se a importância do Código de Defesa do Consumidor, primeira legislação nacional a abordar expressamente a proteção de dados pessoais, essencial para a caminhada até a atual redação da Lei Geral de Proteção de Dados.

Ainda nesse capítulo, discutiu-se a lacuna presente na LGPD quanto ao regime de responsabilidade civil aplicável aos agentes tratadores de dados em caso de vazamento ou tratamento ilícito, identificando a dificuldade de extrair uma posição concreta a partir da literalidade da lei.

Nesse ponto, se adentrou o tema da responsabilidade civil do Poder Público em matéria de proteção de dados pessoais, quando o Estado é o próprio agente tratador. Para tanto, foi necessário analisar o capítulo IV da LGPD, que trata especificamente do Poder Público, assim como o artigo 37, §6º, da Constituição Federal.

Na última etapa desse trabalho, visou-se a analisar os casos de vazamento de informações contidas no banco de dado do INSS, gerenciadas pela Dataprev, por meio da análise sobre a coleta e o tratamento desses dados pessoais. Nessa perspectiva, foi demonstrado que o vazamento de informações sob guarda do INSS é fenômeno de ampla repercussão social, envolvendo terceiros de má-fé e agentes públicos que buscam se aproveitar do valor econômico dos dados.

Por fim, realizou-se pesquisa jurisprudencial com a finalidade de observar como os tribunais pátrios julgam os pleitos indenizatórios em face do INSS, em matéria de vazamento ou compartilhamento ilícito de dados pessoais. Dessa maneira, foi constatado que, em razão de se tratar de tema relativamente recente, os tribunais regionais e superiores ainda não possuem entendimento pacificado quanto ao tema, existindo entendimentos diversos.

Apesar disso, observa-se a tendência à adoção da responsabilidade civil objetiva, nos termos do artigo 37, §6º da Constituição Federal de 1988, dispensando a configuração de culpa para a responsabilização da autarquia previdenciária.

Desse modo, tendo em vista que esses dados coletados, sem anuência de seus titulares, são utilizados como moeda de troca no mercado, torna-se ainda mais urgente a criação de um sistema jurisprudencial sólido de proteção de dados pessoais, a fim de assegurar os direitos à privacidade e à autodeterminação informativa, superando as lacunas legais e impedindo a impunidade de agentes tratadores e a violação de direitos.

REFERÊNCIAS

A LGPD e o INSS. 2021. Disponível em: https://www.gov.br/inss/pt-br/centrais-de-conteudo/publicacoes/apresentacoes/SaibaMaisLGPDINSS.pdf/view. Acesso em: 28 out. 2023.

BRANCO, Mariana. Vazamento de dados gera direito a indenização por danos morais? **JOTA**, São Paulo, 2021. Disponível em: https://www.jota.info/justica/vazamento-de-dados-danos-morais-16082021. Acesso em: 04 nov. 2023.

BRASIL. (Constituição [1988]). **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 set. 2023.

BRASIL. **Decreto nº 10.047, de 9 de outubro de 2019**. Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações. [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm. Acesso em: 12 out. 2023.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 14 set. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD)**.** Brasília: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 set. 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 12 out. 2023.

BRASIL. Superior Tribunal De Justiça. **Recurso Especial nº 223.378/RS**. Relator: Ruy Rosado de Aguiar – Quarta Turma. Diário de Justiça Eletrônico, Brasília, 20 mar. 1995. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=199200114466&dt_pu. Acesso em: 22 set. 2023.

BRASIL. Tribunal Regional Federal da 3ª Região. **Recurso Inominado Cível nº 5000086-03.2021.4.03.6345/SP**. Relator: Janaina Rodrigues Valle Gomes – 12ª Turma Recursal. Diário de Justiça Eletrônico, São Paulo, 15 jun. 2022. Disponível em: https://www.conjur.com.br/dl/inss-indenizar-beneficiaria-vazamento.pdf. Acesso em: 04 nov. 2023.

BRASIL. Tribunal Regional Federal da 4ª Região. **Apelação Cível nº 5042071-61.2016.4.04.7100/RS**. Relator: Francisco Donizete Gomes – Quinta Turma. Diário de Justiça Eletrônico, Rio Grande do Sul, 04 mai. 2022. Disponível em: https://eproc.trf4.jus.br/eproc2trf4/controlador.php?acao=acessar_documento_publico&doc=416516766087672002009204756 39&evento=40400188&key=f3e8de83c62a1a432807d28df9d4ea3c258173c452ed006bd48ab7a237000192&hash=ecd7a73a1e050a9b5b86984578e26f82. Acesso em: 04 nov. 2023.

BRASIL. Tribunal Regional Federal da 4ª Região. **Apelação Cível nº 5001738-29.2019.4.04.7111/RS**. Relator: Vivian Josete Pantaleão Caminha – Quarta Turma. Diário de Justiça Eletrônico, Rio Grande do Sul, 12 ago. 2022. Disponível em: https://eproc.trf4.jus.br/eproc2trf4/controlador.php?acao=acessar_documento_publico&doc=416603252633618919182259102 32&evento=40400188&key=0199bb66c3941c2ef14fde760f7e7582a76a8ad41f9cb333ace15e8637b286fd&hash=14f58ffcfc19c6212b17a14fb6fde580. Acesso em: 04 nov. 2023.

BRUNO, Marcos Gomes da Silva. Da responsabilidade e do ressarcimento de danos. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de dados comentada. Revista dos Tribunais, São Paulo, 2019. p. 323.

CAMPOS, Álisson Thiago de Assis. A revolução da internet: significados e repercussões. In: BOLZAN DE MORAIS, José Luís; LOBO, Edilene (org.). **Temas de Estado de Direito e Tecnologia**, Porto Alegre: Editora Fi, 2021. p 49-84.

CAMPOS, Ricardo Resende. **Palestra on-line:** A constitucionalização da proteção de dados. Uma visão comparada Brasil-Alemanha. YouTube, 21 mar. 2022. Disponível em: https://www.youtube.com/watch?v=7TYUCSvWhhU. Acesso em: 10 set. 2023.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. Rio de Janeiro: Grupo GEN, 36. ed. 2022. p. 514. E-book.

COSTA, Anna Gabriela. Em 2021, Brasil ficou no topo de vazamento de informações no mundo, diz especialista. **CNN Brasil**, São Paulo, 18 dez. 2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/. Acesso em: 26 out. 2023.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 35 ed. Rio de Janeiro: Editora Forense, 2022.

DIZARD JUNIOR, Wilson. **A nova mídia:** a comunicação de massa na era da informação. 2. ed. Rio de Janeiro: Editora Jorge Zahar, 2000.

DÖHMANN, Indra Spiecker Gen. A proteção de dados pessoais sob o regulamento geral de proteção de dados da União Europeia. In: BIONI, Bruno (coord. exec.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. p. 113-129. E-book.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em 01 nov. 2023.

DONEDA, Danilo. Panorama histórico de proteção de dados pessoais. In: BIONI, Bruno (coord. exec.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. p. 22-39. E-book.

EMITIR Extrato de Contribuição (CNIS). **Gov.br**, Brasília, 20 jun. 2023. Disponível em: https://www.gov.br/pt-br/servicos/emitir-extrato-de-contribuicao-cnis. Acesso em 23 out. 2023.

FREIRE JÚNIOR, Américo Bedê. **O conteúdo retórico do direito à privacidade e a validade da prova obtida mediante filmagens nos ambientes público e privado**. 2014. 228 f. Tese (Doutorado em Direitos e Garantias Fundamentais) - Programa de Pós-Graduação em Direitos e Garantias Fundamentais, Faculdade de Direito de Vitória, Vitória, 2014. Disponível em: http://repositorio.fdv.br:8080/bitstream/fdv/9/1/americo-bede-freire-junior-.pdf. Acesso em 19 out. 2023.

GOLPE da aposentadoria: fuja das ofertas abusivas de crédito consignado. **Instituto Brasileiro de Defesa do Consumidor**, São Paulo, 2019. Disponível em:https://idec.org.br/golpe-aposentadoria. Acesso em 01 nov. 2023.

GONÇALVES, Arthur. O direito à proteção de dados como garantia à autodeterminabilidade informacional do sujeito. In: SOARES, Ricardo Maurício Freire; MACHADO, Flávia Sulz Campos; CARVALHO FILHO, João Francisco Liberato de Mattos (org.). **Novas fronteiras do neoconstitucionalismo**: direitos fundamentais, processo e cidadania. Salvador: Editora Paginae, 2019. p. 45-68. Disponível em: https://ppgd.ufba.br/sites/ppgd.ufba.br/files/novas_fronteiras_do_neoconstitucionalismo_1.pdf. Acesso em: 3 set. 2023.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro:** Responsabilidade Civil. v. 4. São Paulo: Editora Saraiva, 2023. E-book.

GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotado pela Lei de Proteção de Dados brasileira. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). **Caderno especial**: Lei Geral de Proteção de Dados (LGPD). São Paulo: Editora Thomson Reuters, 2019. p. 168-182. Disponível em: http://giselasampaio.com.br/wp-content/uploads/2021/12/24.-Regime-de-responsabilidade-adotado-pela-Lei-de-Protecao-de-Dados-brasileira.pdf. Acesso em: 4 out. 2023.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da Ajuris**, [S.l], v. 41, n. 135, 2014. Disponível em: https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/206. Acesso em: 12 set. 2023.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 15. ed. São Paulo: Editora Saraiva, 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista dos Tribunais**, São Paulo, v. 120, p. 469-483, nov./dez. 2018.

MENEZES NETO, Elias Jacob de; BOLZAN DE MORAIS, Jose Luis. A fragilização do Estado-Nação na proteção dos direitos humanos violados pelas tecnologias da informação e comunicação. **Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 23, n. 3, p. 231-257, set./dez. 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 173-222, nov. 2019. Disponível em: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 01 out. 2023.

MULHOLLAND. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 162, set./dez. 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555/574. Acesso em: 21 set. 2023.

OLIVEIRA, Luciano Rocha de. **Proteção de Dados Pessoais no Processo Penal e na Segurança Pública**: problemas atuais e perspectivas. São Paulo: Editora Dialética, 2022. E-book.

OPERAÇÃO apura vazamento de dados sigilosos do INSS e compre mandados em MT, PR, RS, RJ e ES. **G1 MT**, Mato Grosso, 2018. Disponível em: https://g1.globo.com/mt/mato-grosso/noticia/2018/12/11/operacao-apura-vazamento-de-dados-sigilosos-do-inss-e-cumpre-mandados-em-mt-pr-rs-rj-e-es.ghtml. Acesso em 07 nov. 2023.

PINHEIRO, Victor Sales; BONNA, Alexandre Pereira. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito. **Revista de Direitos e Garantias Fundamentais**, *[S. l.]*, v. 21, n. 3, p. 365–394, 2020. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555. Acesso em: 1 nov. 2023.

ROSENVALD, Nelson; FARIAS, Cristiano Chaves de; NETTO, Felipe Peixoto Braga. **Novo Tratado de Responsabilidade Civil**. 4. ed. São Paulo: Editora Saraiva, 2019. E-book.

SARLET, Ingo Wolfgang. Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo

Horizonte, a. 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875/985. Acesso em: 17 out. 2023.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: BIONI, Bruno (coord. exec.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. p. 330-349. E-book.

SILVA, Alex Matoso. A revolução da internet versus privacidade. In: BOLZAN DE MORAIS, José Luís; LOBO, Edilene (org). **Temas de Estado de Direito e Tecnologia**, Porto Alegre: Editora Fi, 2021. p 85-106.

SOLUÇÕES digitais para governo e cidadão: A Dataprev está presente na vida do cidadão brasileiro, provendo a tecnologia necessária para os programas estratégicos e sociais do governo. **Dataprev**, Brasília, 2023. Disponível em: https://www.dataprev.gov.br/conheca-dataprev-quem-somos/empresa. Acesso em 25 out. 2023.

SOUZA, Carlos Affonso; PADRÃO, Vinicius. Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). **Caderno especial***:* Lei Geral de Proteção de Dados (LGPD). São Paulo: Editora Thomson Reuters, 2019. p. 168-182.

TAURION, Cezar. ***Big Data***. 1. ed. Rio de Janeiro: Editora Brasport, 2013. Ebook.

THE WORLD'S most valuable resource is no longer oil, but data. **The Economist**, Londres, mai. 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 27 dez. 2023.

VÉLIZ, Carissa. **Privacidade é Poder**: Por que você deveria retomar o controle dos seus dados. 1 ed. São Paulo: Editora Contracorrente, 2021. E-book.