CENTRO UNIVERSITÁRIO CURITIBA – UNICURITIBA
MESTRADO EM DIREITO EMPRESARIAL E CIDADANIA

FRANKLYN DE SOUSA FERRAZ

DADOS PESSOAIS, DIREITOS VULNERÁVEIS: DA INGENUIDADE NORMATIVA FRENTE AO PODER TECNOLÓGICO

Curitiba
2025

FRANKLYN DE SOUSA FERRAZ

DADOS PESSOAIS, DIREITOS VULNERÁVEIS: DA INGENUIDADE NORMATIVA FRENTE AO PODER TECNOLÓGICO

Dissertação apresentada ao Programa de Pós-Graduação em Direito Empresarial e Cidadania do Centro Universitário Curitiba – UNICURITIBA como exigência parcial à obtenção do título de Mestre em Direito Empresarial e Cidadania.

Linha de Pesquisa: Atividade empresarial e Constituição: inclusão e sustentabilidade.

Orientadora: Profa. Dra. Laís Gomes Bergstein.

Curitiba

2025

FRANKLYN DE SOUSA FERRAZ

DADOS PESSOAIS, DIREITOS VULNERÁVEIS: DA INGENUIDADE NORMATIVA FRENTE AO PODER TECNOLÓGICO

Dissertação apresentada ao Programa de Pós-Graduação em Direito Empresarial e Cidadania do Centro Universitário Curitiba – UNICURITIBA como exigência parcial à obtenção do título de Mestre em Direito Empresarial e Cidadania.

APROVADO EM: ____/_____/2025

BANCA EXAMINADORA

_____

Profa. Dra. Laís Gomes Bergstein (Orientadora)
Centro Universitário Curitiba – UNICURITIBA

_____

Profa. Dra. Karla Pinhel Ribeiro (Membro Interno – UNICURITIBA)
Centro Universitário Curitiba – UNICURITIBA

_____

Profa. Dra. Andreza Cristina Baggio (Membro Externo – UNICURITIBA)
Centro Universitário Curitiba – UNICURITIBA

Dedico este trabalho à minha esposa, Mônica Saboia, e à minha querida filha, Mônica Ferraz, por sempre estarem perto quando o cansaço chega, dando fôlego e renovando as esperanças.

AGRADECIMENTOS

Minha imensa gratidão à Dra. Laís Gomes Bergstein pela paciência e dedicação no acompanhamento deste trabalho.

Aos professores do Mestrado em Direito Empresarial e Cidadania da UNICURITIBA, pela forma singela, mas profunda, de ministrarem as aulas e, por serem exemplos de vida.

Às Professoras Dra. Viviane Coêlho de Séllos Knoerr e Lindaura Pinheiro por tornarem este sonho, antes tão distante, possível. Muito obrigado!

“O maior inimigo do conhecimento não é a ignorância, é a ilusão do conhecimento”.

Stephen Hawking

RESUMO

O direito à privacidade é uma construção recente dentro dos direitos da personalidade, que por sua vez, não tem sua origem há muito no tempo. Cuida-se de um núcleo íntimo, que guarda pertinência com afeição a intimidade (vida íntima familiar, pessoal e de dados sensíveis). O estudo teve como objetivou uma análise de conteúdo normativa, doutrinária e jurisprudencial, tendo como referência normativa a Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, complementada por outros diplomas que integram o microssistema de proteção de dados no Brasil, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet. Trata-se de uma pesquisa jurídico, dogmática e teórica, foi utilizado como procedimento a análise de conteúdo, mediante o estudo da Lei nº 13.709/2018. Dessa forma, o estudo foi desenvolvido em 3 capítulos, sendo o primeiro reservado a compreensão doutrinária do direito da personalidade a partir do Código Civil de 2003, bem como, ao fornecimento voluntário de dados. O capítulo 2 (dois) se encarrega de conceituar a autodeterminação informativa no fornecimento de dados com base na Lei nº 13.709/2018. O capítulo 3 (três), buscou verificar como têm reagido os tribunais superiores na tutela da autodeterminação informativa, dos dados e dos bancos de dados, considerando a previsão normativa em vigor desde a Lei nº 13.709/2018. Diante do exposto, conclui-se que o controle dos dados já não está nas mãos do titular, e o simples consentimento tornou-se insuficiente diante da complexidade do tratamento automatizado. A sofisticação dos sistemas de tratamento de dados e o uso intensivo de inteligência artificial demandam uma superação das dicotomias normativas, como a separação rígida entre dados sensíveis e não sensíveis em prol de uma abordagem mais realista e dinâmica.

Palavras-chave: Direito à privacidade. Proteção de dados. Lei Geral de Proteção de Dados.

ABSTRACT

The right to privacy is a recent construction within personality rights, which, in turn, do not originate long ago. It concerns an intimate core, which is closely related to intimacy (private family life, personal life, and sensitive data). The study aimed to analyze normative, doctrinal and jurisprudential content, using as a normative reference the General Personal Data Protection Law - Law No. 13,709/2018, complemented by other diplomas that integrate the data protection microsystem in Brazil, such as the Consumer Defense Code, the Positive Registration Law and the Internet Civil Framework. This is a legal, dogmatic, and theoretical study, using content analysis as a procedure, through the study of Law No. 13,709/2018. Thus, the study was developed in three chapters, the first of which focuses on the doctrinal understanding of personality rights based on the 2003 Civil Code, as well as the voluntary provision of data. Chapter two (2) conceptualizes informational self-determination in the provision of data based on Law No. 13,709/2018. Chapter three (3) sought to determine how higher courts have responded to the protection of informational self-determination, data, and databases, considering the regulatory provisions in force since Law No. 13,709/2018. Given the above, it is concluded that control over data is no longer in the hands of the data subject, and simple consent has become insufficient given the complexity of automated processing. The sophistication of data processing systems and the intensive use of artificial intelligence demand overcoming normative dichotomies, such as the rigid separation between sensitive and non-sensitive data, in favor of a more realistic and dynamic approach.

Keywords: Right to privacy. Data protection. General Data Protection Law.

LISTA DE ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados
ANPD	Agência Nacional de Proteção de Dados
CFOAB	Conselho Federal da Ordem dos Advogados do Brasil
GDPR	General Data Protection Regulation
IBGE	Instituto Brasileiro de Geografia e Estatística
LGPD	Lei Geral de Proteção de Dados Pessoais
RGPD	Regulamento Geral sobre a Proteção de Dados
STF	Supremo Tribunal Federal
TFH	Tools for Humanity
UNICURITIBA	Centro Universitário Curitiba.

SUMÁRIO

1. INTRODUÇÃO

No atual momento de desenvolvimento tecnológico, observa-se que a existência, a percepção de existência, passou a ser fracionada entre duas realidades, um material e outra virtual. A realidade material é aquela a que toma conhecimento quando do nascimento, reduzida as relações sensoriais provocadas por uma existência física frágil e limitada, porém, na qual se tem um controle parcial.

A existência virtual, por sua vez, é uma abstração, um somatório de informações, que em detrimento não possuírem gatilhos de dor no sentido de sensações físicas, estão de tal forma indissociáveis da percepção de existência, que podem somatizar sensações tão excruciantes quanto aquelas impostas ao corpo físico. Ao ponto de ser um viés de existência recente, observa-se a ausência de autonomia em negar fazer parte dela. Não faz parte do espectro de autonomia a decisão sobre existir ou não no universo virtual. É uma imposição sob a qual não se admite resistência.

Nesse viés, a percepção e apropriação do conceito de Direito da Personalidade e Autodeterminação Informativa em relação a formação dos bancos de dados, passam a ser relevantes, em um primeiro momento, na tentativa de resguardar um mínimo de privacidade e autonomia dentro dessa nova realidade, uma vez que a cada minuto, uma infinidade de dados é extraída, transferida e organizada de forma incalculável (Tepedino; Teffé, 2020).

Dados genéticos, preferências culturais, estéticas e de consumo, orientações políticas ou religiosas e opção sexual, tudo é coletado em tempo real e nos mais variados meios. Tais informações relacionam-se diretamente com os direitos da personalidade e afetam as liberdades fundamentais do ser humano, devendo ser protegidas de forma destacada e contextualizada com o desenvolvimento tecnológico (Rodotá, 2008).

É nesse contexto que se espera uma evolução jurisprudencial adequada a proteção dos dados, proteção dos Direitos da Personalidade, reconhecendo-se as duas percepções de existência, material e virtual, como um todo de uma existência humana, ganhando músculo a salvaguarda da autodeterminação informativa frente mineração de dados/perfilamento e a integridade digital.

A dúvida que se estabelece diz respeito a suficiência e eficácia dos conceitos normativos para salvaguardar a dignidade, a privacidade e a autonomia dos indivíduos

em um cenário no qual a captação e o tratamento de dados escapam ao controle, como possibilidade de utilização discriminatória dos dados pessoais, tanto por parte do mercado quanto do Estado, associado a conjunturas em que podem estar presentes potenciais violações de direitos fundamentais, em razão da sua natureza (Mulholland, 2018). Principalmente quando nos referimos a sensibilidade de alguns dados, aqueles associados às opções e características basilares da *persona* e, portanto, aptos a gerar situações de discriminação e desigualdade (Moraes, 2008).

A segurança e a proteção do indivíduo no âmbito digital, no que afeta aos inúmeros usos dos dados pessoais e, de modo especial, no contexto da internet, ainda é algo em construção, muito embora já se tenha no Brasil desde 2014 um marco civil que, dentre outros pilares, expressamente previu como princípio estruturante a privacidade, delegando, no entanto, a proteção de dados pessoais a uma legislação específica que se concretizou por meio da promulgação da Lei Geral de Proteção de Dados, Lei 13.709/2018 (doravante LGPD).

Assim, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/18) 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, como os da liberdade de expressão e de comunicação, privacidade, honra, imagem, autodeterminação informativa e livre desenvolvimento da personalidade (art. 2º). Reconhecendo a efetivação e promoção de Direitos Humanos Fundamentais como justificativa para a tutela dos dados pessoais (art. 2º, VII).

Nesse estado de coisas, torna-se necessária a compreensão evolutiva do direito da personalidade e da autodeterminação informativa, com vistas a visão dos tribunais superiores em relação aos bancos de dados, frente a um novo modelo de negócios que se estabelece, onde as informações pessoas são o produto[1].

---

[1] A criação de empresas apenas para monetização de dados pessoais tem se tornada, segundo o capital, uma nova fronteira de negócios. Essa percepção é de fácil constatação quando consultamos os jornais, mais especificamente, quando nos deparamos com duas reportagens veiculadas pelo site UOL, emblemáticas quanto ao tema, onde noticia-se a monetização de dados de clientes pela rede de farmácias RaiaDrogasil.
Segundo afirma a reportagem, a referida rede de farmácias armazenou e continua armazenando por mais de 15 anos, registros de hábitos de consumo de seus clientes (histórico de saúde, comportamento sexual etc), através da exigência de CPF para oportunizar descontos nos preços, ultrapassando os 48 milhões de clientes registrados, com uma projeção de que uma em cada cinco pessoas da população brasileira tenha seus registros junto a referida empresa.
A captação de dados, segundo informou o CEO da empresa a reportagem, iniciou-se ainda no ano de 2006, porém, seu tratamento com esse objetivo se deu a partir do ano 2017, intensificando-se a partir

A fim de analisar a temática proposta, esta monografia foi pautada em uma abordagem jurídico-dogmática e teórica, com ênfase na análise de conteúdo normativa, doutrinária e jurisprudencial, tendo como referência normativa a Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, complementada por outros diplomas que integram o microssistema de proteção de dados no Brasil, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet. Além da legislação, utilizam-se como fontes doutrinas especializadas, artigos científicos e decisões dos tribunais superiores, com destaque para o Supremo Tribunal Federal (STF) e o Superior Tribunal de Justiça (STJ), a fim de identificar tendências interpretativas e lacunas normativas no tratamento da matéria.

O método empregado é qualitativo, exploratório e interpretativo, com a finalidade de compreender o fenômeno jurídico da proteção de dados em sua relação com os direitos da personalidade e a autodeterminação informativa, inserido no contexto do avanço das tecnologias de tratamento automatizado de dados. O procedimento técnico utilizado é a pesquisa bibliográfica e documental, com ênfase na análise crítica e interdisciplinar da legislação e da jurisprudência recente.

Divide-se em 3 (três) capítulos, sendo o primeiro reservado a compreensão doutrinária do direito da personalidade a partir do Código Civil de 2003, bem como, ao fornecimento voluntário de dados. O capítulo 2 (dois) se encarrega de conceituar à autodeterminação informativa no fornecimento de dados com base na Lei nº 13.709/2018.

Por sua vez, o capítulo 3 (três), busca verificar como têm reagido nossos tribunais superiores na tutela dos dados e dos bancos de dados, considerando-se a Lei nº 13.709/2018, tomando como referência o modelo de negócios que se estabeleceu com exploração de dados pessoais.

Espera-se que a pesquisa contribua para o compreensão do modelo normativo atual, especialmente no que se refere à dicotomia entre dados pessoais e dados sensíveis e à centralidade conferida ao consentimento como principal instrumento de

---

de 2021. Para o CEO da RaiaDrogasil a monetização desses dados de hábitos de consumo é possível em face da “autorização” - aceite da política de privacidade - que os clientes firmam no momento do fornecimento de seus CPFs em troca de descontos, o que ocorre em 97 % das compras.
Em poder dessas informações, afirma à reportagem, a RaiaDrogasil criou uma subsidiária no ano 2021, a RD Ads, com o único objetivo de monetizar esses dados junto as indústrias e agências de publicidade, traduzindo-se em uma nova fonte de receita.

proteção. Pretende-se demonstrar que, diante da realidade tecnológica atual, o tratamento dos dados pessoais, o controle da formação e da destinação das informações assumem papel central na proteção da dignidade da pessoa humana no ambiente digital.

A pesquisa almeja oferecer subsídios teóricos e críticos para o aprimoramento do debate jurídico sobre a proteção de dados, propondo uma visão evolutiva e dinâmica dos direitos da personalidade e da autodeterminação informativa, compatível com os riscos da era digital e com a necessidade de atualização interpretativa dos marcos normativos.

2 COMPREENSÃO DOUTRINÁRIA DO DIREITO DA PERSONALIDADE A PARTIR DO CÓDIGO CIVIL DE 2003 E O FORNECIMENTO VOLUNTÁRIO DE DADOS

Do final do século XX ao início do século XXI, foram observadas transformações sem precedentes na evolução tecnológica, assim como na própria evolução da sociedade, seja através dos novos métodos de comunicação, de interação, de socialização, ou mesmo na aquisição ou venda de bens e serviços. E essa evolução surge em tal velocidade que é fato observar que não é possível discernir se a evolução tecnológica decorre da necessidade da evolução humana, ou se esta evolução decorre do rápido desenvolvimento tecnológico.

Nessa realidade, as pessoas ficaram mais expostas ao mundo, na medida da interação ou repassa dados pessoais, por qualquer meio, manual ou digital, sem que se tenha o mínimo de preocupação com a devida segurança destas informações.

No Contrato Social havia uma ideia clara de mitigação da liberdade em face da segurança. Nas relações virtuais, observa-se que não há contrapartida substancial em face do compartilhamento dos dados. Se conhecimento já era poder, no universo virtual, não se apropria de conhecimento, mas do próprio ser, dados genéticos, preferencias culturais, estéticas, de consumo, orientações políticas, religiosas e opções sexuais, com implicações nas interações sociais reais.

Neste capítulo, abordar-se-á compreensão doutrinária do direito da personalidade, tendo como referência o Código Civil de 2003 e o fornecimento voluntário de dados.

Assim, o capítulo aprofundará sobre os direitos da personalidade, inseridos dentre os direitos fundamentais da pessoa humana, que envolvem a privacidade, a intimidade, o sigilo, a honra e a imagem, que não podem ser violados por terceiros não autorizados, em regra, com objetivos comerciais ou fraudulentos, sem que os detentores destes dados autorizem seu uso.

A importância dos direitos fundamentais é uma conquista dentro dos tempos modernos, visto que até o passado os direitos individuais não eram sequer apontados como importantes pelo Estado, o que no Brasil passou a mudar com a promulgação da Constituição Federal de 1988 (Gunther; Macei; Donate, 2020).

2.1 Conceito jurídico de pessoa

O conceito de pessoa tem permeado há muito tempo as reflexões em ética e direito, sem discordância a respeito da sua importância, ainda que haja grande divergência em relação ao seu significado.

Dessa forma, em termos gerais, a questão da definição de pessoa pode ser colocada nos seguintes termos: O que é ser uma pessoa? O que é necessário, e o que é suficiente, para alguma coisa ser considerada como uma pessoa, em oposição a uma não-pessoa? O que as pessoas têm, que as não-pessoas não têm? Isso se resume mais ou menos a pergunta pela definição da palavra pessoa (Olson, 2010).

A terminologia pessoa, do modo que se encontra redigida no Código Civil abrange tanto a pessoa natural, isto é, o ser humano, quanto a jurídica. Importante notar, contudo, que a gênese da palavra pessoa está intimamente relacionada às pessoas físicas, em qualquer das três origens etimológicas que lhe sejam atribuídas (Castañeda, 1989).

Na primeira delas, entende-se que o termo advém do etrusco arcaico Phersu, que decorreria da deusa Perséfone, significando máscara, pois, nas festas em sua homenagem, este adereço seria utilizado. A segunda origem seria a palavra grega prosopon, que, de início, significava rosto e também passou a se identificar com a máscara utilizada nas festas campestres em homenagem a Dionísio (Castañeda, 1989).

A concessão do atual significado à palavra é bastante sugestiva, já que a condição de pessoa é a vestimenta do homem, a maneira como ele se apresenta na sociedade, o papel por ele representado socialmente. Somente se apresenta aos demais aquele que é, antes de tudo, em si mesmo, isto é, aquele que tem consciência de que representa um papel a ser apresentado aos demais (Reale, 2009).

Por essa razão, Reale (2009) define a pessoa (nesse caso, a pessoa natural) como:

> “A dimensão atributiva do ser humano, ou seja, a qualificação do indivíduo como ser social enquanto se afirmar e se correlaciona no seio da convivência através de laços éticos jurídicos (...)”. Convém salientar, desde o início, a relevância conferida, em todos os conceitos, à pessoa natural em detrimento da pessoa jurídica, eis que esta última, como se terá oportunidade de demonstrar, é um instrumento para a consecução de objetivos humanos,

> sendo uma realidade meramente técnica, e não substancial, especialmente quanto aos entes coletivos de direito privado.

Contudo, dentro do contexto jurídico, o conceito de pessoa ganhou outros contornos, de modo a significar todo ser suscetível, ou apto, à aquisição de direitos e deveres, o que, evidentemente, também inclui as pessoas jurídicas. O direito remanesce com conteúdo humanístico mesmo quando confere a outros entes o status de pessoa porque “o faz sempre em razão e benefício do homem”, de maneira a se comprovar “o caráter natural do conceito de sujeito de direito”. (Machado, 2013).

Acredita assim que sua análise do uso do conceito de pessoa teria mostrado que o que é moralmente e legalmente importante para os direitos humanos seriam os fatos subjacentes à pessoalidade e não o próprio conceito de pessoa, o que implica que a “pessoalidade não deveria ser o campo de batalha central para o discurso de direitos humanos” (Ohlin, 2005, p. 238).

Defendendo uma concepção reducionista atribuída a Parfit, Ohlin privilegia os níveis mais baixos quando se trata de fatos e explicações que envolvem vários níveis, o que significa que, no caso de pessoas, são os fatos relacionados à biologia, à racionalidade e à psicologia que deveriam ser considerados relevantes para os direitos humanos e não o conceito de pessoa: “Desde que os fatos de nível mais baixo é que são importantes, o próprio conceito de pessoa não pode ser necessário para os direitos humanos” (Ohlin, 2005, p. 240).

2.2 Direitos da personalidade

No Brasil, somente a partir da Constituição Federal de 1988 e do atual Código Civil, esse instituto foi expressamente incorporado ao direito positivo nacional (Sarlet, 2007).

Essa relativa novidade do instituto veio acompanhada de intenso debate doutrinário. Nesse âmbito, uma série de problemas é colocada, abarcando desde a própria existência, até a natureza e a forma mais adequada de tutela dos direitos de personalidade, dentre outras questões igualmente relevantes (Tepedino, 2004). O que torna pertinente a contextualização histórica para sua melhor compreensão, uma vez que origem remonta a outras civilizações.

2.2.1. Contexto histórico dogmático dos direitos de personalidade

O princípio da personalidade no direito, segundo o qual todo ser humano, independentemente de sua classe social, origem ou condição, era possuidor de personalidade e capacidade jurídicas, já era conhecido por algumas cidades-estado gregas do período clássico (Cabanes, 2009). Mas foi somente a partir dos séculos IV e III a.C. que a noção de um direito geral de personalidade floresceu, em virtude do surgimento da filosofia e do desenvolvimento de uma nova mentalidade entre os gregos.

No direito romano, a plena personalidade era reconhecida apenas aos indivíduos *sui iuris*, isto é, aqueles que titularizassem, conjuntamente, o status *libertatis*, o status *civitatis* e o status *familiae*, restando aos *alieni iuris*, escravos e estrangeiros, uma personalidade jurídica limitada a determinadas situações (Sousa, 2011).

Ressalta-se então, que a personalidade, até o advento da República, era protegida contra a morte, ofensas corporais e rapto, dentre outras condutas consideradas ilícitas, sendo a respectiva sanção, geralmente de natureza corporal e, apenas nos casos de lesão pessoal leve, de caráter pecuniário, implementada contra o ofensor por meio da vingança privada. A tutela se dava de forma genérica através da *actio iniuriarum*, especialmente nos casos de injúria, quando restasse caracterizado o *animus iniuriandi* da parte do ofensor (Szaniawski, 2005).

Durante o período clássico, já sob o Alto Império, alargou-se o alcance da *actio iniuriarum*, que, além de proteger a pessoa em si, passou também a protegê-la em suas relações jurídicas concretas, podendo o julgador livremente estimar a injúria e graduar pecuniariamente a sanção ao quantum *aequum iudici videbitur* (Sousa, 2011).

Ao longo da Idade Média, não se observou qualquer evolução significativa da proteção da personalidade, tendo perdurado como instrumento, com o mesmo alcance e características, a *actio iniuriarum*.

Na Inglaterra do início do século XIII, uma sequência de fracassos do rei João Sem Terra levou a um levante dos barões que, tendo invadido Londres, forçaram-no a assinar, em junho de 1215, um documento que limitava o poder do monarca, inclusive quanto à criação ou majoração de tributos, à apreensão dos bens e ao cerceamento da liberdade dos súditos sem o devido processo, e que ficou conhecido

como *Magna Charta Libertatum* ou, simplesmente, Magna Carta: estava aberto o caminho para as declarações de direitos que marcariam o nascimento do Estado moderno (Billier; Maryioli, 2005).

Assim, muito embora as antigas sociedades grega e romana já dispusessem de instrumentos para a tutela da pessoa, conforme já mencionamos, somente com a aurora da modernidade a discussão dos direitos de personalidade, na esteira dos debates em torno dos direitos humanos e fundamentais, adquiriria os contornos atuais, em cujo bojo essas expressões chegam a se confundir (Chiusi, 2007).

No século XVI, vários outros documentos reconheceram, na Europa e nas colônias inglesas da América do Norte, direitos individuais, através da crescente limitação do poder do Estado. Na França de 1589, o rei Henrique IV assinou o Édito de Nantes, reconhecendo a liberdade de religião para os calvinistas franceses; em 1639, as Fundamental Orders of Connecticut descreviam a estrutura e os poderes do governo colonial; em 1641, o *Body of Liberties* of Massachusetts também reconhecia direitos individuais oponíveis ao governo colonial; na Inglaterra, emergiram a *Petition of Rights*, de 1628, o Habeas Corpus Act, de 1679, o Bill of Rights, de 1688 e o Act of Settlement, de 1701, todos impondo limites à atuação do Estado contra o indivíduo, que passava a ser visto como titular de direitos subjetivos (Peces-Barba, 1995).

Já no terceiro quartel do século XVIII, a moderna filosofia política, construída sobre bases racionalistas e alardeada por toda a Europa e para além do Atlântico pelos teóricos iluministas, resultou em “textos de Declarações de Direitos que, pela primeira vez na história, enunciam e garantem direitos fundamentais” (Dimoulis; Martins, 2009).

A primeira dessas declarações foi proclamada no Estado da Virgínia, em 12 de junho de 1776, ano em que as treze ex-colônias da Inglaterra na América do Norte declararam independência. Direitos como a liberdade, a autonomia e a proteção da vida do indivíduo, a igualdade, propriedade, livre atividade econômica, liberdade de religião e de imprensa e proteção contra a repressão penal foram enunciadas em seu texto, conhecido como *Virginia Declaration of Rights*, ou *Virginia Bill of Rights*, resultando em declarações semelhantes, feitas pelos demais Estados norte-americanos (Dimoulis; Martins, 2009).

Já na França, em 2 de outubro de 1789, foi proclamada a *Déclaration des droits de l’homme et du citoyen*, que seria incorporada à Constituição Francesa de 1791,

também reconhecendo, a exemplo da Declaração da Virgínia, o direito à liberdade, igualdade, propriedade, segurança, resistência à opressão, liberdade de religião e pensamento e garantias contra a repressão penal (Szaniawski, 2005).

Em todos esses casos, não se tratava, ainda, de direitos reconhecidos à pessoa humana em suas relações recíprocas, mas de direitos individuais considerados oriundos do direito natural, oponíveis ao Estado, seus órgãos e agentes. Passou-se a reconhecer, de maneira genérica e abstrata, direitos da pessoa, considerada abstratamente nos termos do racionalismo então em voga, e tendo por fundamento a noção de dignidade da pessoa humana (Szaniawski, 2005).

O século XIX experimentou o que Szaniawski (2005) chamou de "fracionamento do direito geral de personalidade", em virtude do destaque que, naquele momento, ganharam a Escola Histórica do Direito e o Positivismo Jurídico. Nesse sentido, explica o autor que a Escola Histórica do Direito concebia o direito geral de personalidade como um direito que alguém possui sobre si mesmo, tendo por objeto a sua própria pessoa.

Por sua vez, Sousa (2011) atribui também ao positivismo jurídico o direito geral de personalidade no século XIX, e explica:

> [...] sendo o Estado, segundo o sistema positivista, a fonte única de direito, não havia mais lugar para a existência do direito geral de personalidade destinado a tutelar a personalidade humana, mas, tão-somente, seriam reconhecidas, pelo direito positivo, algumas tipificações de direitos de personalidade multifacetados. [...] para o positivismo jurídico, somente poderiam ser reconhecidos como direitos de personalidade os diversos direitos que derivam da pessoa humana, expressamente tipificados na lei, considerados os únicos e verdadeiros direitos subjetivos, merecedores de tutela do Estado. (p.43)

2.2.2. Os direitos de personalidade na legislação brasileira

Como se observa, muito embora alguns autores afirmem, como também se afirmou no início do presente capítulo, que "os direitos da personalidade são de construção recente", não se pode fazer confusão entre direitos de personalidade e tutela da pessoa humana. De fato, a personalidade, a pessoa ou o ser humano têm sido objeto de tutela pelo direito desde seus primórdios. A construção de um arcabouço legal, mediante a criação de um instituto jurídico específico no direito

positivo nacional, por outro lado, é fenômeno relativamente recente no direito brasileiro (Bittar, 2015; Gonçalves, 2010).

Com a instalação dos colonizadores portugueses no Brasil, ainda na primeira metade do século XVI, entraram em vigor na Colônia as Ordenações Manuelinas, compilação do direito vigente em Portugal promulgada em 1521 por D. Manuel I. Nessas Ordenações, a personalidade era protegida, a exemplo do direito romano, de forma genérica através da *actio iniuriarium,* cenário que permaneceu inalterado com a promulgação das Ordenações Filipinas, em 1603, que no Brasil permaneceram até a entrada em vigor do Código Civil de 1916, em 1º de janeiro de 1917 (Szaniawski, 2005).

O Código Civil Brasileiro de 1916 definia alguns direitos de personalidade de forma assistemática, “e sem conferir à garantia desses direitos uma especificidade distintiva dos demais direitos subjetivos tutelados no texto” (Mello, 2006). Nos casos não previstos no Código Beviláqua, a tutela da personalidade era remetida à tutela penal, de que são exemplos a Lei nº 4.117/1962 (Código Brasileiro de Telecomunicações) e a Lei nº 6.538/1978, que dispõe sobre crimes contra o serviço postal.

Para além da tutela penal, a personalidade somente seria legislativamente tutelada com o advento da Lei nº 5.479/1968, que dispunha sobre a retirada e transplante de tecidos, órgãos e partes de cadáveres para utilização com fins terapêuticos e científicos, e da Lei nº 5.988/1973, regulamentando os direitos autorais. Já na década de 1960, o anteprojeto de Código Civil elaborado por Gomes dedicou dezesseis artigos à tutela dos direitos de personalidade, sem trazer a previsão expressa de uma cláusula geral de tutela da personalidade (Szaniawski, 2005).

Com o advento da Constituição Federal de 1988, impôs-se a discussão sobre a tutela dos direitos de personalidade, em virtude do princípio da dignidade da pessoa humana, insculpido no inciso III do artigo 1º da Carta Magna.

Ressentindo-se da ausência, na Constituição, de uma cláusula geral expressa destinada a tutelar amplamente a personalidade do homem, Szaniawski (2005) indica um caminho hermenêutico para se inferir do sistema constitucional tal cláusula geral implícita:

> [...] A pilastra central, a viga mestra, sobre a qual se sustenta o direito geral de personalidade brasileiro, está consagrada no inciso III, do art. 1º da

> Constituição, consistindo no princípio da dignidade da pessoa humana. As outras colunas de sustentação do sistema de tutela da personalidade, consistem no direito fundamental de toda a pessoa possuir um patrimônio mínimo, previsto no Título II, art. 5º, inciso XXIII, e no Título VII, Capítulos II e III; e os demais princípios, consagrados no Título VIII, garantindo, no Capítulo II, a toda a pessoa, o exercício do direito à saúde; no Capítulo VI, o direito ao meio ambiente ecologicamente equilibrado, a fim de poder exercer seu direito à vida com o máximo de qualidade de vida; e, no Capítulo VII, o direito de possuir uma família e de planejá-la, de acordo com os princípios da dignidade da pessoa humana e da paternidade responsável. Todos esses princípios, segundo podemos constatar, asseguram a tutela da personalidade humana segundo a atuação de uma cláusula geral.

No atual Código Civil Brasileiro, os direitos de personalidade estão enunciados na Parte Geral, Livro I (das pessoas), Título I (das pessoas naturais), Capítulo II (dos direitos da personalidade), artigos 11 a 21.

> O art. 11 abre o Capítulo estatuindo que “Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária” (Brasil, 2002).

Ponto essencial nesse aspecto é perceber que o Direito Civil sofreu alteração substancial em seu paradigma da propriedade. Em detrimento não se atribuir apenas as novas tecnologias essa alteração do prisma econômico do direito, fato é que essa nova realidade trouxe a percepção mais clara do deslocamento axiológico de bens materiais para bens existenciais.

É relevante rememorar, que há uma relação de pertinência entre direitos humanos, direitos fundamentais e direitos da personalidade. Direitos humanos está em uma relação de gênero e espécie para os direitos fundamentais, assim como os direitos da personalidade são espécies do gênero direitos fundamentais. Essas relações nos permitem inferir que todo direito da personalidade é um direito fundamental, que por sua vez é um direito humano, todavia, o caminho inverso não é verdadeiro.

Resultando na compreensão de um segundo atributo conceitual da personalidade, além da simples capacidade de direitos, o caráter de ser humano, objeto de proteção do direito em face da afirmação de sua dignidade, algo inerente a sua existência. Dignidade que impõe abstenções e ações, horizontais e verticais, impedindo taxativamente a coisificação do ser humano, assegurando sua autodeterminação ao resguardar suas características existenciais substanciais, a liberdade de escolhas existenciais fundamentais.

Um objeto de proteção mais extenso do que aquilo que se percebe a primeira impressão (integridade física, moral e intelectual), resguardando os diversos aspectos do sujeito e suas irradiações e conexões, algo que vai além da percepção mediana.

Nesse sentido Borges (2007) afirma que o direito positivo não pode deixar a tutela da personalidade a cargo da vontade popular ou da consciência popular, principalmente se se recordar que essa mesma vontade ou consciência popular cometeu enormes crimes contra a humanidade, assim como contra a pessoa. Ter isso em mente é indispensável para analisar a relativa disponibilidade dos direitos de personalidade.

2.3 Direito à privacidade

O direito à privacidade é uma construção recente dentro dos direitos da personalidade, que por sua vez, não tem sua origem há muito no tempo. Cuida-se de um núcleo íntimo, que guarda pertinência com afeição a intimidade (vida íntima familiar, pessoal e de dados sensíveis).

A primeira referência doutrinária sobre a existência de um direito à privacidade ocorreu em ensaio realizado por Samuel Warren e Louis Brandeis em 1890. Baseados em decisões pretéritas dos tribunais ingleses e norte-americanos, perceberam que, gradativamente, a jurisprudência estendia a proteção da propriedade imaterial, chegando a reconhecer um espectro de intangibilidade dos sentimentos, que viria a se constituir em um direito próprio à privacy, significante da prerrogativa de não ser molestado e de ser deixado só (Cachapuz, 2006, p. 76-77).

Em um primeiro momento, por se tratar exatamente de uma abstração em construção, sua percepção ficou atrelada a espinha dorsal do Código Civil, ou seja, a propriedade. Nesse sentido, reconhecida sua existência autônoma, sua proteção se deu de forma negativa, dever geral de abstenção (não fazer), assim como em relação a propriedade.

Através da teoria do núcleo da personalidade, conhecida como teoria das esferas, é possível identificar três esferas distintas de proteção da privacidade, cada qual com um grau de intensidade. Alexy explicita:

> (...) É possível distinguir três esferas, com intensidades de proteção decrescente: a esfera mais interior ('último e inviolável âmbito de liberdade

> humana', âmbito mais interno (íntimo), 'esfera íntima inviolável', 'esfera nuclear da configuração da vida privada, protegida de forma absoluta'), a esfera privada ampliada, que inclui o âmbito privado que não pertence à esfera mais interior, e a esfera social, que inclui tudo aquilo que não for atribuído bem ao menos à esfera privada ampliada (2012, p. 360-361).

Em contrapartida, Luño (2012, p. 92-94), ao se referir ao conceito de intimidade, afirma que o problema desta se relaciona com as manifestações ou incidências exteriores em nossas vidas privadas, cujo exercício se tenha garantido juridicamente. De acordo com o jurista espanhol, não é suficiente conceber a intimidade como um direito de status negativo, ou seja, de defesa frente a qualquer intromissão na esfera privada. É necessário identificá-la também no seu caráter positivo, em outras palavras, como um direito ativo de controle sobre o fluxo de informações que concernem a cada sujeito.

Atualmente, a jurisprudência do Tribunal Constitucional Federal da Alemanha atribuiu novos contornos à teoria das esferas, pois não mais se prende a uma consideração estática dos âmbitos da vida cotidiana, adotando uma análise dinâmica dos modos de desenvolvimento do titular do direito, valorizando a autodeterminação, a autoconservação e a auto-exposição (Schwabe, 2005, p. 188-189).

Esse núcleo mais íntimo, porém, dentro da concepção dos direitos da personalidade, com a evolução tecnológica, passa a ser visto como uma nova fronteira para o capital, como ressaltou o CEO de empresa farmacêutica.

De acordo com o Bittar, coloca-se o direito à privacidade como:

> Um direito à vida privada em que busca proteger o indivíduo de invasões de terceiros na sua esfera íntima e pessoal, abrangendo também o direito à intimidade que tutela o contexto psíquico da pessoa, para resguardar a privacidade em seus múltiplos aspectos, sejam eles pessoais, particulares ou íntimos da vida da pessoa, em sua consciência, ou em seu circuito próprio, compreendendo seu lar, a sua família, sua correspondência e até mesmo aspectos negociais (Bittar, 2015, p. 173).

Sob um prisma valorativo, hoje os bens mais valiosos não são patrimoniais, mas existências. Primeiro na Constituição Federal, posteriormente no Código Civil (Capítulo II do Título I do Livro I da Parte Geral, normativo protetivo do Direito da Personalidade) e agora, mas recentemente, na Lei Geral de Proteção de Dados, a proteção aos bens existenciais nunca esteve implícita, pelo contrário, sempre foi expressa, em detrimento ser exemplificativa.

Os valores expressos no texto constitucional inspiram o construtor do Direito a

deixar definitivamente o patrimonialismo do século XIX para avançar rumo a um novo e promissor Direito pós-moderno: aberto, plural e, principalmente, solidário. A unidade do direito das obrigações, por exemplo, não está mais enraizada nos códigos civis, mas encontra-se “no conjunto de princípios e regras que se elevaram à Constituição e aos tratos internacionais em torno dos quais gravitam os microssistemas jurídicos que tratam das matérias a ele vinculadas” (Bergstein, 2018).

Verifica-se, que devido ao avanço das tecnologias e o rápido processamento de informações pessoais, estas tornaram-se mais expostas e modificou-se o sentindo que denominamos de direito à privacidade e intimidade. Para Bittar (2015) tal como nos alerta, esse direito vem assumindo paulatinamente maior relevo, com a contínua expansão das técnicas de virtualização do comércio, de comunicação, como defesa natural do homem contra as investidas tecnológicas e a ampliação, com a necessidade de locomoção, do círculo relacional do homem, obrigando-se à exposição permanente perante públicos os mais distintos, em seus diferentes trajetos sociais, negociais ou de lazer.

Em detrimento da coleta de informações pessoais não ser uma prática da atualidade, a crescente capacidade de se armazenar e tratar esses dados o é.

2.3.1. Conceituando a privacidade

A privacidade foi definida por Silva (2011) como um “conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso pode ser legalmente sujeito”. Assim o direito à privacidade confere ao indivíduo um direito subjetivo de controlar a intromissão de terceiros em sua vida privada ou se necessário o controle do que deve ou não ser conhecido, exercendo assim a liberdade e autodeterminação de suas informações de caráter individual e pessoal.

De acordo com Hirata (2017) a privacidade, o “direito de estar só” do direito americano, foi consolidado no Estado Moderno, estritamente vinculado ao indivíduo. Ao direito, importava proteger o domicílio do sujeito e a inviolabilidade de seus bens e propriedades. O conceito da privacidade e liberdade no século XX, por outro lado, adquire uma preocupação com a intimidade da vida privada, inspirado pelos direitos de personalidade constitucionais europeus. Além da proteção contra a arbitrariedade

da imprensa buscada no século XIX, o século seguinte também objetiva proteção em face ao Estado e da própria sociedade. Percebe-se que a tutela da privacidade foi sempre voltada à individualidade, progredindo no sentido de tutelar a existência do ser e da liberdade no modo de viver dos sujeitos.

Ressalta-se que a definição mais adequada é a que faz prevalecer a ideia de controle do indivíduo sobre as suas informações, em detrimento da ideia de isolamento do indivíduo. Conceituada dessa forma, a privacidade reflete claramente a existência de uma autonomia do seu titular na conformação desse direito. Isso significa que o titular tem a faculdade de conformar as fronteiras e os limites do exercício de seu direito à privacidade (Mendes, 2008, p.23).

Para Silva (2011) os chamados direitos personalíssimos ou direitos de personalidade são esses direitos que integram a própria noção de pessoa, como a vida, a honra, a integridade física, a imagem, a privacidade etc. No âmbito jurídico, a personalidade tem sido concebida como aptidão para ser sujeito de direitos e obrigações no mundo jurídico. Toda pessoa humana tem essa aptidão, de acordo com todos os sistemas jurídicos, no estágio atual da civilização, e que isso de nada valeria se ao mesmo tempo não lhes assegurasse um mínimo de direitos como condição indispensável à aquisição de todos os demais direitos.

A concepção de privacidade vai muito além do simplesmente “direito de ser deixado só” pois hoje assegurada pela constituição:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação (Brasil, 2003).

Observa-se, que a doutrina traz conceitos distintos entre vida privada, intimidade e privacidade. A profusão de termos utilizados pela doutrina brasileira para representá-la, propriamente ou não, é considerável; além de ‘privacidade’ propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como ‘privatividade’ e ‘privaticidade’, por exemplo (Doneda, 2006), mas como o foco do

trabalho é definir o direito do indivíduo de resguardar suas informações, então bastará a conceituação básica.

De maneira mais abrangente, o direito à privacidade consistiria em um direito subjetivo de toda pessoa sendo ela brasileira ou estrangeira, residente ou apenas de passagem, física ou jurídica, para evitar não apenas de constranger os outros e para que assim possa respeitar sua esfera privada, mas também de controlar suas informações de caráter pessoal (sensíveis ou não) (Nascimento, 2019).

Para Limberger (2007, p. 116), a intimidade como direito fundamental tem sua gênese na dignidade humana e está vinculado à própria personalidade, sendo seu núcleo central. Como direito que é da expressão da própria pessoa, desfruta da mais alta proteção constitucional". Conforme ainda a autora, as exigências do mundo tecnológico atual fizeram com que o direito tutelasse essa nova face da intimidade. A intimidade deriva da dignidade humana, é um direito fundamental que integra a personalidade.

2.4 Dados Pessoais

Na era digital muito se fala na captação e uso de dados pessoais. A informação passou a ser o bem econômico no mundo digital, sendo o motivador da necessidade de criação de normativo específico para tutela de seus titulares.

Para compreensão do conceito fático e até mesmo jurídico sobre o tema, vejamos o artigo 5º, da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a conceituação legal de Dados Pessoais:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

O Brasil adotou o modelo europeu, e aqui, a autoridade constituída para a regulação desta nova lei é a Agência Nacional de Proteção de Dados (ANPD), criada

como órgão da administração direta, vinculada à Presidência da República, sendo esta, uma estrutura provisória, pois no período de 2 anos deve haver um estudo quanto à transformação da sua natureza jurídica, visando ter maior independência e autonomia, uma vez que fiscalizará não só o setor privado como também o setor público (Pinheiro, 2020).

Um estudo realizado por Nascimento (2019) em relação à associação do conceito legal para com dados pessoais, evidenciou que a lei salienta diretamente sobre “dados pessoais”, não se confundindo com dados secundários, algoritmos, segredos de negócio e semelhantes que possuem embasamentos legais em demais diplomas como a Lei de Direitos Autorais e a Lei de Propriedade Industrial. De acordo com o autor, o termo “inclusive nos meios digitais”, ou seja, além dos meios físicos englobam também os produzidos na esfera digital.

Destes conceitos se pode extrair que dados pessoais são informações relacionadas à pessoa natural identificada ou identificável, ou seja, qualquer informação que permita identificar, direta ou indiretamente um indivíduo é considerada um dado pessoal. Relativas à pessoa física identificada ou que possa ser identificada com o cruzamento de duas ou mais informações.

É toda e qualquer informação que possa ser relacionada a uma pessoa natural, identificando-a de alguma maneira, anunciando seus gostos, suas preferências e até a sua intimidade, como expõe Pinheiro (2020, p. 36):

> Os dados pessoais é toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, números de Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

São exemplos de dados pessoais, nome, RG, CPF, gênero, data e local de nascimento, número do telefone, endereço residencial, endereço eletrônico (e-mail), dados de localização via GPS, placa de automóvel, imagem fotográfica ou computacional, cartão bancário, etc.

É importante observar que o dado, quando unitário e avulso, como um número de telefone, um endereço, um número de documento ou última compra realizada, podem, a princípio, não fazer referência a alguém diretamente, mas quando disponíveis em um banco de dados, organizados e cruzados, podem resultar em

informações bastante específicas sobre determinada pessoa, inclusive de caráter sensível, transformando-se em dados poderosos nas mãos de quem as detém (Teffé; Viola, 2020).

Os autores Macei e Silva ao tratar sobre a fundamentação da metafísica dos costumes, estudo preliminar à crítica da razão prática de Kant, traz observações que bem se subsomem a relação entre dados pessoas e dados pessoas sensíveis:

> "[…] seu valor depende do uso que delas se faça. Cabe dizer ... um bem em si, pode mesmo ser uma fonte de corrupção para quem não dispõe de uma boa vontade. Até mesmo certas qualidades superiores, como o domínio de si ou a reflexão, não podem considerar-se verdadeiramente boas, salvo se ao serviço de uma boa vontade" (Macei; Silva, 2017).

Como se verá mais adiante, são as condutas que deverão ser singularmente consideradas, ou seja, é a intenção do agente que tatuará o seu comportamento perante os demais em qualquer relação bilateral. No caso dos dados pessoais, torna-se necessário para além de sua natureza, a sua destinação.

Requisitados em distintas situações, muitas das quais fazem parte das atividades cotidianas das pessoas e das organizações, abrangem o direito à privacidade, significando que cada pessoa tem o direito de obstar a intromissão de estranhos na sua intimidade e vida privada, assim como na prerrogativa de controlar suas informações pessoais, evitando acesso e divulgação que não forem autorizadas.

2.4.1. Dados Pessoais Sensíveis

Como se observa, a legislação estabelece uma relação de gênero e espécie entre dados pessoas e dados pessoais sensíveis, conceituando esses como núcleo de informações da pessoa física que possam causar algum tipo de discriminação. Segundo o texto normativo, artigo 5º, da Lei nº 13.709, de 14 de agosto de 2018:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dados pessoais sensíveis estão relacionadas às características de personalidade e de suas escolhas pessoais como a sua origem racial ou étnica, a sua convicção religiosa, opinião política, filiação sindical ou religiosa, pensamentos filosóficos ou políticos, dados referentes a sua saúde, vida sexual, dado genético ou biométrico (Pinheiro, 2020, p. 37).

Para efeitos de proteção normativa expressa, são aqueles que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical ou organização de caráter religioso, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

Dentro do sistema jurídico de proteção de dados, esses dados guardam um nível de proteção maior e específico. O que quer dizer que são dados que necessitam de autorização expressa, de forma esclarecida e determinada no tempo para seu tratamento e utilização, nunca de forma tácita ou sem previsão de descarte. Desse modo, não sendo o compartilhamento de dados inequívoco quanto ao seu consentimento e transparente quanto a seu destino, não se pode deles dispor.

Os dados pessoais se referem à esfera da intimidade da pessoa, não projetando o indivíduo na sociedade, já os dados sensíveis fazem parte da esfera das suas convicções, seus costumes e preferências, formando, portanto, a sua identidade pública. Observa-se que tais dados são diferentes de um número de CPF, por exemplo, o qual não lhe dão qualquer característica identificável da pessoa. São dados tão característicos e pessoais do indivíduo, que podem ser utilizados de forma discriminatória, afetando o pleno desenvolvimento da personalidade e não permitindo decidir livremente sobre as questões fundamentais da sua vida (Korkmaz, 2019).

Além disso, os dados expostos sobre a opção religiosa, sexual ou política, podem, de certa forma, se resumir em temas excludentes em algoritmos de sistemas de seleção de determinada fatia de consumidor ou de público-alvo (Mendes, 2014).

Podem os diversos dados associados à determinada pessoa, favorecer processos sociais de exclusão e segregação, o que se apresenta como a chave de qualificação de determinados dados como sensíveis para a lei, com vistas violação de direitos fundamentais e outros danos graves à pessoa.

2.4.2. Dados Anonimizados

Ainda dentro da perspectiva do universo de dados pessoas, mas agora em vistas a sua disponibilização a interesses sociais e comercias, a legislação ainda possibilita o tratamento de dados relativos a um indivíduo para que não possa ser identificado, em razão ter passado por algum meio técnico de tratamento para garantir sua desvinculação, direta ou indireta, de uma pessoa. No texto da lei, assim vem expresso:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa. Para que os dados sejam considerados verdadeiramente anonimizados, é necessário que todas as informações que possam identificar uma pessoa sejam removidas ou tornadas irreversíveis. Isso significa que, uma vez anonimizados, os dados não podem ser usados para identificar, direta ou indiretamente, qualquer indivíduo em particular, o que afastaria a incidência da Lei nº 13.709/2018.

Só é considerado efetivamente anonimizado se não permitir, pelos meios técnicos disponíveis, que se reconstrua o caminho para encontrar o titular dos dados, e alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado.

2.5 Dados pessoais e direitos da personalidade

Percorrido o caminho até aqui, pode-se afirmar que os direitos da personalidade são responsáveis por protegerem a pessoa dos demais direitos, pois viabilizam a aquisição e proteção de características personalíssimas do indivíduo que,

munido deles, é capaz de adquirir e assegurar novos direitos. Imprescindíveis para a vida em sociedade, são caracterizados por serem indivisíveis, intransponíveis, imprescritíveis, impenhoráveis e inalienáveis, pois, sem eles, o sujeito é inábil de defender seu patrimônio ou adquirir novos bens (Szaniawski, 2005).

Nesse viés, fragmentados em três esferas: i) físicos; ii) morais; iii) psicológicos (Bittar, 2015) a proteção de dados pessoais, lato senso, representa um novo tipo de externalização de identidade das pessoas, compreendida nessa tradicional categoria dos direitos da personalidade, caracterizados como uma projeção, extensão ou dimensão do seu titular. Onde se observam também três tipos jurídicos a serem resguardados: o direito à liberdade, a privacidade, e o direito ao livre desenvolvimento da personalidade.

Sua omissão, fere diretamente a personalidade do titular da informação, pois abre a possibilidade a terceiros do uso frequente dessas informações sem o conhecimento e menos ainda anuência daquele que é portador pessoal da informação. Em tal caso, o desafio da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709) é de adequar o consentimento dos dados fornecidos à internet, fornecendo maior transparência aos usuários (Brasil, 2018).

No direito internacional já há referências relevantes tratando do tema. A proteção dos indivíduos no que se refere ao tratamento dos dados pessoais é regida pela Diretiva 1995/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados) e pela Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Tais Diretivas, interessante destacar, são plenamente aplicáveis ao fornecimento de conteúdos digitais (Bergstein; Kirchner, 2020).

Embora, os direitos da personalidade, pertençam a relações jurídicas sem expressão financeira, como já afirmamos, são informações portadoras de valor imensurável para o seu titular, como a honra, autoria, intimidade e liberdade. Sendo necessário que esses direitos não se separem do indivíduo, pelo contrário, eles devem possuir eficácia máxima, já que, sem eles, a vida digna é impossibilitada. Em virtude da sua eficácia absoluta, oponibilidade *erga omnes* e do caráter *excludendi alios*, os

direitos da personalidade são oponíveis contra qualquer outra pessoa ou instituição (Gagliano; Pamplona Filho, 2012).

Diante dessa realidade, a previsão normativa da defesa da personalidade na liberação de dados pessoais assim está posta: Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo. Para Bioni (2019), porém, não é suficiente, *in verbis*:

> É evidente, portanto, sob qualquer aspecto, a insuficiência dos termos do art. 21 do CC para tutelar todos os matizes da tutela da privacidade, diante de um cenário atual de desenvolvimento dos bancos de dados, das técnicas disruptivas de captação, catalogação e tratamento de dados, propulsionadas por algoritmos específicos, por mecanismos de big data e de análise preditiva de padrão de atuação no mercado de consumo, entre outros instrumentos que se utilizam dos dados como combustível para seguir com a aceleração da atividade econômica. Mecanismos de tutela da privacidade tornam-se, portanto, a cada dia mais relevantes. (p.45)

Com base nessa perspectiva, é importante a tutela de todos os direitos inerentes à personalidade, para que tenha êxito as políticas de privacidade, para que o ganho financeiro dentro do mundo de compartilhamento de dados seja feito da melhor e maior maneira da conservação da privacidade e por consequência da personalidade.

Neste sentido, para assegurar os direitos da personalidade, assim como a proteção dos dados, importante, portanto, a defesa dos direitos fundamentais de privacidade, liberdade, identidade, intimidade e imagem, direitos esses resguardados pelo artigo 5.º, caput e incisos II e X, entre tantos outros, da Constituição Federal e artigos 11 a 21 do Código Civil.

Afinal, como afirma a Professora Drª. Lais Bergstein, ao se referir a normativo protetivo do Código de Defesa do Consumidor, paralelo perfeitamente aplicável ao estudo que aqui se realiza: É importante afirmar, que a vulnerabilidade da pessoa natural também é resultante das falhas da percepção humana acerca dos riscos envolvidos na utilização de produtos ou serviços (Bergstein, 2019).

3 AUTODETERMINAÇÃO INFORMATIVA NO FORNECIMENTO DE DADOS PESSOAIS

3.1 Conceito de autodeterminação informativa

Por autodeterminação informativa entende-se o poder do indivíduo em determinar a coleta e utilização de seus dados pessoais. No contexto da sociedade da informação, como abordado anteriormente, diferentes cruzamentos de dados criam novos dados, o que faz com que não existam dados insignificantes, pois, a depender de um cruzamento e da finalidade do tratamento, um dado pode fazer diferença. O risco do processamento está na finalidade e nas possibilidades do processamento, e não no tipo do dado que está se tratando (Mendes, 2020), daí porque a autodeterminação, dentro do espectro dos direitos da personalidade, é um primeiro substrato a ser analisado.

3.1.1 Contexto histórico da autodeterminação informativa

Na segunda guerra mundial o estado nazista estruturou um processo de extermínio de grupos determinados, levando à morte milhões de pessoas no Holocausto. Nesse processo, a coleta de dados dos cidadãos judeus, ciganos e homossexuais tornou o Holocausto possível e cruelmente eficiente, o que motivou, nos anos subsequentes ao término da guerra, a criação de leis pelos legisladores europeus para tornar o uso de dados pessoais mais rigoroso, buscando impedir que se repetisse tratamento com tal finalidade (Kaiser, 2020).

Com o fim da segunda guerra, alguns diplomas explicitaram a preocupação com a vida privada das pessoas. Um desses é a Declaração Universal dos Direitos Humanos de 1948, que serviu de modelo para as Constituições adotadas por novas nações e para inclusão de direitos nas velhas Constituições. Ela expõe em seu artigo 12, que “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (United Nations, 2025).

O preâmbulo da citada declaração afirma que o desconhecimento e o desprezo dos direitos do ser humano conduziram a atos de barbárie que revoltam a consciência da Humanidade, e frente a isso, a declaração busca proteger direitos que são base e dentre eles o resguardo contra interferências ou ataques à vida privada.

Outros dois diplomas que introduziram tal preocupação foram a Convenção Europeia dos Direitos do Homem de 1950 e o Pacto Internacional de Direitos Civis e Políticos de 1966, os quais afirmam nos artigos 8º e 17, respectivamente, o direito ao respeito com a vida privada, família, domicílio e correspondência.

Com a passagem do tempo e o desenvolvimento da tecnologia da informação, chegamos ao ano de 1983, onde o Tribunal Constitucional Alemão debruçou-se sobre queixas constitucionais dirigidas contra a lei de Censo de 25 de março de 1982 (lei federal nº 369). No entendimento do Tribunal:

> [...] processamento de dados modernos, a proteção dos indivíduos contra coleta, armazenamento, uso e divulgação ilimitadas de seus dados pessoais é coberta pelo direito geral de personalidade do GG Art. 2 sec. 1 em conjunto com o GG Art. 1 sec. 1. Nesse sentido, o direito fundamental garante à autoridade do indivíduo determinar por si mesmo a divulgação e o uso de seus dados pessoais.

Com suporte no direito geral de personalidade e a dignidade humana inviolável, presentes nos artigos 1º e 2º da Lei Básica da República Federal da Alemanha, o Tribunal Constitucional conceituou autodeterminação informativa quando consignou que o indivíduo por si mesmo tem a autoridade para determinar a divulgação e uso dos dados pessoais. O direito geral de personalidade é um direito fundamental de conceito aberto visando a proteger o indivíduo como um todo, inclusive perante novos perigos (Ody; Cunha, 2021, p. 5).

Entendendo na oportunidade, porém, que este direito não era irrestrito, explicitando que:

> Restrições a esse direito à “autodeterminação informacional” são permitidas apenas no interesse público predominante. Eles exigem uma base jurídica constitucional que deve cumprir o requisito constitucional de clareza das normas. Em seus regulamentos, o legislador também deve observar o princípio da proporcionalidade. Ele também deve tomar precauções organizacionais e processuais que neutralizam o risco de violação do direito de personalidade.

Observa-se, que existiu um interesse público a justificar o tratamento dos dados pessoais, sendo possível em virtude dessa circunstância realizar o tratamento sem que o titular possa exercer sua autodeterminação sobre a coleta e o tratamento em questão. Todavia, precisam estar claros a justificativa do tratamento e os instrumentos que neutralizem o risco de violação, isto é, processos, técnicas, ferramentas que sejam aplicadas a resguardar os titulares.

A questão primária da análise foi o compartilhamento e não a proporcionalidade e, como ponto secundário, o tratamento de dados (Sarlet; Ruaro, 2021). Nesse sentido, o Tribunal Constitucional Alemão assim, entendeu que a lei do censo era constitucional, destacando que os resultados das estatísticas são indispensáveis para o monitoramento da situação social e econômica e seu desenvolvimento, servindo de subsídio para a elaboração de projetos, sendo de grande importância para uma política de Estado voltada ao princípio de bem estar social, o que está de acordo com os princípios e diretrizes da lei básica, mas considerou os recursos parcialmente fundamentados, anulando as regras de transmissão, com exceção da transmissão de dados anonimizados.

Ainda no que diz respeito a transmissão dos dados, o Tribunal entendeu que os dados coletados para fins estatísticos e que ainda não foram anonimizados podem ser encaminhados, desde que com expressa autorização legal, para o processamento estatístico por outras autoridades e desde que se apliquem as medidas necessárias para proteger o direito da personalidade, medidas referentes a sigilo e anonimização. Caso isso não seja respeitado e dados não anonimizados e coletados com finalidades estatísticas sejam compartilhados para execução administrativa, o direito à autodeterminação seria violado de forma inadmissível (Deutschland, 2022).

Ficando claro a intenção em consignar que o direito à autodeterminação informativa garante o poder ao indivíduo para que esse tenha controle sobre a coleta e tratamento de seus dados, agindo também como direito objetivo no âmbito privado, devendo ser levado em consideração pelos juízes na análise do caso concreto. Dessa forma, não vale apenas na relação do indivíduo com o Estado, mas também nas relações horizontais e nesse sentido outra decisão do mesmo Tribunal Constitucional Alemão, no ano de 1991, decidiu em um caso de locação de imóvel, em que o locatário não revelou sua interdição, pela autodeterminação informativa, já que poderia haver

consequências prejudiciais ao locatário, que poderia passar por rotulação social e ter dificuldades para alugar uma moradia (Mendes, 2020).

3.1.2 Consentimento informado um prelúdio a autodeterminação informativa?

Dentro do espectro da autodeterminação informativa, ao se retornar ao Código Civil e ao capítulo anterior, é importante registrar a construção do consentimento informado, existindo uma linha de conexão entre os dois termos. E por que é relevante essa digressão referencial, porque o consentimento informado é também substância que permeia e autoriza o tratamento de dados dentro da Lei 13.709/2018.

Assim, os bases da compreensão do consentimento informado construídos dentro da garantia à integridade física nos direitos da personalidade, são perfeitamente transportados para proteção dos dados pessoais. E não se estranhe essa interconexão, no direito é comum esse intercambiamento, a exemplo da construção jurisprudencial da ação rescisória no direito processual do trabalho que foi sendo apropriada pelo processo civil, quando a regra era o inverso.

Nesse sentido, o que se observa é que o consentimento/autordeterminação através de formulário padrão ou tácito, genérico por natureza, não afasta o dever de indenizar e as responsabilidades acessórias, já que não se perfaz com o mesmo a informação leal e concreta, uma vez que a autodeterminação só se torna juridicamente efetiva se for específica e delimitada.

3.2 Autodeterminação informativa a partir da Lei 13.709/2018

O direito à autodeterminação informativa exige uma base constitucional que possibilite o conhecimento pelo cidadão, de forma clara e reconhecível, dos pressupostos e da extensão das limitações, atendendo ao princípio da transparência (ou clareza normativa) do Estado de Direito (Schwabe, 2005, p. 237-239).

As primeiras referências a autodeterminação informativa surgiram em duas decisões paradigmáticas do Supremo Tribunal Federal (STF), fazendo menção explícita à relação umbilical entre as garantias constitucionais da liberdade individual, da privacidade e do livre desenvolvimento da personalidade (artigo 5°, *caput* e incisos X e XII) e a lei de n. 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), que

positivou o princípio em seu artigo 2°, inciso II. Nesse sentido, seguiu a linha do Tribunal Constitucional Federal alemão, que, em 1983, consagrou a autonomia do referido princípio ao declarar a inconstitucionalidade da Lei do Censo alemã.

A primeira decisão estabeleceu o princípio da autodeterminação informativa na Ação Direta de Inconstitucionalidade nº 6.387, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) em face da medida provisória nº 954/2020, que estabelecia o compartilhamento de dados dos usuários do serviço telefônico fixo e móvel pelas empresas prestadoras de serviço com o Instituto Brasileiro de Geografia e Estatística (IBGE) (Brasil, 2020a). Nesse caso, o princípio da autodeterminação informativa foi utilizado na motivação apresentada no acórdão na quase totalidade dos votos apresentados pelos ministros da Corte Constitucional.

A segunda decisão, na Arguição de Descumprimento de Preceito Fundamental nº 722, interposta pela Rede Sustentabilidade, em face da atividade de inteligência do Ministério da Justiça e Segurança Pública na produção e disseminação do dossiê com informações de servidores federais e estaduais integrantes do movimento antifascismo (Brasil, 2020).

O acórdão do STF determinou a suspensão imediata das atividades do referido ministério que estabeleciam a produção ou o compartilhamento de informações pessoais sobre os servidores que integravam o movimento antifascista. No voto da ministra Rosa Weber, verifica-se a menção ao princípio da autodeterminação informativa como decorrente dos direitos de personalidade e cita-se:

> Com efeito, informações relacionadas à identificação – efetiva ou potencial – de pessoa natural, como as alegadamente contidas no documento em questão, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

Observa-se, que as decisões do STF vão além da mera menção: declara que a autodeterminação informativa decorre dos direitos de personalidade, como o direito à privacidade, trazendo como impacto a sua obrigatória observância a qualquer

regime informacional. Ou seja, os dados pessoais não são propriedade ou meros objetos de tratamento de dados em amplo sentido. Eles estão ligados à personalidade de seus titulares, pessoas naturais, de forma inalienável, gerando um rol de obrigações jurídicas para os atores econômicos, estatais e sociais que os tratem ou manipulem em qualquer dimensão.

A natureza autônoma ligada aos direitos de personalidade perpassa toda a decisão emitida pela Suprema Corte, o que, por si só, já mereceria análise em trabalho específico. Mas, para fins desta reflexão, são destacadas algumas passagens, entre elas a manifestação do ministro Luiz Fux (Brasil, 2020b, p. 8):

> A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), todos previstos na Constituição Federal de 1988.

No contexto nacional, muito embora a LGPD traga à autodeterminação informativa como um de seus fundamentos expressos no inciso II do artigo 2° (Brasil, 2018), e a sua promulgação tenha sido acompanhada de grande interesse por parte da sociedade, faz-se necessário afirmar que se trata de direito autônomo já consagrado pelo ordenamento jurídico nacional tanto na Carta Magna como na legislação infraconstitucional.

No voto do ministro Gilmar Mendes pode-se destacar a assimilação do processo ocorrido pela Corte Constitucional alemã, que se tornou o marco histórico do princípio da autodeterminação informativa. Cita-se (Brasil, 2020c, p. 13):

> Essa abertura da jurisdição constitucional à transformação tecnológica enquanto instrumento de preservação dos direitos fundamentais também é consolidada na tradição continental. No icônico precedente da Lei do Censo alemã de 1983, cuja análise será aprofundada neste voto, resta evidente que o avanço das técnicas de coleta e processamento de dados foi tomado como válvula de reconfiguração da proteção jurídica à personalidade. A decisão baseou-se principalmente no diagnóstico de que, a partir da coleta e cruzamento de dados do censo, “seria possível a criação de um quadro abrangente e detalhado da respectiva pessoa, um perfil de personalidade, mesmo na área íntima; o cidadão torna-se uma verdadeira ‘pessoa transparente’”.

Nestes termos, o princípio da autodeterminação informativa estabelece um critério de legitimidade jurídica para o tratamento de dados na contemporaneidade. Os diferentes atores, processos, tecnologias e regras organizacionais devem obrigatoriamente respeitar os limites desse princípio que reafirma a centralidade do indivíduo titular dos dados e das informações, afastando concepções que tratem os dados pessoais como meras commodities, objetos científicos ou meros dados estatísticos, entre outras concepções possíveis.

3.2.1. Dos dados na era digital a Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados - LGPD é sem dúvidas um grande marco na proteção de dados e no direito à privacidade de pessoas físicas, especialmente no meio digital, estando presente no ordenamento jurídico brasileiro desde 14 de agosto de 2018, com previsão inicial para entrar em vigor plenamente 18 meses após sua publicação.

Em face de alterações promovidas pela Lei 13.853/2019 (Lei que criou a Autoridade Nacional de Proteção de Dados - ANPD), seu prazo para vigência foi ampliado para dois anos, estando em vigor, dessa forma, desde 16 de agosto de 2020.

É de se destacar que, além de questões jurídicas, a demora para entrada em vigor da LGPD estava relacionada diretamente a todas as suas implicações econômicas. Afinal, a utilização de dados pessoais para fins de publicidade das redes é uma das principais responsáveis pelo sucesso de algumas das maiores empresas do mundo, especialmente Amazon, Apple, Facebook e Google, conhecidos como os ‘’Big Four’’ da tecnologia.

Todas essas grandes corporações, e muitas outras, trabalham com algoritmos capazes de entender o comportamento dos usuários e, a partir disso, enviar anúncios direcionados e específicos para eles. De acordo com Laura Schertel Mendes (2014), no século XX a economia era majoritariamente baseada na produção em massa, com bens padronizados, em grande quantidade e por baixo custo. No entanto, nessas primeiras décadas do século XXI vêm sendo observada uma mudança desse modelo para um marketing segmentado, com mercados investindo em produtos customizados, singulares e pautados na alta qualificação do mercado consumidor.

Desse modo, atualmente, temos a chamada publicidade comportamental, também conhecida por *behavior advertising*, justamente pelo fato de as empresas, especialmente no mercado digital, buscarem anúncios personalizados com base nos dados e comportamentos dos usuários da internet. Essa prática é possibilitada pela técnica *data mining*, ou mineração de dados, entendida por Mendes (2014) nos seguintes termos:

> Data mining, ou mineração de dados, é o processo pelo qual dados de difícil compreensão são transformados em informações úteis e valiosas para a empresa, por meio de técnica informática de combinação de dados e de estatística. Isso significa que, por meio de uma única tecla, empresas são capazes de unir e combinar dados primitivos de uma pessoa, formando novos elementos informativos (p. 204).

Dessa forma, o indivíduo no mundo digital é formado por dados, que formam um perfil a seu respeito. Com base em uma análise desse perfil, é possível entender suas decisões e traçar o seu perfil de consumidor, de modo a mostrar para ele majoritariamente anúncios personalizados e relevantes, aumentando o lucro das empresas envolvidas.

Para Bioni (2018) esse modelo explica o porquê de a ampla maioria dos conteúdos da internet ser ‘’gratuita’, destoando do padrão de consumo tradicional, no qual um produto ou serviço é oferecido em troca de uma prestação pecuniária. Enquanto Pinheiro (2021, p.91) afirma que: “Há uma expressão atual para retratar o modelo de riqueza da web que diz: se o serviço for gratuito, você não é o freguês, você é produto.”

Observa-se então, que nesse modelo, o produto é o usuário, enquanto a contraprestação é o fornecimento de dados. Dito de outro modo, paga-se o Facebook, por exemplo, informando data de nascimento, CEP, compartilhando localização ou simplesmente interagindo na rede social.

A autora Cathy O’Neil, no livro ‘’Algoritmos de Destruição em Massa’’ explica que hoje somos somados de todas as formas possíveis conforme estatísticos e matemáticos organizam como podem uma salada de dados, de nossos CEPs e padrões de navegação na Internet a nossas compras recentes. Muitos de seus modelos pseudocientíficos tentam estimar nossa credibilidade, dando a cada um de nós assim chamados e-escores (O’neil, 2021, p. 134).

Com esse modelo, como afirma, fica muito mais difícil, por exemplo, um jovem de origem humilde conseguir um empréstimo bom e justo para investir em seu próprio negócio. Além de todas as dificuldades, ele teria que ‘’carregar nas costas’’ o peso de ter nascido naquele determinado local. Não é difícil de imaginar, portanto, que essa forma de tratamento realizada por algumas instituições tende a aumentar ainda mais a desigualdade social e a marginalização de pessoas com menor poder aquisitivo.

Todas essas questões envolvendo os dados dos usuários levaram a elaborada a Lei Geral de Proteção de Dados, de modo a regulamentar os direitos do titular dos dados, o compromisso e as responsabilidades das empresas que trabalham com os dados, além de estabelecer diretrizes para determinar como sites e redes sociais devem apresentar sua política de privacidade.

3.2.2 A Regulamentação da Lei Geral de Proteção de Dados Brasileira

A Lei Geral de Proteção de Dados - LGPD estabelece “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, conforme o artigo 1º (Brasil, 2018).

O primeiro ponto importante é que a regra não vale apenas para o mundo digital, os dados pessoais impressos em um papel, por exemplo, também estão sob a égide da LGPD. Outro ponto importante é que a lei se destina à pessoa natural, isso é, à pessoa viva, dado o entendimento trazido pela no artigo 6º do Código Civil Brasileiro, que explicita que a existência da pessoa natural termina com a morte (Brasil, 2002).

A LGPD “assegura a integralidade da proteção à pessoa humana na medida em que consagra a obrigatoriedade do gerenciamento seguro do início até ao fim da operação que envolve os dados pessoais” (Sarlet, 2021). Referida lei traz, em seu artigo 5º, inciso X, uma lista de tratamentos que compreendem desde a coleta até a exclusão do dado pessoal, abarcando, assim, do nascimento até a morte do dado pessoal o controle pela LGPD, exceto se o tratamento não estiver no rol de excludentes previstas no artigo 4º da referida Lei (Brasil, 2018).

A autodeterminação informativa está presente no artigo 2º da LGPD como um fundamento desta lei, juntamente com outros como a dignidade, o livre desenvolvimento da personalidade, inviolabilidade da intimidade, honra e imagem, a livre iniciativa e a livre concorrência, por exemplo.

Registre-se o poder do titular de exercer o controle sobre seus dados pessoais, somado a pontos que resguardam a sua intimidade, liberdade e o desenvolvimento econômico e tecnológico tão presentes na Sociedade da Informação. Deve-se respeitar bases, princípios e dar possibilidade de os titulares exercerem os seus direitos, conforme explicitado na lei. Os dados podem ser utilizados, mas se faz necessário orquestrar este uso (Brasil, 2018).

O primeiro tema a se observar são os princípios previstos no artigo 6º, que regem o tratamento. Com base na doutrina de Flumignan e Flumignan (2020), tem-se como pontos centrais a Boa-fé: comportamento leal, correto e com probidade sobre o tratamento de dados pessoais; Finalidade: propósitos legítimos, devendo ser específicos, explícitos e informados ao titular. É o que se espera de resultado ao se tratar os dados pessoais; e Adequação: os tratamentos deverão ser adequados para alcançar a finalidade do tratamento.

Além desses princípios, os tratamentos devem seguir uma das bases legais previstas nos artigos 7º ou 11 da LGPD, a depender se os dados tratados são pessoais (artigo 7º) ou dados pessoais sensíveis (artigo 11), que são aqueles com maior poder de discriminação do titular. Conforme o artigo 5º, inciso II, são dados sensíveis os de “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico” (Brasil, 2018).

Nesse sentido, o tratamento de tais dados pode trazer perigo a liberdade, integridade, dignidade e até mesmo a vida das pessoas. Dado essa possibilidade, o legislador traz maior rigor sobre o uso desses dados.

As bases legais para o tratamento dos dados pessoais previstos no artigo 7º são o consentimento; cumprimento de obrigação legal; execução de políticas públicas pela administração pública; estudos por órgãos de pesquisa; para execução de contrato ou procedimentos preliminares para sua confecção; exercício regular de direito em processos judiciais, administrativo ou arbitral; proteção da vida ou incolumidade física do titular ou terceiro; tutela da saúde por profissional da saúde;

serviço de saúde ou autoridade sanitária; interesse legítimo do controlador ou de terceiros e para proteção de crédito.

O artigo 11 traz como suporte para o tratamento de dados pessoais sensíveis o consentimento; cumprimento de obrigação legal ou regulatório; execução de políticas públicas pela administração pública; estudos por órgãos de pesquisa; exercício regular de direito em contrato e processos judiciais, administrativos ou arbitrais; proteção da vida ou incolumidade física do titular ou de terceiros; tutela da saúde por profissional da saúde, serviços de saúde ou autoridade sanitária e garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação em sistemas eletrônicos (Brasil, 2018).

É a autorização do titular, substrato do consentimento e da relação voluntária por ele estabelecida, que faz presumir sua vontade pelo tratamento. Independentemente da autorização ou não do titular para realização do tratamento, o controlador deve observar os princípios, boas práticas e os direitos dos titulares. Tal estruturação é de suma importância, pois todos esses tratamentos devem ocorrer de forma transparente aos titulares e a sociedade.

Não se podendo esquecer que a privacidade e a proteção de dados é um direito da personalidade, imprescindível para a pessoa humana na Sociedade da Informação, permitindo a liberdade de se expressar, ter acesso à informação, de não ser discriminado em ambiente de trabalho ou qualquer outro. A exploração das informações seja em relações verticais entre Estado e particular como nas horizontais, entre empregado e empregador, devem observar as normas constitucionais e infraconstitucionais que reafirmam a dignidade da pessoa humana, conforme expresso no art. 3º, inciso III, da Constituição da República Federativa do Brasil de 1988.

Assim, a LGPD é aplicável a todos os entes públicos, com exceção no tratamento de dados pessoais realizados para fins exclusivos de (a) segurança pública; (b) defesa nacional; (c) segurança do Estado; ou (d) atividades de investigação e repressão de infrações penais, isentando o Estado desta responsabilidade (Brasil, 2018).

Por outro lado, quando se trata de empresa pública e sociedades de economia mista que explorem atividade que necessitem ter acesso a dados pessoais, a Lei se aplica integralmente, conforme disposto no artigo 24, com a ressalva de não se

sujeitarem às sanções pecuniárias que possam vir a ser impostas pela Autoridade Nacional de Proteção de Dados (ANPD), uma vez que não existe hierarquia entre os entes públicos (Peccicacco; Souza, 2021).

3.2.3 Da Autoridade Nacional de Proteção de Dados

Ainda dentro do arcabouço normativo da proteção de dados, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), para promover o aumento da privacidade e da proteção de dados no Brasil, sobretudo no tocante à fiscalização e efetividade da Lei Geral de Proteção de Dados. Por um momento ela compreendeu apenas como um mero órgão da Administração Pública Federal. Essa condição, por si só, gerou grande desvantagem para a ANPD, tendo em vista que ela não possuía uma completa independência administrativa e funcional, estando em condição de vulnerabilidade e podendo sofrer interferências, notadamente da União.

Essa realidade mudou quando a Mesa Diretora do Congresso Nacional promulgou no dia 26 de outubro de 2022 a Lei nº 14.460, que converteu a Medida Provisória nº 1.124/22 em lei ordinária. Essa nova lei manteve a competência e a estrutura organizacional, mas converteu a ANPD em autarquia de natureza especial, com autonomia administrativa e financeira. Atualmente a Autoridade Nacional de Proteção de Dados está definida no art. 55-A da Constituição Federal, o qual afirma que “Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.” (Brasil, 2018).

Neste ensejo, a ANPD passou a ter personalidade jurídica, além de seu próprio patrimônio, com funcionamento semelhante às agências reguladoras. Dessa forma, possuindo mais liberdade para trabalhar em prol da proteção de dados dos indivíduos, de forma muito mais autônoma em relação a pressões políticas.

Uma ampla autonomia orçamentária e jurídica fez-se extremamente necessária para uma atuação plena e eficiente da ANPD, o que a deixou forte na missão de dar efetividade a Lei Geral de Proteção de Dados. A autarquia passou a ter mais liberdade para requerer relatórios de impacto de controladores, de modo a assegurar o cumprimento das medidas necessárias para proteger o tratamento de dados dos usuários.

Com independência se permite que se aprimore o consentimento dos usuários, com melhor fiscalização de cláusulas obscuras de contratos, dando mais contexto ao consentimento, uma vez que o consentimento muitas vezes é coletado de maneira formal, supostamente seguindo os padrões da LGPD, mas eivados de vícios, onde apenas uma análise do contexto possibilita entender se aquele consentimento foi dado de forma totalmente ciente ou não.

Sendo assim, formou-se o tripé da proteção de dados no Brasil. O primeiro ente é o próprio titular, resguardado pela própria LGPD como dotado de autodeterminação informativa devido ao poder do seu consentimento. O segundo seria as empresas, com técnicas de *privacy by design*, *risk analysis e accountability* que as tornarão também uma parte ativa da busca pela privacidade e proteção de dados no Brasil, trabalhando desde a concepção e analisando os riscos e assumindo responsabilidades para proteger esses direitos fundamentais. E em terceiro a Autoridade Nacional de Proteção de Dados, que trabalha com autonomia e independência para fiscalizar os controladores, requerer os relatórios de impacto e cuidar com mais eficiência dos dados de todos os brasileiros.

3.3 Autodeterminação informativa na formação dos bancos de dados

Como já se percebeu, a coleta de dados se tornou comum apenas no século XX, as legislações sobre proteção de dados, como não poderia ser diferente, bastante escassas. As primeiras ocorreram apenas na década de 70, em decorrência da necessidade de regulamentação por conta da introdução do processamento eletrônico de dados nas empresas privadas e nas administrações públicas em parte da Europa e nos Estados Unidos.

Assim, surgiram leis em diversos países, como Suécia e Alemanha. A autora Mendes (2014) analisou bem a situação:

> São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o Fair Credit Reporting Act (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o Privacy Act (1974), aplicável à administração pública. (p.45)

Verifica-se, que essas legislações foram específicas para regular a coleta e o tratamento de dados que ocorriam nessas corporações, mas não havia ainda a ideia consolidada de um direito fundamental à privacidade.

Contudo, ainda na década de 70 começaram a surgir os primeiros dispositivos constitucionais que versavam sobre a proteção de dados. Os grandes marcos foram a Constituição Portuguesa de 1976 e a Constituição Espanhola de 1978. O artigo 35 da Constituição Lusa abordou sobre a proteção de dados nos três termos, onde o primeiro todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização. O segundo a informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. E o terceiro era proibida a atribuição de um número nacional único aos cidadãos.

Como se observa, a ideia de um direito à proteção de dados foi bem introdutória, se limitando a aspectos bem específicos. Com o passar dos anos, o desenvolvimento da proteção de dados se deu mais por decisões específicas de tribunais europeus, que buscavam tutelar esse direito de forma pontual.

Mais uma vez registramos, que uma das mais célebres decisões ocorreu em 1983, no Tribunal Constitucional Alemão, que declarou a inconstitucionalidade da Lei do Censo no país, reafirmando que os indivíduos têm direito à autodeterminação informativa, defendendo a ideia do controle do indivíduo no processamento dos seus dados.

Porém, o grande marco da proteção de dados na Europa ocorreu com a assinatura do Regulamento Geral sobre a Proteção de Dados (RGPD), ou General Data Protection Regulation (GDPR), assinado em 14 de abril de 2016 e implementado em 25 de maio de 2018. Com ele, foi efetivada em solo europeu a proteção de dados dos habitantes da União Europeia, que passaram a ter um código completo versando sobre princípios, diretrizes, direitos e deveres para o tratamento e a regulação de dados.

No Brasil, como já mencionamos o marco referencial veio com a implementação da Lei Geral de Proteção de Dados, bastante semelhante com a

RGPD, e busca conferir maior segurança para o tratamento de dados realizado no território nacional.

Quando nos referimos a proteção dos bancos de dados, por sua vez, no Brasil as previsões legislativas específicas para a proteção de dados já se encontravam incertas na Lei 8.078/90, o Código de Defesa do Consumidor, onde a regulamentação dos bancos de dados e cadastros de consumidores estava presente no artigo 43. Além disso, há a regulamentação do chamado cadastro positivo pela Lei 12.414/2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Para a doutrina a proteção da privacidade dos dados por meio da concepção da autodeterminação informativa podia ser extraída da cláusula geral prevista no artigo 21 do Código Civil, conjugada com aquela de responsabilidade objetiva contida no artigo 187 do mesmo diploma legal e com os princípios do consentimento e da confiança. Segundo Cachapuz (2006), o debate sobre a privacidade envolve o reconhecimento de uma autodeterminação informativa a toda pessoa e permite que se discuta, não apenas em que medida pretende o indivíduo participar de uma vida comum, compartilhando experiências tecnológicas, mas, inclusive, com que extensão também é possível ao indivíduo expressar seu desejo de aparecer e de fazer-se visto pelos demais.

Registre-se, nos debates sobre proteção de dados pessoais, o direito à autodeterminação informativa representa uma das expressões mais renomadas. O conceito não fez apenas uma “carreira brilhante” (Bull, 2011, p. 25) na Alemanha, como também influenciou diversos ordenamentos estrangeiros, tendo sido inclusive incorporada como um dos fundamentos da Lei Geral de Proteção de Dados brasileira (art. 2º, II).

Entender sua evolução é tarefa essencial para bem compreender tanto o seu núcleo fundamental quanto seus contornos e releituras. Ademais, a análise da jurisprudência do Tribunal Constitucional, no tocante à forma como terceiros lidam com dados e informações, pode fornecer esclarecimentos sobre características importantes da proteção de dados em geral.

Pode-se afirmar que o direito à proteção de dados pessoais não se concretiza sem os direitos à privacidade e à autodeterminação informativa. Os direitos

mencionados constituem parte imprescindível de qualquer sistema de proteção de dados pessoais, e atuam em mútuo reforço.

O indivíduo, na sociedade contemporânea, perde facilmente a centralidade de sua existência no emaranhado e no intenso fluxo de dados e informações. Torna-se incapaz de dar sentido à sua própria existência, de ter domínio sobre as suas próprias experiências, ao perder o controle total de como é visto e entendido (Davenport, 2014). As novas tecnologias e os artefatos que vêm com ela têm influenciado e reconfigurado o ambiente organizacional, assim como a privacidade das pessoas e as relações que elas estabelecem entre si (Zuboff, 2019).

Esse novo contexto social, que engloba diferentes relações e interações por meio de mídias e dispositivos digitais interconectados, é o que se chama de capitalismo de vigilância, termo proposto por Zuboff (2019). O conceito de capitalismo de vigilância é representado por um sistema tecnológico, que integra indivíduos, suas relações e seus comportamentos, mediado por plataformas digitais, que, posteriormente, são gerenciadas por algoritmos (Kellogg; Valentine; Christin, 2020).

Grandes organizações que atuam com serviços digitais acabam exercendo poder pela forma com que fazem a gestão e se relacionam com outros atores, a exemplo dos usuários, com outras organizações e também com o Estado. Isso ocorre pelo fato de elas coletarem diferentes tipos de dados, oriundos de comportamentos e interações nas redes sociais (Leonardi; Treem, 2020). Dessa forma, o indivíduo, entendido como pessoa natural, torna-se objeto dos tratamentos de dados, e as dimensões de sua vida e personalidade são absorvidas nesse fluxo informacional como dados.

Neste sentido, devido a esta nova configuração, a resposta das instituições típicas do Estado moderno, como o Parlamento e o Judiciário, foi a institucionalização do princípio da autodeterminação informativa. Uma tentativa de proteger o indivíduo no contexto atual de produção informacional caracterizado pelo capitalismo de vigilância, que o objetifica e que invade o núcleo de sua personalidade, cujas consequências ainda não são totalmente conhecidas.

O princípio da autodeterminação informativa é uma reação da matriz axiológica, típica da modernidade, aos processos de objetificação do ser humano produzidos pelos diferentes regimes informacionais estabelecidos por atores econômicos e estatais. Esse princípio se constitui numa proteção dinâmica das dimensões da

personalidade do ser humano, atribuindo-lhe, na dimensão jurídica, o controle sobre as suas próprias informações (Rodotá, 2008), transcendendo a dicotomia entre o público e o privado, ao mesmo tempo que institui um parâmetro axiológico e avaliativo para a análise dos regimes de informação estabelecidos.

3.4 Autodeterminação informativa no novo modelo de negócios

Como já observamos, quando as empresas estabelecem um novo modelo de negócios focado na captação e compartilhamento de dados pessoais, a autodeterminação informativa ganha relevância.

Patrícia Verônica Nunes Carvalho Sobral de Souza e Ronaldo Batista Dória, porém, alertam que:

> "Diante da problemática do comércio de dados pessoais, Tannner (2013) salienta de forma crítica que, em relação ao consentimento do titular e a autodeterminação informativa, os sistemas de 'termos de uso' ou 'aceite de uso' de determinadas ferramentas digitais, são propositalmente redigidos de forma complexa e extensa, conduzindo os usuários ao desconhecimento das suas cláusulas e possibilitando, ainda, que a mesma aceitação, sem a devida ciência do seu inteiro teor pelo usuário, autorize o uso e coleta irrestrita de dados, sem nenhum vínculo com o serviço em questão, para fins ilegítimos como a transação de dados, sob justificativa de que o titular teria inserido os dados 'por livre e espontânea vontade'.

Nesse mesmo sentido, Sadowski (2016) registra que quando as empresas buscam consentimento do titular dos dados é por meio de termo de acordos de serviço, contratos excessivamente longos repletos de linguagem jurídica densa com a qual os usuários devem "concordar" sem entender, o que implicaria, consequentemente na autodeterminação informativa.

Verifica-se assim, que a forma de consentimento obtida para o tratamento dos dados, por sua vez, não sobrevive a uma análise de validade e eficácia do negócio, dentro das dimensões do negócio jurídico, principalmente quando nos referimos a vontade desembaraçada, longe de qualquer possibilidade de conversão substancial[2].

---

[2] É que para o consumidor ter acesso aos descontos nas compras junto a RaiaDrogasil, descontos que ultrapassam os 40% (quarenta por cento), é condição *sine qua non* o fornecimento de CPF válido, o que torna a voluntariedade do consumidor uma simulação, uma vez que ninguém em sã consciência deixaria de sucumbir a essa exigência em face da percentagem absurda de "desconto no preço", como afirmou o próprio CEO ao mencionar que 97% (noventa e sete por cento) dos clientes fornecem "voluntariamente" o CPF no momento das compras.

A validade da manifestação de vontade sofre mitigação com interesse comercial e a agressividade das empresas, fato que preocupa os pesquisadores quanto a abrangência e efeitos da manifestação de vontade nos contratos eletrônicos com vistas ao tratamento de dados. Afirmar que o cliente anuiu tacitamente na alienação ou disponibilidade de seus dados pessoais quando forneceu seu CPF, é um esforço interpretativo que não se justifica, uma vez que a norma é expressa ao afirmar que a presunção é limitada e restrita ao propósito da capitação.

Outra contradição no discurso, é afirmar anonimizar as informações quanto a individualização dos dados, e ao mesmo tempo confirmar que o eventual parceiro comercial que adquirir esses dados, saberá a quem direcionar os anúncios.

O texto da Lei nº 13.709/2019, alerta para a reversão, identificação, como empecilho a consideração dos dados como anomizados:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
>
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
> § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Observa-se que as implicações desse tipo de conduta não se restringem a um simples descumprimento expresso de lei civil, o que por si só autorizaria o Estado a determinar sua conformidade de fato, mas tem repercussões no Código Civil, Código de Defesa do Consumidor, Código Penal e na legislação administrativa. O gerenciamento de dados que confronta com a previsão expressa da Lei nº 13.709/2018, não se traduz em mera ilegalidade, mas violação a direitos fundamentais constitucionalmente assegurados.

Essa apropriação de dados, fez acelerar a percepção de que sua proteção não se satisfaz apenas com o dever geral de abstenção, exigindo-se uma atitude mais ativa, de caráter positivo dinâmico. Como afirma o autor, “os dados pessoais não podem ser tratados como bens patrimoniais, que, uma vez fornecidos, podem ser

livremente utilizados pelo destinatário ou retransmitidos para quem quer que seja.” Principalmente quando se considera que o fornecimento desses dados se torna condição sem a qual o consumidor não tem acesso ao produto.

Ressaltando assim, que aquele que faz a captação de dados assume pouca responsabilidade pela segurança da informação que coleta e nenhuma pela maneira como as demais empresas com as quais compartilha esses dados farão uso. Criando-se um mecanismo de sucessivos compartilhamentos, dissipando-se as responsabilidades a ponto de tornar-se o mais difícil possível identificar a cadeia de responsabilidades.

Com bem já se registrou, na era do *big data,* a ordem é coletar o máximo de dados que se conseguir antes mesmo de saber se tais informações serão úteis. Isso porque esses dados podem ser tratados de forma a auxiliar a tomada de decisão, bem como serem submetidos a procedimentos que podem agregar bastante valor às organizações empresárias (Zanatta, 2015).

Neste sentido, não raramente essas organizações criam mecanismos diversos para coletarem os dados pessoais, seja obrigando os indivíduos a fornecerem uma quantidade demasiada e desnecessária de dados para poderem concluir uma relação contratual, seja coletando por meio de tecnologias da internet como os *cookies*, o que muitas vezes acontece sem o conhecimento do titular desses dados.

Dessa forma, a economia, aproveita-se do fenômeno do *big data*, fazendo surgir novos modelos de negócios, que coletam e tratam estes dados. Essa nova economia se caracteriza por ser um ambiente no qual ocorrem rápidas transformações e surgem novos tipos de negócios, mas, a principal característica é a quantidade de informações disponíveis para processamento (Cohen, 2002, p. 26).

O desenvolvimento desse novo modelo de negócios, todavia, traz ao centro do debate a questão da violação à privacidade dos indivíduos cujos dados pessoais são utilizados como insumo, de modo que aos governos nacionais põe-se o desafio de sopesar desenvolvimento econômico e proteção à privacidade, buscando instrumentos capazes de permitir crescimento econômico e minimizar os impactos sobre a privacidade (Adjei, 2015, p. 01).

Na atualidade, como já se pode perceber, o direito à privacidade tem sua compreensão ampliada em razão exatamente da evolução das formas de divulgação e apreensão de dados pessoais ter expandido as possibilidades de violação da esfera

privada, máxime pelo acesso não autorizado de terceiros a esses dados. Dessa feita, a tutela da privacidade alarga seus contornos tradicionais de “direito a ser deixado só” ou “direito de ser deixado em paz” para apresentar-se também como o direito de manter o controle sobre as próprias informações (Schereiber, 2014, p. 137).

E esse é desafio de nossos tribunais, sopesar toda essa evolução da proteção a personalidade, à privacidade dos dados e banco de dados, na construção de referenciais que possam ser mais claros e objetivos, dentro da realidade social se apresenta.

Como no uso de dados pessoais de núcleo mais sensível, por exemplo histórico trabalhista, orientação política, sexual e religiosa, e o seu armazenamento em bancos de dados informatizados que abre margem para a descoberta de diversos aspectos sobre a intimidade dos cidadãos. Esse risco é potencializado ainda mais quando eles são relacionados, no que são chamados bancos de dados cruzados, permitindo que o detentor dessas informações possa utilizá-las de forma comercial (Doneda, 2020).

Como se observa, a primeira insuficiência enfrentada pelo paradigma do consentimento advém de sua abordagem quanto ao próprio titular dos dados e seu processo cognitivo decisório. É que, sob tal ótica, esse indivíduo é guiado pela maximização de seus interesses em face dos custos e benefícios envolvidos em consentir, ou não, com os termos que lhe são apresentados. Assim, caso esteja munido de amplo conhecimento acerca do que é feito com seus dados pessoais, poderá sopesar os custos envolvidos para sua personalidade e contrapô-los em face dos benefícios trazidos, por exemplo.

Dessa forma, torna-se necessário: (i) informar o titular dos dados pessoais acerca de quais dados estão sendo coletados e como eles serão usados (*notice)*; em seguida, (ii) permitir com que ele detenha o poder de decidir se aceita, ou não, os referidos usos de seus dados pessoais (*consent*) (Solove, 2013, p. 1883). Com base nas informações disponibilizadas pressupõe-se que o indivíduo está apto a tomar decisões racionais, embasadas e efetivamente autônomas.

A segunda insuficiência vivenciada pelo paradigma do consentimento advém da desconsideração da assimetria de poderes existente na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados (Mendes, 2014). É que, sob essa perspectiva, o consentimento do indivíduo se apresenta como base legitimadora para praticamente toda a operação de tratamento de dados,

independentemente das assimetrias existentes quanto ao poder de barganha das partes, o que poderia prejudicar a tomada de uma decisão realmente livre e autônoma.

Não raras vezes, o titular dos dados pessoais se encontra em situação de vulnerabilidade nessa relação contratual eletrônica (Marques; Miragem, 2012, p. 117). Primeiro, pois, como já dito, os termos das políticas de privacidade podem ser demasiadamente complexos e abstratos, impossibilitando uma compreensão mais transparente a respeito do concreto emprego dos dados. Segundo, porque vários desses termos negociais se baseiam em uma lógica binária "*take it or leave it*": consentir ou não consentir, sem outras opções. Porém, ao não consentir, o custo é o de não desfrutar o serviço almejado, v.g., o uso de uma rede social ou de um aplicativo online (Balkin, 2018, p. 3).

Evidencia-se então, que mesmo estando exposto a tamanhos riscos, o titular dos dados pessoais pode acabar realizando seu consentimento com base em proveitos tais como: a conexão com suas amizades, a disponibilidade de meios de comunicação em tempo real, a possibilidade de ouvir músicas e assistir filmes etc. Assim, muitas vezes esse consentimento é meramente aparente (Schwenke, 2006, p. 58), sendo questionável sua contribuição para o objetivo de proteger o titular dos dados, coloca-se em dúvida o grau concreto pelo qual ele reflete a autonomia decisória desse titular.

A terceira insuficiência de uma visão centrada no consentimento advém de sua menor capacidade em oferecer respostas aos desafios decorrentes da "massificação da produção, coleta, armazenamento, tratamento e compartilhamento de dados pessoais" (Queiroz; Ponce, 2020, p. 75). Apesar do nome sugestivo, a proteção de dados não se volta exclusivamente aos dados em si. O seu enfoque protetivo está no titular desses dados: quem arcará com os riscos e com as eventuais consequências prejudiciais do uso de seus dados pessoais.

Nesse sentido, percebe-se que o papel regulatório é mais amplo: disciplinar a informação gerada a partir do processamento e do tratamento dos dados pessoais, em um devido contexto (Albers, 2014, p. 222), uma vez que são essas informações extraídas a partir desses dados, e não eles próprios, que formarão a representação virtual do indivíduo na sociedade.

Porém, essa regulação não consegue acompanhar o dinamismo dos processos. Dados considerados "irrelevantes" ou "públicos" como idade, altura,

nacionalidade, os locais de moradia e de trabalho podem servir de insumo para correlações, predições e ranqueamentos acerca da personalidade do titular dos dados pessoais ou de determinados grupos sociais (O'neil, 2018). Essas possuem a capacidade prática de determinar "a vida das pessoas: desde a seleção de currículos para uma vaga de emprego, chegando até os seguros, acesso ao crédito e serviços do governo" (Teffé; Medon, 2020).

A criação de detalhados perfis a respeito dos cidadãos pode criar sérios riscos à sua personalidade na medida em que essas representações virtuais têm o condão de diminuir ou de aumentar oportunidades sociais "em aspectos centrais da vida humana" como "emprego, moradia, crédito, justiça criminal" (Queiroz; Ponce, 2020, p. 81-82), justamente de acordo com a classificação ou o score conferido ao seu perfil.

Em viés mais positivo, o uso desses dados transformados em conhecimento permite empreender com mais eficiência no mercado, produtos ficam melhores, o tratamento do cliente fica mais personalizado e a abordagem publicitária se torna mais efetiva, além do fortalecimento de influência de pessoas e marcas.

O que possibilita a melhora na qualidade de vida quando se consegue perceber que a análise adequada desses dados pode revelar padrões, tendências e associações que podem ser usados para gerar novas hipóteses, orientar a tomada de decisões clínicas e informar políticas de saúde. Sendo usados para várias aplicações, como prever surtos de doenças, desenvolver tratamentos personalizados, otimizar a eficiência operacional e melhorar a tomada de decisões estratégicas. Sem esse tratamento, muitos dos dados coletados em experimentos laboratoriais, ensaios clínicos e estudos observacionais seriam inúteis ou, pelo menos, subutilizados.

Como se percebe, não se trata de limitar todo e qualquer tipo de tratamento de dados. Ao revés, cuida-se de avaliar sua capacidade para efetivar essa proteção a partir do contexto particular em que inserido. Em um mundo marcado pela tecnologia do *Big Data*, muitas inovações tecnológicas positivas decorrem justamente dessa habilidade de "reutilizar uma mesma base de dados para propósitos diferentes" (Bioni, 2019, p. 317).

Muhlbauer (2019) aponta para a falta de conhecimento e interesse dos usuários quanto ao tema, ou seja, eles "não sabem quais são os limites da privacidade digital. É o tipo de anuência que se dá, sem convicção e clareza, com um check 'Concordo' ou 'I agree' como se estivesse no escuro".

Esse problema não se limita as redes sociais e a conteúdo postado, a autora cita como exemplo o Google que, apesar de todas as críticas que recebe, pode ser considerado uma referência em termos de orientar os seus clientes sobre o conteúdo de termos e condições aceitos, fornecendo informações que facilitam a compreensão de termos técnicos e possíveis nuances de sua Política de Privacidade (Muhlbauer, 2019).

Por outro lado, a adoção do critério do risco integral constitui uma modalidade extremada da doutrina do risco, pois a imputação de responsabilidade ao agente dispensa até mesmo a existência do nexo causal. A obrigação de indenizar resulta da mera ocorrência do dano, ainda que presente, no caso, culpa exclusiva da vítima, fato de terceiro, caso fortuito ou força maior. Esta teoria somente é aceita em casos extremos, não havendo grande repercussão no âmbito do direito privado (Cavalieri Filho, 2010, p. 144-145).

Sendo mais razoável na análise das condutas, a licitude dos atos. Os atos ilícitos, ao contrário dos atos lícitos, são proibidos por lei, direta ou indiretamente. Por isso, a prática de ato ilícito gera o direito ao ofendido à indenização por dano moral ou material. O artigo 927, do Código Civil, dispõe que “Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo”. Logo, o ilícito cria um dever de reparação ao agente e um direito subjetivo à reparação aos ofendidos (Stankevecz; Baracat, 2025).

Porém, essa é uma discussão que tem que ser aferida nas manifestações de nossos tribunais, uma vez que há argumentos consistentes estando a favor como contra uma maior limitação da capitação e destinação dos bancos de dados, com extensas manifestações doutrinárias como se pode perceber até aqui.

Com o desenvolvimento exponencial da tecnologia e o crescente dinamismo das relações sociais exsurgiram novos e imensuráveis riscos. Nesse contexto não é possível, tampouco desejável a criação de uma doutrina estática e completa para solucionar todos os problemas relacionados à responsabilidade civil. Assumir a existência do dano e responsabilizar o seu autor é o primeiro passo em direção a um sistema realmente comprometido com a precaução e a prevenção de danos Bergstein e Marques (2017).

4. Tendências jurisprudenciais que se desenham em nossos tribunais superiores quanto exploração de dados pessoais, compreensão dos limites do tratamento

Estabelecido um corte referencial a partir da vigência da Lei nº 13.709/2018 até fevereiro de 2025, é possível observar no Supremo Tribunal Federal e Superior Tribunal de Justiça manifestações que introduzem em nossos tribunais as tendências decisórias quanto à autodeterminação informativa e tratamento de dados em face desse novo modelo de negócios que tem como objeto os dados pessoas.

Tais manifestações, porém, tendem a repetir o texto normativo sem aprofundar na análise, fazendo uso de uma interpretação mais positivista, em detrimento do estabelecimento de alguns paradigmas interpretativos sensíveis, como se verá mais adiante.

4.1 Da realidade factual objeto da discussão

Quando se verifica que a evolução conceitual de Direito da Personalidade e seu viés da autodeterminação informativa com vistas a proteção de dados pessoais, têm suas bases na jurisprudência alienígena ainda na primeira metade do século XX, não se espera que no século XXI, modelos de negócio focados em dados pessoais encontrem pouco amadurecimento jurisprudencial.

A origem das considerações postas neste trabalho tem referência exatamente nessa realidade, a princípio em reportagens veiculados nos meios de comunicação, inicialmente no sítio eletrônico UOL, dando conta desse modelo de negócios e em outras notícias anteriores onde já se estabelecia essa forma de exploração econômica.

4.1.1 RaiaDrogasil

No ano de 2023, foram veiculadas pelo site UOL duas reportagens onde se noticiava a exploração econômica de dados de clientes pela rede de farmácias RaiaDrogasil.

Segundo afirma a reportagem, a referida rede de farmácias armazenou e

continua armazenando por mais de 15 anos, registros de hábitos de consumo de seus clientes (histórico de saúde, comportamento sexual etc), através da exigência de CPF para oportunizar descontos nos preços, ultrapassando os 48 milhões de clientes registrados, com uma projeção de que uma em cada cinco pessoas da população brasileira tenha seus registros junto a referida empresa[3].

A captação de dados, segundo informou o CEO da empresa a reportagem, iniciou-se ainda no ano de 2006, porém, seu tratamento com esse objetivo se deu a partir do ano 2017, intensificando-se a partir de 2021. Para o CEO da RaiaDrogasil a monetização desses dados de hábitos de consumo é possível em face da "autorização", aceite da política de privacidade - que os clientes firmam no momento do fornecimento de seus CPFs em troca de descontos, o que ocorre em 97 % das compras.

Para o consumidor ter acesso aos descontos nas compras junto a RaiaDrogasil, descontos que ultrapassam os 40% (quarenta por cento), é condição *sine qua non* o fornecimento de CPF válido, o que torna a voluntariedade do consumidor questionável.

Em poder dessas informações, afirma à reportagem, a RaiaDrogasil criou uma subsidiária no ano 2021, a RD Ads, com o único objetivo de auferir lucro com esses dados junto as indústrias e agências de publicidade, traduzindo-se em uma nova fonte de receita.

Ou seja, criou-se uma empresa apenas para comercialização de dados pessoais obtidos sem autorização expressa para esse fim, transferidos por outras pessoas jurídicas, cujo objeto social originário também não previa a transferência de dados.

Observa-se que se trata de manipulação de dados conceitualmente sensíveis, como histórico de saúde e comportamento sexual, dados estes previstos na Lei Geral

---

[3] www.uol.com.br. Disponível em: https://www.uol.com.br/. ROSSI, Amanda. **Vitamina usada para tentar engravidar pode direcionar até anúncio de carro**. São Paulo, SP, [2023]. Disponível em:https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2023/09/01/remedio-para-engravidar-pode-direcionar-ate-propaganda-de-carro.htm. Acesso em: 01 setembro 2023.

www.uol.com.br. Disponível em: https://www.uol.com.br/. ROSSI, Amanda. **Ministério da Justiça notifica RaiaDrogasil após reportagem do UOL**. São Paulo, SP, [2023]. Disponível em: https://economia.uol.com.br/noticias/redacao/2023/10/23/ministerio-da-justica-notificaraiadrogasil-apos-reportagem-do-uol.htm. Acesso em: 23 outubro 2023.

de Proteção de Dados Pessoas – LGPD – Lei nº 13.709/2018 de autonomia privada limitada e específica, nunca genérico ou indefinido no tempo.

Coincidentemente no Brasil, esse novo modelo de negócios se estabeleceu de forma clara e objetiva concomitante com a advento da Lei nº 13.709/2018. Afirmação que fazemos corroborada pela veiculação das reportagens onde se noticia pela primeira vez a intenção de monetização de dados de clientes pela rede de farmácias RaiaDrogasil.

4.1.2 Antivírus Avast e Imagens Faciais

Ainda no ano de 2020, o sitio eletrônica Agência Mestre alertava para a venda de dados pela empresa do Antivírus Avast a uma subsidiária chamada Jumpshot e a formação do banco de dados criado por aplicativo de imagens faciais.

No caso do Avast, entre outras empresas que comercializam dados, alertava-se que elas faziam a captação de informação por meio da instalação de um software por parte do usuário, seja uma extensão do navegador ou um programa em seu computador, onde havia uma cláusula que perguntava se a empresa poderia usar as suas informações. Existindo a concordância, a empresa vai salvaria em um banco de dados todo o seu histórico de navegação, sob o argumento de descaracterizar sua identidade/anonimização.

Ocorre, que uma outra companhia conseguiu a regressão dos dados e a identificação de algumas variáveis que não deveriam estar acessíveis, como idade, sexo e localização aproximada das pessoas, o que levou ao fechamento da subsidiária Jumpshot, porém, com manutenção do vasto banco de dados.

Outra situação de exposição de dados, segundo informa, ocorreu com a disseminação de um aplicativo que ficou bem conhecido por pegar uma foto e transformar seu rosto para uma versão mais velha.

Os dados eram armazenados em servidor externo, formando, segundo noticia, um dos maiores acervos de rostos do mundo, com possibilidade de reconhecimento de rostos maior inclusive que organizações como CIA e FBI, abrindo a oportunidade para vender as informações para empresas que trabalhavam com estética por exemplo, possibilitando a segmentação do público para o melhor tratamento de beleza para cada lugar do mundo.

E projetava: “Pode parecer teoria da conspiração, mas um fato, é que os próximos anos o público terá que embarcar em grandes brigas por privacidade. Então, cuidado com suas informações. Elas são só suas”.[4]

4.1.3 Vivo

Em abril de 2020, no Brasil, reportagens investigativas já alertavam para a fragilidade da anonimização de dados como processo irreversível.

Segundo a reportagem veiculada no intercept.com.br, ao ter acesso a uma planilha vendida pela Vivo à Secretaria de Turismo do Espírito Santo, foi possível identificar em mais de uma oportunidade os autores dos dados supostamente anonimizados. Onde afirma:

> “Cliente da Vivo, maior operadora de celular do Brasil, Rocha não imaginava que seu celular, monitorando seus movimentos, estava também produzindo dados que a empresa, depois, transformaria em dinheiro”.

Argumentando ainda que na planilha vendida em 2017 ao governo do Espírito Santo, Rocha não é exatamente Rocha. É um indivíduo não identificado, homem, idade entre 50 e 59 anos, que vive em Domingos Martins, cidade de 33 mil habitantes, e vai esporadicamente a Santa Maria de Jetibá, que tem 40 mil habitantes. Pertence à classe B e é classificado como integrante de ‘famílias populares’, uma categoria criada pelo estudo para definir a típica família brasileira de classe média.

Esses dados, segundo a empresa, seriam anonimizados e organizados nos chamados clusters comportamentais, que agrupam as pessoas segundo suas características sociodemográficas onde vivem, quanto ganham e como consomem.

Segundo ainda a reportagem, a compilação de dados do Espírito Santo, feita em 2016 e 2017, rendeu à Vivo R$ 625 mil. A planilha detinha informações pessoais de milhares de pessoas não identificadas, mas combinadas e cruzadas com outras bases, essas informações permitiam que se chegasse a perfis bem específicos e às detentoras dos dados. Concluindo que: ‘É fácil identificar indivíduos para fins

---

[4] www.agenciamestre.com. SOUZA, Daniele. **Guerra dos Dados – Empresas Vendem Seus Dados que São Usados em Marketing Digital**. [02.2020]. Disponível em: https://www.agenciamestre.com/marketing-digital/guerra-dos-dados-empresas-vendem-seus-dados-que-sao-usados-em-marketing-digital/. Acesso em: 01 de fevereiro de 2025.

discriminatórios e ilícitos, como perseguição de adversários políticos, golpes financeiros e manipulações eleitorais'.

Alertava ainda a reportagem, que a Lei Geral das Telecomunicações permitia que as operadoras divulgassem a terceiros 'informações agregadas sobre o uso de seus serviços' desde que elas não permitissem a identificação, direta ou indireta, do usuário, nem a violação de sua intimidade. Por sua vez, realizada na ocasião consulta a Anatel, a agência reguladora não viu nenhum problema na venda de informações, feita pela Vivo por meio do programa Smart Steps.

E registrava quanto à autodeterminação informativa:

> "Lá, nas letras pequenas do termo de adesão, os clientes autorizam, sem perceber, que seus dados de localização sejam cedidos a terceiros. A assessoria da Vivo diz que o uso das informações para "construção de soluções estatísticas" é feito por adesão voluntária (ou *opt in* no jargão tech). Mas, nas lojas da empresa, não é bem assim que funciona. Os vendedores não informam, e, ao preencher o termo com os dados do cliente, já costumam deixar marcada a caixa "eu concordo" para utilização de "dados pessoais e de localização e uso da rede". Perguntei à Vivo o que exatamente os clientes autorizavam, em que momento eles eram informados e o que estava escrito no contrato. A empresa se limitou a dizer que solicita o consentimento no momento da contratação."[5]

4.1.4 Drumwave

No ano de 2022, um sitio eletrônico ligado a XP Controle e Participações S/A, noticiava a seus leitores que a empresa Drumwave (fundada em 2015 em Palo Alto, na Califórnia, pelo colombiano Santiago Ortiz e pelos brasileiros Alberto Blumenstein e André Vellozo), startup que funcionava como uma espécie de cartório de dados digitais, teria lançado uma plataforma que permitia a consumidores e empresas negociarem a venda de seus dados.

Segundo noticiava, a startup reunia, certificava e precificava dados de consumidores detidos pelas empresas. Depois compilava essa massa de informações e entrega aos consumidores (seus donos originais) por meio de uma carteira digital.

---

[5] www.intercept.com.br. DIAS, Tatiana. **VIGIAR E LUCRAR Nós identificamos dois clientes dos dados de localização "anônimos" vendidos pela Vivo**. [04.2020]. Disponível em: https://www.intercept.com.br/2020/04/13/vivo-venda-localizacao-anonima/. Acesso em: 01 de fevereiro de 2025.

Estes, por sua vez, poderiam vender os dados a outras empresas interessadas por meio de agentes intermediadores. E explicava:

> “Por exemplo: um consumidor gera muitos dados ao acessar um site ou aplicativo de loja de roupas: que tipo de produtos pesquisa, tamanho, quantas vezes compra etc. A mesma coisa se repete na relação com bancos, farmácias, academias, entre outros, gerando informações que são úteis para que outras empresas possam desenvolver ou aperfeiçoar produtos e serviços, captar tendências de mercado, realizar customizações e por aí vai.

O serviço passaria a funcionar comercialmente no fim daquele mesmo ano no Brasil e no ano seguinte nos Estados Unidos. A escolha pelo Brasil teria sido motivada pelo tamanho da economia local e pelo gosto da população por novas tecnologias, segundo Teles. A carteira digital da Drumwave apareceria dentro de aplicativos de companhias que tenham uma quantidade relevante de clientes, de modo a massificar os conteúdos, tais como empresas de telecomunicações e bancos, por exemplo.

Tratava-se de uma aposta em um mercado embrionário, mas com potencial para movimentar globalmente US$ 1,8 trilhão de dólares no longo prazo, segundo o presidente da companhia, Fernando Teles[6].

4.1.5 Tools for Humanity

Em janeiro de 2025, o sítio eletrônico de notícias da CNN Brasil entre outros meios de comunicação, trouxeram a público que naquela última semana, viralizaram nas redes sociais diversos relatos de pessoas que estavam indo até locais em São Paulo para “vender a íris” em troca de uma quantia em dinheiro. Cerca de 500 mil pessoas venderam os dados da íris[7].

Segundo a reportagem, a responsável pela captação dos dados era a empresa Tools for Humanity (TfH). “Utilizando câmeras de última geração, a TfH escaneia a íris

---

[6] www.infomoney.com.br. Estadão Conteúdo. **Startup lança serviço que inaugura comércio de dados pessoais**. [2022]. Disponível em: https://www.infomoney.com.br/negocios/drumwave-lanca-servico-que-inaugura-comercio-de-dados-pessoais/. Acesso em: 01 de fevereiro de 2025.

[7] www.cnnbrasil.com.br. MIIANEZI, Gabriela. **Empresa paga cerca de R$ 500 por escaneamento de íris; entenda como é feito**. São Paulo, SP, [2025]. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/sp/empresa-paga-cerca-de-r-500-por-escaneamento-de-iris-entenda-como-e-feito/. Acesso em: 01 de fevereiro de 2025.

da pessoa para criar o que chama de World ID (“documentação mundial”, em tradução livre)”, apresentando-se como uma verificação de humanidade.

O objetivo do projeto, de acordo com a empresa, era obter um código único que não poderia ser reproduzido pela inteligência artificial, registrando a reportagem o argumento utilizado: “A inteligência artificial também é usada para o mal. O objetivo aqui é dar mais segurança”.

Em detrimento da determinação, pela Autoridade Nacional de Proteção de Dados (ANPD), da suspensão do pagamento pela coleta da íris, a empresa continuou ainda por um período a realizar a captação dos dados, resumindo-se a afirmação que não ficaria com os dados dos usuários.

4.2 A percepção de nossos tribunais superiores

Pelo que se é possível observar, esse modelo de negócios tem sua exegese na nulificação de todos os conceitos derivados dos direitos da personalidade que já foram mencionados nos capítulos dois e três. Surge exatamente quando se inicia o tratamento de dados através das novas tecnologias, com uma capacidade de processamento mais agressivo e nunca antes visto.

Assim, estabelece-se em relação a nossos tribunais superiores, na incidência das normas, a necessidade de emergir os limites impostos pela autodeterminação informativa na proteção dos dados pessoais nos bancos de dados. Principalmente ao constatarmos que a construção doutrinaria dos direitos da personalidade e de seu viés da autodeterminação informativa são anteriores ao advento da existência virtual, tornando-se logicamente inadmissível que uma empresa ao realizar a captação de dados pessoas, desconsidere e ignore toda evolução doutrinária com vistas a proteção da dignidade humana.

E se consegue perceber isso quando se tem como parâmetro inicial um esboço das decisões que antecederam a análise sob a vigência da Lei nº 13.709/2018. Considerando-se que a Lei nº 13.709/2018 entrou em vigor de maneira escalonada:

- Em 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, que tratam da constituição da Autoridade Nacional de Proteção de Dados – ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD;

- Em 18 de setembro de 2020, quanto aos demais artigos da Lei, com exceção dos dispositivos que tratam da aplicação de sanções administrativas;
- Em 1º de agosto de 2021, quanto aos arts. 52, 53 e 54, que tratam das sanções administrativas.

Antes da Lei Geral de Proteção de Dados havia uma construção jurisprudencial efetiva quanto a proteção da privacidade com suporte na dignidade da pessoa humana expressamente previsto no texto constitucional, permitindo uma abertura interpretativa mais expressiva face a ausência de uma "regulamentação" mais específica. O que permitia um dinamismo a norma, que a regulamentação legal mais específica impede em um primeiro momento, principalmente quando se constata que quando a lei surge, o tempo até sua maturidade de vigência não fica estático quanto ao dinamismo dos fatos.

Porém, o sistema normativo era carecedor dos parâmetros conceituais que já vinham sendo amadurecidos pela doutrina e mencionados casuisticamente por nossos tribunais, e sobre os quais o trabalho interpretativo poderia estender sua eficácia.

4.2.1 Supremo Tribunal Federal

No Supremo Tribunal Federal se pode verificar essa linha de raciocínio e o desenvolvimento dos argumentos com o advento da Lei nº 13.709/2018. Em manifestação na Medida Cautela na Ação Direta de Inconstitucionalidade nº 6.387, de maio de 2020, encontra-se uma das primeiras referências naquele Supremo Tribunal Federal ao normativo da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. O momento era de apreensão em face da pandemia do vírus Sars-Cov-2 e a edição da Medida Provisória nº 954/2020, que determinava o compartilhamento de dados pessoas por concessionária de serviço público com ente público, o que suscitou resistência e questionamento junto ao Supremo Tribunal Federal.

A ementa da referida decisão então estabeleceu como premissa à análise, a norma incerta no art. 2º da Lei nº 13.709/2018.

> "1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

Sem, todavia, afastar-se do suporte constitucional que permeavam as decisões antes da Lei nº 13.709/2018:

> "2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.

Naquele momento sob a pandemia do Sars-Cov-2, o compartilhamento de dados para efeitos de avaliação e manejo de riscos para a saúde pública parecia razoável, porém, por não dispor como seriam tratados e utilizados esses dados com vistas ao fim proposto, suscitaram dúvidas sobre sua real necessidade diante de outros meios menos invasivos de análise. Somando-se ainda o fato de não dispor de previsão sobre mecanismos idôneos de proteção dos referidos dados de ingerência de terceiros.

As ressalvas que fizeram o Supremo Tribunal Federal reconhecer, no caso sob exame, a impossibilidade do compartilhamento dos dados, como a ausência de forma de tratamento e de proteção dos dados, estavam previstas na Lei nº 13.709/2018. Na referida decisão, em detrimento reconhecer que a Lei nº 13.709/2018 não se encontrava em pleno vigor, a sua menção se tornava relevante para a situação que se apresentava, já lançando irradiações sobre as manifestações naquele tribunal superior:

> "8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020."

Na oportunidade a relatora, Ministra Rosa Weber, em seu voto deixou registrado que o dinamismo social e econômico exige que se redefina, de tempos em tempos, a exata natureza e extensão da proteção à privacidade do indivíduo e por via de consequência a extensão da autodeterminação informativa:

> “No clássico artigo The Right to Privacy, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima.”

No voto, não fugiu à percepção da relatora, um ponto de muita relevância para o que aqui se propõe, e que já foi mencionado no capítulo dois, que talvez naquele momento o leitor não tenha percebido a importância de suas implicações para a proteção da privacidade. Com as novas tecnologias e a virtualização da existência, o cruzamento e tratamento de dados não sensíveis e por vezes até irrelevantes, em um primeiro momento, permitem a dedução e construção de perfis detalhados de informações sensíveis:

> “4. Certamente há quem ainda se lembre de que há poucas décadas, antes da ubiquidade da telefonia móvel, era comum a edição de listas telefônicas impressas contendo nomes, telefones e endereços dos assinantes residenciais e comerciais dos serviços de telefonia em uma dada localidade. Além de ser facultado aos usuários dos serviços de telefonia optarem pela exclusão dos próprios dados dessas listas, é crucial ter presente que o que podia ser feitos a partir da publicização de tais dados pessoais não se compara ao que pode ser feito no patamar tecnológico atual, em que poderosas tecnologias de processamento, cruzamento e filtragem de dados permitem a formação de perfis individuais extremamente detalhados.” p.28

Sendo relevante repetir, agora dentro da análise jurisprudencial, que o dado, quando unitário e avulso, como um número de telefone, um endereço, um número de documento ou última compra realizada, podem, a princípio, não fazer referência a alguém diretamente, mas quando disponíveis em um banco de dados, organizados e cruzados, podem resultar em informações bastante específicas sobre determinada pessoa, inclusive de caráter sensível, transformando-se em dados poderosos nas mãos de quem as detém (Teffé; Viola, 2020).

A relevância paradigmática da referia decisão foi o reconhecimento da existência de um direito fundamental autônomo à proteção de dados pessoas e a autodeterminação informativa, reproduzindo, como requisitos à legitimidade desse tratamento, o disposto normativo da Lei nº 13.709/2018, ainda não vigente, sem interpretações além do texto expresso.

Resultando do julgamento algumas balizas para análises sobre o tema:

> a) primeiro a privacidade dos usuários só pode ser afastada a partir de uma justificação exaustiva das finalidades atribuídas ao tratamento de dados;
> b) garantia de transparência suficiente para o titular ter um nível de controle adequado a verificação prospectiva da licitude do tratamento de dados;
> c) envolver apenas os dados estritamente necessários para o alcance das finalidades eleitas; e
> d) vir acompanhado do incremento dos protocolos e mecanismos de segurança do sistema de informação, de acordo com o grau de risco gerado pela relativização do direito fundamental à autodeterminação informativa[8].

Segundo o Ministro Gilmar Mendes em seu voto na ADI nº 6.649, a decisão proferia pela relatora Ministra Rosa Weber, foi relevante por:

> "Primeiro por contribuir para a construção de uma dogmática constitucionalmente adequada para o que se tem chamado de era digital, berço de uma sociedade fundada no desenvolvimento tecnológico e no intercâmbio de informações digitais. Segundo pela enunciação dos vetores interpretativos e do substrato axiológico que devem orientar a compreensão e a aplicação de toda a legislação existente sobre o tema."

Em pleno vigor a Lei nº 13.709/2018, o Ministro Nunes Marques no Mandado de Segurança nº 37.968, monocraticamente ao analisar pedido de quebra de sigilos

---

[8] BRASIL. Supremo Tribunal Federal. ADI 6387 MC-Ref. […] MEDIDA PROVISÓRIA Nº 954/2020. **Emergência de saúde pública de mportância internacional decorrente do novo Coronavírus (Covid-19). Compartilhamento De Dados Dos Usuários Do Serviço Telefônico Fixo Comutado E Do Serviço Móvel Pessoal, Pelas Empresas Prestadoras, Com O Instituto Brasileiro De Geografia E Estatística**. [...]. Relatora: Minª.Rosa Weber, 07 de maio de 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1123008775. Acesso em: 14 de mai. 2025.

Lei nº 13.709/2018: Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade; II - a autodeterminação informativa. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de mai. 2025.

3. Lei nº 13.709/2018:
Art. 5º Para os fins desta Lei, considera-se: (…) X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
(…) XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de mai. 2025.

Na ocasião foi determinada a tramitação conjunto das Ações Diretas de Inconstitucionalidade nº 6.387, 6.388, 6.389, 6.390 e 6.393.

telefônico e telemático por Comissão Parlamentar de Inquérito, em novembro de 2021 registrou:

> "Este último ponto precisa ser devidamente ressaltado porque, nos tempos que correm, o modo de vida das pessoas está cada vez mais ligado ao uso de tecnologias das comunicações. Os computadores pessoais e telefones inteligentes (smartphones) servem, na atualidade, para comunicações e registros os mais diversos, desde aspectos ligados aos chamados "dados sensíveis" (dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico), que a princípio não apresentam nenhum interesse para investigação parlamentar, às questões ligadas ao trabalho e aos negócios — essas, sim, de possível interesse para uma CPI. A grande convergência de informações para esses mecanismos implica o dever, por parte das autoridades investigativas, de minimizar o acesso aos dados pessoais do investigado, limitando-se ao estritamente necessário para a investigação, sob pena de ferimento irreparável do direito à intimidade e à privacidade. O direito "fundamental à privacidade (CF, art. 5, X), como tal entendido "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução Danilo Doneda e Luciana Cabral Doneda, p. 15), está na ordem do dia das discussões constitucionais justamente pela circunstância de que as tecnologias da informação têm induzido a hiperdocumentação do dia a dia das pessoas, desde os menores atos domésticos até às suas movimentações físicas e às manifestações públicas em redes sociais; isso, associado à facilidade de manipulação e recuperação das informações a partir de dados, por meio de mecanismos apropriados, deixa vulneráveis aspectos sensíveis da vida íntima dos cidadãos. Nesse contexto, a quebra de sigilo das comunicações deve ser medida excepcionalíssima, e, ainda mais, deve recair sobre o mínimo possível para o desenvolvimento da investigação (seja ela judicial ou legislativa). A Lei Geral de Proteção de Dados - LGPD, aliás, embora não se dirija especificamente à disciplina das medidas de investigação, deixou claro, no art. 4º, § 1º, que tais medidas devem sempre ser proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na própria LGPD."

Dois pontos são relevantes na manifestação do Ministro Nunes Marques, primeiro a percepção de um estado de coisas de hiperdocumentação e segundo a facilidade da manipulação e recuperação de informações em virtude do avança tecnológico. Parte-se então da premissa que todos os dados estão em permanente estado de vulnerabilidade[9].

---

[9] BRASIL. Supremo Tribunal Federal. **MS nº 37.968**. […] 1. Hélio Angotti Neto formalizou mandado de segurança, com pedido de liminar, contra ato do Presidente da CPI da Pandemia mediante o qual determinada a quebra de seus sigilos telefônico e telemático. [...]. Relator: Min. Nunes Marques, 11 de novembro de 2021. Disponível em: portal.stf.jus.br/processos/downloadPeca.asp?id=15348771598&ext=.pdf. Acesso em: 14 de mai. 2025.

Registrando o Ministro a abrangência dos princípios previstos na Lei nº 13.709/2018, para além de seu objeto inicial, irradiando sobre todos os ramos do direito a necessidade de se tratar os dados no estrito limite de sua necessidade só e somente.

O reconhecimento jurisprudencial de um direito fundamental autônomo à proteção de dados pessoas e à autodeterminação informativa, foi posteriormente positivado pelo Legislativo de forma expressa através da Emenda Constitucional 115, de 10 de fevereiro de 2022, no art. 5º, inciso LXXIX, da Constituição Federal:

> **Art. 5º (...):**
>
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).

Passando a partir desse momento o arcabouço constitucional da proteção da personalidade contar com os incisos X, XII e LXXIX do art. 5º ao dar suporte a legislação infraconstitucional da Lei nº 13.709/2018:

> Art. 5º (...)
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> (...) XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).

Voltando a permitir ao sistema normativo uma abertura interpretativa mais expressiva, semelhante àquela que se dava antes do advento da Lei nº 13.709/2018, mesmo diante de uma “regulamentação” mais específica presente na Lei nº 13.709/2018, permitindo um maior dinamismo a norma.

Em maio de 2022, na Arguição de Descumprimento de Preceito Fundamental nº 722, de relatoria da Ministra Cármem Lúcia, o Supremo Tribunal Federal quando em análise suposta coleta de dados de servidores contrários ao governo (produção e a disseminação de dossiês sobre um grupo de 579 servidores federais e estaduais de

segurança identificados como integrantes do ‘movimento antifascismo’ e dos professores universitários citados, sob a desculpa de atividade de inteligência) deixou registrado a importância da constitucionalização do tema, ressalvando que a validade do texto legal e integral cumprimento ao comando normativo infralegal há de ter como única interpretação e aplicação juridicamente legítima, aquela que conforma a norma à Constituição da República[10]:

> “2. A efetividade das atividades de inteligência associa-se, com frequência, ao caráter sigiloso do processo e das informações coletadas. No Estado Democrático de Direito essa função submete-se ao controle externo do Poder Legislativo (inc. X do art. 49 da Constituição) e do Poder Judiciário (inc. XXXV do art. 5º da Constituição) para aferição da adequação do sigilo decretado às estritas finalidades públicas a que se dirige. 3. Para validade do texto legal e integral cumprimento ao comando normativo infralegal do Poder Executivo, há de se adotar como única interpretação e aplicação juridicamente legítima aquela que conforma a norma à Constituição da República. É imprescindível vincularem-se os dados a serem fornecidos ao interesse público objetivamente comprovado e com motivação específica. 4. O fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal. 5. Práticas de atos contra ou à margem do interesse público objetivamente demonstrado, especificado em cada categoria jurídica, devem ser afastadas pelo Poder Judiciário, quando comprovado o desvio de finalidade. 6. A ausência de motivação expressa impede o exame da legitimidade de atos da Administração Pública, incluídos aqueles relativos às atividades de inteligência, pelo que a motivação é imprescindível. 7. A prática de atos motivados pelo interesse público não torna juridicamente válidos comportamentos de órgãos do Sistema Brasileiro de Inteligência para fornecerem à ABIN dados configuradores de quebra do sigilo telefônico ou de dados. Competência constitucional do Poder Judiciário (...)”.

A importância de se constitucionalizar a garantia fundamental a proteção de dados pessoais, diz respeito principalmente a superação da compreensão, já esboça pelo Supremo Tribunal Federal de que norma hierarquicamente inferior, mesmo sob o argumento de resguardar direito constitucionalmente assegurado, não pode se sobrepor a norma constitucional. Encontrando-se formado os sistemas jurídicos de

---

[10] BRASIL. Supremo Tribunal Federal. **ADPF 722**. Rede Sustentabilidade e Ministro de Estado da Justiça e Segurança Pública. [...] Produção e disseminação de dossiê com informações de servidores federais e estaduais integrantes de movimento antifascismo e de professores universitários. Desvio de finalidade. Liberdades de expressão, privacidade, reunião e associação. [...]. Relatora: Min. Cármen Lúcia, 16 de maio de 2022. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=761255398. Acesso em: 14 de mai. 2025.

proteção dos dados pessoais em qualquer ambiente, com irradiações na autodeterminação informativa.

Em setembro de 2022, ao analisar o tratamento de dados realizado pelo Estado, na Ação Direta de Inconstitucionalidade nº 6.649, o Supremo Tribunal Federal reforçou o normativo da Lei nº 13.709/2018 de forma expressa, com adaptação ao tratamento feito pelo Estado.

O relator, Ministro Gilmar Mendes, na abertura da análise registrou como controvérsia a relativa aos limites, ao âmbito de proteção e à dimensão axiológica dos direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade, especificamente no que diz respeito ao tratamento de dados pelo Estado brasileiro, coleta, armazenamento, transferência e divulgação de dados pessoais.

Consignando ainda a necessidade de se analisar no âmbito de proteção do direito à autodeterminação informativa, os limites e as salvaguardas institucionais que se aplicariam no compartilhamento de informações:

> "Põe em perspectiva, portanto, uma questão de crucial importância para qualquer sociedade democrática contemporânea, qual seja, o alcance, os limites e a fisionomia do direito à autodeterminação informativa." p. 30

Observa-se que a Lei Geral de Proteção de Dados é na presente manifestação, em virtude já se encontrar em pleno vigor, um dos principais suportes jurídicos a análise em conformidade com a Emenda Constitucional nº 115/2022, que estabelece de forma expressa o direito fundamental à proteção de dados pessoais.

Registra o Ministro relator, que na era da tecnologia, a atualização da tutela dos direitos fundamentais torna-se indispensável, em face da possibilidade de manipulações pelo poder da comunicação. Assim explica:

> "O crescimento exponencial das atividades de coleta, tratamento e análise de dados pessoais possibilita que governos e empresas utilizem algoritmos e ferramentas de data analytics, promovendo classificações e esteriotipações discriminatórias de grupos sociais na tomada de decisões estratégicas para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham." p.40

Continua:

> "É por isso que, diante dos riscos inerentes à sociedade da informação, cabe ao Tribunal, de um lado, reconhecer que a disciplina jurídica do

> processamento e da utilização de dados pessoais acaba por afetar o sistema de proteção de garantias individuais como um todo e, de outro, proceder a uma releitura de mecanismos clássicos de defesa das liberdades públicas e do Estado Democrático de Direito.” p. 41

E conclui:

> “É justamente essa reconfiguração que possibilita a afirmação do direito à autodeterminação informacional como contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo. Nas palavras ilustres de Stefano Rodotà, a privacidade também passa a ser definida como ‘o direito de manter o controle sobre suas próprias informações e de determinar como a privacidade é alcançada e, em última instância, como o direito de escolher livremente o seu modo de vida’ (tradução livre) (Rodotà, 2012, p. 48).

Como já consignado anteriormente, em face da capacidade tecnológica do tratamento de dados a que se chegou, é ingenuidade acreditar na separação estática de dados pessoais e dados pessoais sensíveis para efeitos de proteção maior ou menor. Quando do início desse trabalho, tinha-se de forma equivocada essa premissa e face da previsão legislativa expressa.

Como registra o Ministro Gilmar Mendes em seu voto, não mais existe dados insignificantes nas circunstâncias modernas do processamento automatizado de dados, em face das finalidades propostas pelos interesses mais diversos. E aqui há um ponto de atenção, a Lei nº 13.709/2018 talvez refletindo uma realidade anterior, de forma estática, estabelece a divisão entre dados não sensíveis (insignificantes?) e dados sensíveis.

Nesse sentido, a Emenda Constitucional nº 115/2022 ao alçar de forma explícita a proteção de dados pessoais a direito fundamental, autoriza os mecanismos de interpretação para superação dessa divisão estática introduzida pelo texto da Lei Geral de Proteção de Dados, confirmando a ideia da necessidade de atenção a atualização permanente da tutela dos direitos fundamentais.

E aduz o relator:

> “A rigor, os gatilhos que acionam o direito à autodeterminação informática relacionam-se mais propriamente com o grau de sensibilidade das informações e com o risco de malversação dos dados pessoais, tornando estéril qualquer tentativa de abrandar o nível de proteção dispensado pela ordem jurídica sob o pretexto da simplicidade ou trivialidade das informações envolvidas.” p. 51

Consignando por fim como resultado do julgamento:

> “4. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.”

É saber, até que ponto se pode agregar informações sobre pessoas naturais, dispersas entre várias bases temáticas, para produzir conhecimento sobre elas. Que garantias procedimentais e materiais devem ser oferecidas ao titular dos dados, a fim de que tal associação estruturada de informações não seja abusiva?

Considerando-se que “A rigor, os gatilhos que acionam o direito à autodeterminação informática relacionam-se mais propriamente com o grau de sensibilidade das informações e com o risco de malversação dos dados pessoais, tornando estéril qualquer tentativa de abrandar o nível de proteção dispensado pela ordem jurídica sob o pretexto da simplicidade ou trivialidade das informações envolvidas[11].”

O Estado não pode repetir o modus operandi do mercado, até porque não há interesse econômico envolvido, podendo-se atribuir esse comportamento semelhante apenas ao estado de coisas ainda incipiente, o que deixa para as empresas uma abertura para agir como têm feito, alheias as fronteiras entre dados pessoais e dados pessoais sensíveis, conceitos estes já superados diante das decisões do Supremo Tribunal Federal colacionadas até o presente momento.

O estudo de Macei e Silva (2017) aponta que garantias constitucionais também servem para avaliar o comportamento do Estado como agente que exerce vontades e porque não dizer pulsões e inclinações, sentimentos estes que se não coadunam com o que se espera de um Estado moderno democrático de direito.

---

[11] BRASIL. Supremo Tribunal Federal. **ADI 6649**. […] Tratamento de Dados Pessoais pelo Estado Brasileiro. Compartilhamento de Dados Pessoais entre Órgãos e Entidades da Administração Pública Federal. [...]. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683585. Acesso em: 14 de mai. 2025.

Conclusão diversa não se pode chegar, as manifestações sobre dados não sensíveis estão intimamente relacionadas a proteção dos dados sensíveis, como consequência em muitos aspectos, vez porque a construção de sua proteção, é ponto relevante para percepção da proteção dos dados sensíveis.

Nesse sentido, parecia até o momento que tinha ficado bem claro o fato de que a divisão estática entre dados sensíveis e não sensíveis, para o Supremo Tribunal Federal, não poderia se sustentar e que o texto da Lei nº 13.709/2018, necessitaria de uma interpretação conforme.

Na Ação Direta de Inconstitucionalidade nº 5.545, proferida em abril de 2023, de relatoria do Ministro Luiz Fux, que tratava de banco de dados genéticos de mães e bebés com fim de evitar a troca na maternidade, o Ministro André Mendonça consignou a necessidade de adequar a intenção de proteger a mãe e filho de um dano dessa natureza com a garantia da proteção de dados presente na Constituição Federal e na Lei Geral de Proteção de Dados. Diante de opções menos gravosas possíveis de serem implementadas:

> “A par disso tudo, a lei impugnada também viola o direito fundamental à proteção de dados pessoais. Quanto ao tema, está Suprema Corte, ao julgar as ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, teve a oportunidade de declarar o seu assento constitucional, antes mesmo do advento da Emenda de n. 115/2002, que acrescentou o inciso LXXIX ao art. 5º da Constituição de 1988. Nesse sentido, colho trecho do voto do eminente ministro Gilmar Mendes nas citadas ações: ‘No caso do direito fundamental à proteção de dados, este envolve, em uma perspectiva subjetiva, a proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e, em uma perspectiva objetiva, a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados. (MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 176-177). Nesse aspecto, a autodeterminação do titular sobre os dados deve ser sempre a regra, somente afastável de maneira excepcional. A justificativa constitucional da intervenção deve ser traduzida na identificação da finalidade e no estabelecimento de limites ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área.’A norma impugnada afronta também o direito fundamental à autodeterminação informativa ao obrigar a colheita do material genético de todos os bebês e mães.”

O Ministro Alexandre de Morais por sua vez:

> “As intervenções no âmbito de proteção do direito à privacidade devem ser consideradas legítimas quando: (1) adequadas para libertar outros princípios constitucionais; (2) necessárias, ante a inexistência de outro meio eficaz; (3) proporcionais em sentido estrito, por promoverem a realização de princípios,

cujas razões, no caso concreto, são mais fortes que as decorrentes do direito à privacidade. No restrito âmbito familiar, os direitos à intimidade e vida privada devem ser interpretados de uma forma mais ampla, levando-se em conta as delicadas, sentimentais e importantes relações familiares, devendo haver maior cuidado em qualquer intromissão externa. Dessa forma, concluímos como Antonio Magalhães, no sentido de que as intromissões na vida familiar não se justificam pelo interesse de obtenção de prova, pois, da mesma forma do que sucede em relação aos segredos profissionais, deve ser igualmente reconhecida a função social de uma vivência conjugal e familiar à margem de restrições e intromissões (Gomes Filho, Antônio Magalhães. Direito à prova no processo penal. São Paulo: Revista dos Tribunais, 1997. p. 128).
(...)

Diante desse quadro, é imperioso assentar que a proteção de dados pessoais é um dos pilares e um dos maiores desafios do constitucionalismo contemporâneo. A normatização jurídica do tratamento conferido aos dados pessoais, consolidando marcos regulatórios propícios a sua proteção, constitui uma atividade recente do Poder Legiferante, impelida tanto pelo avolumamento maciço de informações reunidas em bancos de dados, viabilizado por avanços tecnológicos recorrentes, quanto pelo crescente interesse em sua preservação e sua utilização. É bem jurídico cuja tutela se revela imprescindível à sociedade, na Era da Informação.

(...)

Impõe-se, dessa maneira, averiguar se conteúdo impugnado nessa Ação Direta está alinhado ao complexo principiológico da LGPD que, com suporte em preceitos constitucionais (art. 5º, LXXIX, CF), exige que o tratamento de dados seja realizado com finalidade, transparência e respeito à autodeterminação das pessoas afetadas."

E afirma:

"Portanto, diferentemente do direito à privacidade assegurado no Art. 5º, X, CF/88, que consubstancia uma garantia constitucional de caráter negativo, o direito à proteção de dados ostenta caráter positivo e com ele não se confunde. Ademais, apesar de não haver sido igualmente reconhecido como um direito fundamental no ordenamento brasileiro, o Tribunal Constitucional Federal alemão identificou um terceiro desdobramento, proveniente de uma leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade: o direito à autodeterminação informativa.

(...)

Ocorre que os dados pessoais acabam sendo elementos constitutivos da própria identidade pessoal, uma vez que, na "era da informação", a existência da pessoa humana não está limitada aos seus atributos psicofísicos,

> estendendo-se às representações digitais destes atributos. É deste contexto que surge o conceito da integridade digital, isto é, a partir da premissa de que, se as pessoas vivem no mundo digital, então sua dignidade deve ser estendida a ele. Dessa forma, uma proteção satisfatória da dignidade da pessoa humana não deve ser limitada a sua autodeterminação informacional. Como um verdadeiro desdobramento da dignidade da pessoa humana, a integridade digital evita o processo de comoditização dos nossos dados pessoais, garantindo sua proteção ainda nas hipóteses em que seu titular não saiba sobre a existência das respectivas aplicações digitais (Vandanyan *et al.,* 2022, p. 175-179).”

Continua:

> “Essas duas declarações constituem importantes balizas para nortear o processo decisório das cortes, considerando o notório conhecimento técnico dos integrantes desse órgão deliberativo. Neste sentido, observe-se o disposto no artigo 8º da Declaração Universal sobre o Genoma Humano de 2004, a saber: “(a) O consentimento prévio, livre, informado e expresso, sem tentativa de persuasão por ganho pecuniário ou outra vantagem pessoal, deverá ser obtido para fins de recolha de dados genéticos humanos, de dados proteômicos humanos ou de amostras biológicas, quer ela seja efetuada por métodos invasivos ou não-invasivos, bem como para fins do seu ulterior tratamento, utilização e conservação, independentemente de estes serem realizados por instituições públicas ou privadas. Só deverão ser estipuladas restrições ao princípio do consentimento por razões imperativas impostas pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos.”

Ressaltando os diversos desenhos normativos para obtenção de consentimento:

> “Em sentido semelhante, o tema do consentimento é muito relevante para os Australian Privacy Principles (APP), treze princípios sobre privacidade que informam a norma que regula o tratamento de dados pessoais no país (Privacy Act 1988), o que expressamente inclui “saúde (incluindo informação genética preditiva).
>
> (…)
>
> A respeito do consentimento, as orientações gerais estabelecidas pelo setor responsável pela fiscalização e sanções delimitaram quatro elementos principais: “o indivíduo ser adequadamente informado antes de dar o consentimento; o indivíduo dar o consentimento voluntariamente; o consentimento ser atual e específico, e o indivíduo ter a capacidade de entender e comunicar seu consentimento” (B.35, tradução livre). Isso não impede que, excepcionalmente, haja consentimento implícito, pelo uso de opções “opt-out”. Para essas hipóteses, o Guia apresenta novas orientações: B.38 Uma entidade APP não deve presumir que um indivíduo tenha consentido em uma coleta, uso ou divulgação, ainda que pareça ser vantajoso para essa pessoa. Nem uma entidade pode estabelecer consentimento implícito afirmando que, se o indivíduo soubesse sobre os benefícios da coleta, uso ou divulgação, provavelmente consentiria com isso.

> B.39 Geralmente, não se deve presumir que um indivíduo tenha dado consentimento apenas com base no fato de que não se opuseram a uma proposta para lidar com informações pessoais de uma maneira particular. Uma entidade APP não pode inferir consentimento simplesmente porque forneceu a um indivíduo uma notificação de uma coleta, uso ou divulgação de informações pessoais. Será difícil para uma entidade estabelecer que o silêncio de um indivíduo pode ser tomado como consentimento. O consentimento pode não estar implícito se a intenção de um indivíduo for ambígua ou se houver dúvida razoável sobre a intenção do indivíduo. B.40 O uso de um mecanismo opt-out para inferir o consentimento de um indivíduo só será apropriado em circunstâncias limitadas, já que a intenção do indivíduo de não optar por não participar pode ser ambígua."

Os princípios da adequação, necessidade e finalidade foram expressamente trazidos no artigo 6º da Lei nº 13.709/2018[12], que determina, ainda, a observância da boa-fé. À configuração da necessidade, limita-se o tratamento ao mínimo necessário para a realização das finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Já de acordo com a finalidade, a lei impõe que a realização do tratamento de dados pessoais se dê para propósitos legítimos, específicos, explícitos e informados ao titular. Assim a lei exige a compatibilidade do tratamento de dados pessoais com as finalidades informadas ao titular, consoante o contexto do tratamento, porém, a referida decisão alerta para percepção de algo mais, presente no espectro da dignidade da pessoa humana para além da autodeterminação informativa no tratamento de dados, a integridade digital, conceito que dentro do espectro da dignidade da pessoa humana evita o "processo de comoditização dos nossos dados

---

[12] BRASIL. Supremo Tribunal Federal. **ADI 5545**. Procurador-Geral da República e Assembleia Legislativa do Estado do Rio de Janeiro. [...] Lei estadual que obriga a adoção de medidas de segurança que evitem, impeçam ou dificultem a troca de recém-nascidos nas dependências de hospitais públicos ou privados, casas de saúde e maternidades e que possibilitem a posterior identificação através de exame de DNA. Coleta do material genético de todas as mães e filhos na sala de parto [...]. Relator: Min. Luiz Fux, 13 de abril de 2023. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768636835. Acesso em: 14 de mai. 2025.

2. 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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de mai. 2025.

pessoais, garantindo sua proteção ainda nas hipóteses em que seu titular não saiba sobre a existência das respectivas aplicações digitais (Vandanyan *et al.,* 2022).”

Em setembro de 2023 o Ministro Edson Fachin, na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.561, na análise da criação de um cadastro de usuários e dependentes de drogas pelo Estado do Tocantins, manifestou-se consignando, porém, como limites ao tratamento dos dados, aqueles estritamente previstos no texto, inclusive limitando a análise os conceitos ali presentes que distinguem dados sensíveis e não sensíveis:

> “Se a biopolítica é uma característica quase inevitável do estado moderno, os direitos fundamentais e estes em especial têm a função de preservar espaços de autonomia privada e autodeterminação, senão inalcançáveis, ao menos resguardados pela garantia de que o seu acesso deve observar um rigoroso e legal processo substancial e formal.
> É assim que a evolução dos sistemas de tratamento de dados e centralidade que eles adquirem hoje no funcionamento da política, da economia, do direito, e dos demais setores da sociedade, fizeram com que o constitucionalismo brasileiro se reconfigurasse para atualizar princípios que já se inscreviam no texto da Constituição da República. Nessa toada, a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, traz em seu bojo o princípio da autodeterminação informativa (art. 2º, II) e a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV), a partir da concretização de princípios constitucionais que já se encontravam plenamente em vigor na ordem jurídico brasileira. Ali, dados referentes à saúde são classificados como “dados pessoais sensíveis” (art. 5º, II) e, por isso, seu tratamento submete-se a um regime jurídico especial (art. 11).
> Esse sistema constitucional especial de proteção é violado pela lei impugnada, a qual, ademais, não prevê formas de controle prévio à inclusão no cadastro, não prevê a comunicação e o consentimento do interessado e, para a sua exclusão, exige laudo médico e informação oficial sobre a não reincidência. Tampouco existe protocolo claro de proteção e tratamento desses dados[13].” p.10

Demonstrando, a princípio, um retrocesso em toda a construção do tribunal até aquele momento, considerando-se as decisões anteriores aqui mencionadas, que em detrimento reafirmarem os termos normativos, abrem a discussão da impossibilidade estática da divisão entre dados não sensíveis e dados sensíveis, com viés de identificação não por sua natureza, mas pela sua destinação.

---

[13] BRASIL. Supremo Tribunal Federal. **ADI 6561**. Ação direta de inconstitucionalidade. Lei 3.528 de 2019 do Estado do Tocantins. Cadastro Estadual de usuários e dependentes de drogas. [...]. Relator: Min. Edson Fachin, 04 de setembro de 2023. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=772302784. Acesso em: 14 de mai. 2025.

A tensão inicial criada por um retrocesso aparente, no entanto, não se confirmou, no Agravo Regimental no Habeas Corpus 222.141, de relatoria do Ministro Ricardo Lewandowski e posteriormente relatado pelo Ministro Gilmar Mendes, datado de fevereiro de 2024, ao analisar o congelamento do conteúdo de comunicações privadas e de dados pessoais com base no art. 13, § 2º, do Marco Civil da Internet, por determinação do Ministério Público, sem prévia autorização judicial:

> "8. A concepção do direito à privacidade como uma garantia individual de abstenção do Estado na esfera privada individual passou por profundas transformações no decorrer do século XX. Devido ao próprio avanço das tecnologias da informação, assistiu-se a uma verdadeira mutação jurídica do sentido e do alcance do direito à privacidade. A releitura do direito à privacidade coincide com o desenvolvimento jurisprudencial do conceito de autodeterminação informacional (*die informationelle Selbsstbestimmung*) pelo Tribunal Constitucional Alemão. Essa nova abordagem revelou-se paradigmática por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso. 9. A maior abrangência da proteção atribuída ao direito de autodeterminação repercute no âmbito de proteção do direito à proteção de dados pessoais, que não recai sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros. A força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade de proteção da dignidade da pessoa humana, vis-à-vis a contínua exposição dos indivíduos ao risco de comprometimento da autodeterminação informacional.
>
> (…)
>
> 11. Uma vez inserida na equação à autodeterminação informacional, o mero congelamento de dados sem autorização judicial e fora das hipóteses legais afronta a tutela da privacidade.
>
> (…)
>
> 13. Ao requerer o congelamento fora das hipóteses legais, o Ministério Público pretendeu retirar dados pessoais e comunicações privadas do âmbito de disponibilidade dos investigados. E como tal, a medida afronta não apenas a legislação, como também o direito à autodeterminação informativa."

Pelo que ser percebe o aparente retrocesso registrado na ADI 6561 ficou isolado, reafirmando-se no âmbito do Supremo Tribunal Federal a necessidade de uma proteção dinâmica e permanente do direito à privacidade, principalmente ao se considerar que a maior abrangência da proteção atribuída ao direito de autodeterminação informativa não repercute no âmbito de proteção de dados pessoais, mas sim sobre os riscos atribuídos ao seu processamento.

Reafirmando-se, na oportunidade, o que já havia sido consignado na ADC 6649:

> "Como destaca Claudio Franzius, a característica especial do direito à autodeterminação informativa não é resultante de invencionismo, mas sim de "várias linhas de argumentação da jurisprudência do Tribunal, que já na decisão do microcenso, com recurso à sua jurisprudência sobre a dignidade humana, atribuiu ao cidadão individual uma esfera inviolável da vida privada, da qual se supõe que a influência da autoridade pública deve ser removida (Franzius, 2015, p. 262).
>
> (…)
>
> Como destacou a decisão, a identificação de um constante avanço tecnológico demanda a afirmação de um direito de personalidade que integre o contexto das "condições atuais e futuras circunstâncias do processamento automático de dados" ("heutigen und künftigen Bedingungen der automatischen Datenverarbeitung"). Essa releitura possibilita a afirmação do direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo.
> (…)
>
> A maior abrangência da proteção atribuída ao direito de autodeterminação repercute no âmbito de proteção do direito à proteção de dados pessoais, que não recai sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros.
> Entre nós, o reconhecimento da autonomia do direito fundamental à proteção de dados foi desenvolvido a partir das contribuições da Professora Laura Schertel Mendes. Nas suas palavras: 'Para além da coincidência do léxico com os modernos instrumentos internacionais de tutela da privacidade, certo é que a proteção da dignidade humana e a inviolabilidade da intimidade e da vida privada numa sociedade da informação somente pode ser atingida hoje por meio da proteção contra os riscos do processamento de dados pessoais. Assim, quando se interpreta a norma do art. 5º, X, em conjunto com a garantia do habeas data e com o princípio fundamental da dignidade humana, é possível extrair-se da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais.'
>
> (…)
>
> Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade.
> Todas essas transformações tecnológicas ensejam aquilo que Bruno Bioni enxerga como um cenário de hipervulnerabilidade no regime de proteção de dados pessoais, que se desdobra em traços vulnerantes peculiares sob as perspectivas informacional, técnica e econômica (Bioni, op. cit., p. 164).
> Desse modo, a força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade de proteção da dignidade da pessoa humana, vis-à-vis a contínua exposição dos indivíduos ao risco de comprometimento da autodeterminação informacional.
>
> (…)

> A mera supressão da autodeterminação informacional configura de pleno direito a nulidade dos elementos probatórios obtidos a partir do conjunto de informações."

Ao se manifestar o Ministro Ricardo Lewandowski citando doutrina do Ministro Alexandre de Morais também anuiu a jurisprudência que procurava se estabelecer[14]:

> "A inviolabilidade do sigilo de dados (art. 5º, XI) complementa a previsão ao direito à intimidade e vida privada (art. 5º, X), sendo ambas as previsões de defesa da privacidade regidas pelo princípio da exclusividade, que pretende assegurar ao indivíduo, como ressalta Tercio Ferraz, a "sua identidade diante dos riscos proporcionados pela niveladora pressão social e pela incontrastável impositividade do poder político. Aquilo que é exclusivo é o que passa pelas opções pessoais, afetadas pela subjetividade do indivíduo e que não é guiada nem por normas nem por padrões objetivos. No recôndito da privacidade se esconde, pois, a intimidade. A intimidade não exige publicidade porque não envolve direitos de terceiros. No âmbito da privacidade, a intimidade é o mais exclusivo dos seus direitos".
> Dessa forma, a defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e à espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão do segredo profissional. (Direito Constitucional. 33. ed. São Paulo: Atlas, 2017. p. 74; grifei)'
>
> (...)
>
> Outrossim, foi devidamente elucidado que – de acordo com o firme entendimento desta Suprema Corte - a privacidade alcança "[…] o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública."

Por mais que se observe o cuidado do Supremo Tribunal Federal em trazer às discussões à autodeterminação informativa como conceito conformador de todo tratamento de dados, não se adentra em suas minucias conceituais e limitadoras, termina-se por tirar o foco de seu conteúdo, focando-se nas suas irradiações, a ponto

---

[14] BRASIL. Supremo Tribunal Federal. **HC 222141 AgR**. […] Provedores e plataformas dos registros de conexão e registros de acesso a aplicações de Internet. 4. Congelamento do conteúdo de comunicações privadas e de dados pessoais da paciente, com base no art. 13, § 2º, do Marco Civil da Internet, por determinação do Ministério Público, sem prévia autorização judicial. Ilegitimidade. [...]. Relator: Min.Gilmar Mendes, 06 fevereiro de 2024. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=775652964. Acesso em: 14 de mai. 2025.

de afirmar, que mais relevante do que os limites de sua conceituação são os parâmetros para os tratamentos dos dados.

Nosso tribunal tem analisado o tema de forma transversal, partindo dos mecanismos de segurança que o texto normativo trouxe no tratamento dos dados pessoais e os impedimentos que não digam respeito a prestação de serviço imediada na utilização dos dados pessoais.

Por outro lado, é fato ser indiscutível a presença, no sistema constitucional brasileiro, mesmo antes da Emenda de n. 115/2022, de um direito à proteção de dados pessoais, o qual restringe a possibilidade de compartilhamento de dados pessoais, tanto pelo poder público como no âmbito da iniciativa privada, em ordem a assegurar a intimidade e a autodeterminação informativa da pessoa humana em face de processos de produção de conhecimento a partir da combinação e recombinação de dados, por processos automatizados ou não, em meio digital ou analógico.

A abrangência dessa proteção é o que se procura descortinar trazendo as decisões aqui colacionadas.

4.2.2 Superior Tribunal de Justiça

Nas manifestações do Superior Tribunal de Justiça sobre o tema, em face de sua competência infraconstitucional, percebe-se o foco mais nas consequências após a práticas dos atos em confronto com a norma, do que no estabelecimento de paradigmas conceituais.

Pouco tempo após a publicação da Lei nº 13.709/2018, em agosto de 2018, a exemplo do que se encontrava no Supremo Tribunal Federal, o Superior Tribunal de Justiça tinha somente no texto constitucional seu suporte conceitual. A Ministra Nancy Andrighi, relatora do acórdão no Edcl no Recurso Especial nº 1.630.889[15], assim consignou:

---

[15] BRASIL. Superior Tribunal de justiça. Edcl. **No Resp. 1.630.889**. […] Bancos de Dados. Proteção ao Crédito. Privacidade e Intimidade. Autodeterminação Informativa. Direitos Fundamentais. Eficácia Horizontal. Princípio da Máxima Efetividade. [...]. Relatora: Min. Nancy Andrighi, 27 de novembro de 2018. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201602636651&dt_publicacao=06/12/2018. Acesso em: 14 de mai. 2025.

> 7. Os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais.

Como afirmou a Ministra, a proteção da privacidade e da intimidade está intimamente relacionada aos direitos fundamentais e a dignidade da pessoa humana, o que sempre autorizou sua proteção mesmo antes do advento dos institutos da Lei nº 13.709/2018. Outras decisões no mesmo sentido no Recurso em Mandado de Segurança nº 61.302 – RJ[16], Recurso em Mandado de Segurança nº 60.698 – RJ[17] e Recurso Especial nº 1.758.799.

Nesse sentido, algumas decisões monocráticas, em detrimento não apresentarem um posicionamento colegiado, têm suporte em entendimentos já consolidados no referido tribunal, o que lhes dá autoridade para constar nesse trabalho.

Em decisão monocrática proferida em junho de 2020, no Agravo em Recurso Especial nº 1.673.128, o Superior Tribunal de Justiça teve oportunidade de se manifestar sobre a exploração econômica de dados pessoas captadas de forma ilegal. No caso sob análise, a obtenção dos dados pessoas se dava através de acesso ilegal ao site do DENATRAN e sua negociação ocorria através de site criado com esse objeto[18]:

---

[16] BRASIL. Superior Tribunal de justiça. **RMS 61302**. […] Direito a Privacidade e a Intimidade. Identificação de Usuários em determinada localização geográfica. [...]. Relator: Min. Rogerio Schietti Cruz, 26 de agosto de 2020. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201901991320&dt_publicacao=04/09/2020. Acesso em: 14 de mai. 2025.

[17] BRASIL. Superior Tribunal de justiça. **Resp. 1.758.799**. […] Ação de Compensação de Dano Moral. Banco De Dados. Compartilhamento de Informações Pessoais. Dever de Informação. Violação. Dano Moral. IN RE IPSA. [...]. Relatora: Minª. Nancy Andrighi, 12 de novembro de 2019. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700065219&dt_publicacao=19/11/2019. Acesso em: 14 de mai. 2025.

[18] BRASIL. Superior Tribunal de justiça. **A Resp. 1.673.128**. […] Apelação Cível. Ação Ordinária. Venda de Dados Sigilosos e Acesso Ilegal aos Dados do DENATRAN. [...]. Relator: Min. Herman Benjamin, 16 de junho de 2020. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=1673128&operador=e&b=DTXT&p=true&tp=T. Acesso em: 14 de mai. 2025.

> “2. A União Federal ajuizou ação ordinária em face da ora Apelante, objetivando, em sede de tutela antecipada, "que seja expedida ordem obrigando a requerida a cessar imediatamente a venda de dados protegidos e acesso ilegal aos dados do DENATRAN, suspendendo ainda o funcionamento do site www.carchek.com.br". Como provimento final, requer seja a Ré "condenada a cessar os acessos ilícitos ao banco de dados do DENATRAN e subsequente divulgação, sob pena de multa e, na ineficácia desta, de retirada compulsória do site da internet, sem prejuízo de outras medidas executivas necessárias a cessar a divulgação".
>
> 3. A sentença proferida às fls. 862/874 julgou procedente o pedido autoral, confirmando a decisão de fls. 639/647, que deferiu o pedido de tutela antecipada, determinando que a ré cessasse a venda de dados protegidos e acessos ilegais aos dados do DENATRAN, suspendendo o funcionamento do site www.carchek.com.br.
>
> 4. Conforme se depreende da análise dos autos, o Denatran foi alvo de auditoria da CGU, ocorrida em 2016, onde restou expressa a recomendação OS 201412890, no sentido de que aquele órgão identificasse junto ao Serpro "a origem do vazamento das informações e notifique o agente responsável, adotando as medidas administrativas e judiciais cabíveis".
>
> 5. Naquela oportunidade, foi instaurado o processo administrativo, onde restou constatado que a empresa ora Apelante conseguiu ter acesso ao sistema Denatran sem atender os requisitos legais para tanto. Ademais, os dados sigilosos eram disponibilizados mediante pagamento, através do sítio eletrônico www.carchek.com.br.
>
> 6. Por fim, mesmo após ter sido alertada sobre a ilegalidade quanto à disponibilização dos dados, a ora apelante continuou a praticar a referida atividade normalmente.”

Em outra decisão monocrática no Agravo no Resp. 2.130.619, de março de 2023, de relatoria do Ministro Francisco Falcão, após a vigência da Lei nº 13.709/2025, observa-se a menção e concordância com a divisão estática normativa entre dados não sensíveis e sensíveis como parâmetro em relação ao dever de indenizar[19]:

> “IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais, mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.
> V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano

[19] BRASIL. Superior Tribunal de justiça. **AResp. 2.130.619**. Eletropaulo Metropolitana Eletricidade de São Paulo S.A e Maria Edite de Souza. […] Indenização por Dano Moral. Vazamento de Dados Pessoais. Dados Comuns e Sensíveis. Dano Moral Presumido. Impossibilidade. Necessidade de Comprovação do Dan [...]. Relator: Min. Francisco Falcão, 07 de março de 2023. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: 14 de mai. 2025.

> moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações."

A referida decisão parte do pressuposto de que o vazamento de dados pessoas se enquadraria na ideia de mero dessabor, caso não fosse comprovado o efetivo dano moral.

Ponto relevante a se observar nessa manifestação, é que ela vem após as ADIs 6387 – MC e 6649, além da Emenda Constitucional nº 115. ADI's que estabeleceram parâmetros paradigmáticos para interpretação normativa da Lei nº 13.709/2018 no que se refere a proteção dos dados pessoais, não sustentando a ideia de que vazamentos de dados seja mero dessabor[20].

No Resp. 2.077.278, de outubro de 2023, de relatoria da Ministra Nancy Andrighi, desta feita em decisão colegiada, ao analisar o caso de vazamento de dados bancários, foi suscitada a necessidade de se analisar quais dados foram vazados para se tentar aferir a fonte do vazamento. O tipo de dado pode determinar sua origem comum ou restrita, podendo levar ao responsável pelo seu vazamento, por se saber quem o detinha e seu objeto, não sendo possível, no caso, captar de fontes alternativas:

> "13. Da mesma maneira, os dados pessoais sensíveis (relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, nos termos do art. 5º, II, LGPD), também podem ser obtidos de outras pessoas jurídicas com as quais o consumidor haja se relacionado e consentido especificamente.
>
> (...)
>
> 16 " O(A) consumidor(a) em alguns dos casos informa apenas seu CPF, e, de posse dele, o fraudador obtém os demais dados (número do contrato, endereço, valor necessário para quitação etc.), indicando que o estelionatário tem acesso aos dados da operação e que há falha na proteção dos dados da operação contratada, os quais deveriam ser protegidos. [...]."

---

[20] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.077.278**. Daniela Ferreira Ramos e BV Financeira S.A Crédito Financiamento e Investimento. […] Ação declaratória de Inexigibilidade de Débito por Vazamento de Dados Bancários Cumulada com Indenização por Danos Morais E Repetição De Indébito. Golpe Do Boleto. Tratamento De Dados Pessoais Sigilosos De Maneira Inadequada. Facilitação Da Atividade Criminosa. [...]. Relatora: Minª. Nancy Andrighi, 03 de outubro de 2023. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301909798&dt_publicacao=09/10/2023. Acesso em: 14 de mai. 2025.

> (...)
>
> 18. Sobre o art. 44 da LGPD, inclusive, a doutrina leciona que “a regra coloca em destaque, assim como ocorre em relação à responsabilidade do fornecedor no CDC, a questão relativa aos riscos do desenvolvimento, uma vez que delimita a extensão do dever de segurança àquela esperada em razão das 'técnicas de tratamento de dados disponíveis à época em que foi realizado' e, considerando “a previsibilidade de uma atualização e avanço técnico em atividades vinculadas à tecnologia da informação, mais veloz do que em outras atividades econômicas (Miragem, 2019).”

Registra a relatora a necessidade de se considerar, para efeitos de proteção do banco de dados, o desenvolvimento tecnológico disponível no momento do vazamento, utilizando-se da orientação normativa da Lei nº 13.709/2018.

Outro ponto relevante a ser considerado, é a utilização conceitual normativa de dados sensíveis para construção do raciocínio, o que mais uma vez desafia a construção jurisprudencial iniciada nas ADIs 6387 – MC e 6649.

Há aqui a percepção de que o Superior Tribunal de Justiça tem sua forma particular de interpretar a norma da Lei nº 13.709/20218, de forma mais estrita ao texto, ignorando, pelo menos nesse primeiro momento, a construção jurisprudencial desenhada pelo Supremo Tribunal Federal nas ADIs 6387 – MC e 6649.

Não se pode ignorar o fato de que há lei expressa autorizando, em situação específica, exploração econômica de dados para efeito de avaliação do risco de concessão de crédito - “banco de dados” para efeitos de *credit scoring* - formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Tema sobre o qual o Superior Tribunal de Justiça tem se debruçado em diversas decisões, o que tem possibilitando caso a caso, uma construção jurisprudencial de referência em relação ao art. 7, X da Lei nº 13.709/2018[21], com algumas irradiações para os direitos da personalidade.

---

[21] Lei 13.709/2018: Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (…) X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de mai. 2025.

No Resp. 2.104.036[22], de novembro de 2023, relator Ministro João Otávio de Noronha, em decisão monocrática sobre a validade da comercialização de dados para efeito de avaliação do risco de concessão de crédito - *credit scoring* – por exemplo, o ministro acolheu o argumento do tribunal de origem ao afirmar:

> '"[...] isto porque a simples divulgação de seus números de telefone em bancos de dados mantidos pela recorrida, ainda que sem prévia autorização ou mesmo de notificação dirigida ao interessado, não viola os limites impostos pelas Leis nº 12.414/11 e 13.709/18, portanto, não se mostrando capaz de gerar danos de ordem extrapatrimonial, o que acaba levando a necessária rejeição do presente recurso, porque manejado com adequado suporte.
>
> [...]
>
> Assim, é de se considerar que no caso em exame, inexistem elementos que conduzam ao reconhecimento de prática que venha a implicar em exploração dos dados pessoais do recorrente, isto porque os números de seus telefones em verdade se apresenta como dado de natureza intrinsecamente ligada a informações normalmente disponibilizadas para os mais variados atos da vida civil, a exemplo da contratação de serviços bancários, de telefonia, educacionais, dentre tantos outros que exigem preenchimento de cadastros, e consequentemente, a coleta de dados pessoais, sendo certo, ademais, que o telefone do recorrente não se enquadra na categoria de informações sensíveis, assim especificadas no art. 5º, inc. II, da LGPD, como já transcrito."'

Ou seja, o fato de ser comum a disponibilização de dados não sensíveis em diversos atos da vida cotidiana, autorizaria sua exploração econômica, sem ofensa aos textos das Leis 12.414/11 e 13.709/18

No Resp. 2.122.613, de abril de 2024, relator Ministra Maria Isabel Gallotti e Resp. 2.132.461, de maio de 2024, relator Ministro Antônio Carlos Ferreira, ao analisarem a validade da comercialização de dados para efeito de avaliação do risco de concessão de crédito – SERASA – *credit scoring*, prospecção de clientes, o que se extrai é a distinção entre o compartilhamento de dados pessoais sensíveis e os dados referentes ao histórico para crédito, em que se prescindiria do consentimento prévio

---

[22] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.104.036**. Claudovir Marcasso […] Entidade mantenedora de cadastros protetivos do crédito - inclusão de dados em cadastro de proteção ao crédito - alegação de violação da lei geral de proteção de dados (LGPD) por suposta comercialização de informações - informações mantidas pela ré que não se relacionam com a intimidade da parte, tampouco abrangem dado pessoal de maior repercussão - inteligência dos ARTS. 5º, E 7º DA LEI 13.709/2018 - Exercício regular do direito - autorização do consumidor que não se mostra necessária - ilicitude não configurada [...]. Relator: Min. João Otávio de Noronha, 14 de novembro de 2023. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=2104036&operador=e&b=DTXT&p=true&tp=T. Acesso em: 14 de mai. 2025.

do consumidor para comercialização, razão pela qual o entendimento firmado no precedente em repetitivo do Tema 710[23] (Brasil, 2011) só seria aplicável a esse último caso. Todavia, eventual violação a direitos de personalidade teria sido deduzida de modo genérico pela recorrente, inviabilizando o reconhecimento no caso, de violação a direitos de personalidade.

As referidas decisões são relativamente recentes, levando-se a conclusão que há um distanciamento entre os parâmetros estabelecidos no Supremo Tribunal Federal e o Superior Tribunal de Justiça no momento da análise da ofensa aos Direito da Personalidade, fazendo o Superior Tribunal de Justiça a opção por uma análise mais positivista em relação ao Supremo Tribunal Federal, que, por sua vez, introduz uma interpretação mais sistemática e evolutiva, considerando o atual estado de coisas do desenvolvimento tecnológico.

---

[23] BRASIL. Superior Tribunal de justiça. **Tema 710**. I - O sistema "*credit scoring*" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). II - Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo).

III - Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011.
IV - Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas.
V - O desrespeito aos limites legais na utilização do sistema "*credit scoring*", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. Relator: Min. Paulo de Tarso Sanseverino, 12 de novembro de 2014. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&cod_tema_inicial=710&cod_tema_final=710. Acesso em: 14 de mai. 2025.

Esse distanciamento interpretativo e observado ainda no Resp. 2.111.284[24] e Agravo no Resp. 2.586.773[25], de junho de 2024, de relatoria do Ministro Ricardo Villas Boas Cueva, onde reafirma a divisão estática entre dados não sensíveis e dados sensíveis para efeito de análise.

As decisões monocráticas têm, em sua maioria, mantido um apego ao texto normativo e um certo distanciamento da orientação jurisprudencial do Supremo Tribunal Federal, porém, já é possível observar, inicialmente de forma isolada, um sopro de razoabilidade como no Resp. 2.146.806[26], de junho de 2024, onde o relator Ministro Marco Aurélio Bellizze, de forma monocrática a se manifestar sobre o tema e a ausência de comunicação ou autorização, consignou:

> "Com efeito, o consumidor tem o direito de ser cientificado da existência de banco de dados ou qualquer informação armazenada, divulgada ou comercializada a seu respeito. Não se pode olvidar, ainda, que o consumidor pode, ainda, opor-se à divulgação de seus dados, ainda que não sensíveis. Como se vê, a inobservância dos deveres relacionados à coleta, armazenamento, divulgação ou qualquer outro tipo de tratamento dispensado aos referidos dados é passível de ensejar a obrigação de reparação de dados causados ao seu titular, porque agride o direito de personalidade. Dessa forma, a informação e a autorização do proprietário dos dados são imprescindíveis para a regularidade do cadastro"

---

[24] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.122.613**. Elton Nascimento de Souza […] Ação de obrigação de fazer cumulada com indenização por danos morais - divulgação de dados pessoais sem prévia autorização ou consentimento - informações relacionadas aos serviços de proteção de crédito - dispensa legal de prévio consentimento do titular dos dados - art. 7º, X da Lei Geral de Proteção de Dados - inexistência de indícios de comercialização ou divulgação de dados de forma ilícita. [...]. Relator: Minª. Maria Isabel Gallotti, 12 de abril de 2024. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=2122613&operador=e&b=DTXT&p=true&tp=T. Acesso em: 14 de mai. 2025.

[25] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.132.461**. […] Manutenção de cadastro, disponível apenas para associados e com finalidade exclusiva de fornecer subsídios para proteção do crédito encontra amparo no artigo 7º, X, da Lei Geral de Proteção de Dados - Ausência de comprovação de indevida comercialização de dados - Dano moral não configurado. Precedente desta E. Corte. Inteligência da Súmula nº 550 do C. STJ e do Tema nº 710 dos Recursos Repetitivos - Litigância de má-fé não caracterizada [...]. Relator: Min. Antonio Carlos Ferreira, 29 de maio de 2024. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=2132461&operador=e&b=DTXT&p=true&tp=T. Acesso em: 14 de mai. 2025.

[26] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.146.806**. Maria do Rosário Correia dos Santos. […] Ação cominatória c/c indenizatória. Banco de dados. Compartilhamento de informações pessoais. Dever de informação. Violação. Dano moral in re ipsa. Precedente da corte superior [...]. Relator: Min. Marco Aurélio Bellizze, 01 de julho de 2024. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?pesquisaAmigavel=+2146806&b=DTXT&numDocsPagina=10&i=1&O=&ref=&processo=&ementa=&nota=&filtroPorNota=&orgao=&relator=&uf=&classe=&data=&dtpb=&dtde=&tp=T&operador=e&p=true&livre=2146806. Acesso em: 14 de mai. 2025.

Fazendo remissão ao Resp. 1.758.799, de relatoria da Ministra Nancy Andrighi:

> “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.”

Observa-se, a ênfase na autodeterminação informativa, mesmo considerando-se a previsão de *credit scoring*, o que se aproxima dos parâmetros lançados pelo Supremo Tribunal Federal, assim como os limites a exploração econômica dos mesmos e as consequências para os direitos da personalidade.

Registre-se, porém, considerando-se tratar de decisões monocráticas, a ausência de uniformidade no Superior Tribunal de Justiça ao tratar dos consectários irradiados pelo *credit scoring*.

No colegiado, entretanto, parece prevalecer um esforço para proteção dos dados após sua captação, o que se percebe nos Resp. 2.133.261 e 2.115.461 de relatoria da Ministra Nancy Andrighi, a discussão envolvendo ainda “banco de dados” para efeitos de *credit scoring* - formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito - julgado em outubro de 2024, com suporte jurídico nas Leis nº 12.414/2011 e nº 13.709/2018.

O caso chegou à análise do tribunal superior por recurso da parte autora, por descobrir que seus dados pessoais oriundos do banco de dados, tinham sido comercializados sem sua autorização ou comunicação prévia. Relevante registrar como o Superior Tribunal de Justiça entendeu assegurar a autodeterminação informativa na captação de dados para o *credit scoring*, afirmando tratar-se de hipótese distinta da que originou o Tema 710, cingindo-se a discussão a gestão do banco de dados e sua cessão a terceiros sem comunicação ou consentimento. Partindo da seguinte premissa:

> “4. O gestor de banco de dados com a finalidade de proteção do crédito, pode realizar o tratamento de dados pessoais não sensíveis e abrir cadastro com informações de adimplemento de pessoas naturais e jurídicas, sem o consentimento prévio do cadastrado, em observância aos arts. 4º, I, da Lei nº 12.414/2011 e 7º, X, da LGPD.”

Afirmando que no presente caso a ausência de consentimento na captação somente se justifica em face da previsão expressa de lei específica – Lei nº 12.414/2011, resguardando-se, porém, sua disponibilização:

> “5. Todavia, o gestor de banco de dados regido pela Lei nº 12.414/2011 somente pode disponibilizar a terceiros consulentes (I) o score de crédito, sendo desnecessário o consentimento prévio; e (II) o histórico de crédito, mediante prévia autorização específica do cadastrado (nos moldes do Anexo do Decreto nº 9.936/2019), conforme o art. 4º, IV, "a" e "b" da referida lei.
>
> 6. Por outro lado, em observância o inciso III do art. 4º da Lei nº 12.414/2011, as informações cadastrais e de adimplemento armazenadas somente podem ser compartilhadas com outros bancos de dados, que são geridos por instituições devidamente autorizadas para tanto na forma da lei e regulamento.
>
> 7. Portanto, se um terceiro consulente tem interesse em obter as informações cadastrais do cadastrado, ainda que sejam dados pessoais não sensíveis, deve ele obter o prévio e expresso consentimento do titular, com base na autonomia da vontade, pois não há autorização legal para que o gestor de banco de dados disponibilize tais dados aos consulentes.
> 8. Em relação à abertura do cadastro pelo gestor de banco de dados, embora não seja exigido o consentimento prévio, é necessária a comunicação ao cadastrado, inclusive quanto aos demais agentes de tratamento, podendo exigir o cancelamento do seu cadastro a qualquer momento, nos termos do art. 4º, I e § 4º, da Lei nº 12.414/2011, além de exercer os demais direitos previstos em lei quanto aos seus dados.”

Na oportunidade consignou a Relatora que o tratamento de dados para os fins propostos, submete-se a um microssistema formado pelo Código de Defesa do

Consumidor, Lei nº 12.414/2011[27] (Lei do Cadastro Positivo), Lei nº 12.965/2014[28] (Marco Civil da Internet) e Lei nº 13.709/2018. Afirmando quanto à autodeterminação informativa que:

> "O art. 2º da LGPD aponta entre os fundamentos da disciplina da proteção dos dados pessoais o respeito à privacidade, a autodeterminação informativa e a inviolabilidade da intimidade, da honra e da imagem. 56. Ao lado dos fundamentos, a LGPD estabeleceu uma série de princípios que devem ser observados nas atividades de tratamento de dados pessoais. 57. Destaca-se, nesse contexto, o princípio da finalidade, segundo o qual o tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I). 58. O princípio da adequação, por sua vez, preceitua que deve existir compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II) 59. Merece menção, ainda, o princípio da transparência, que garante aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI).
>
> (…)
>
> Isso porque, conforme aponta a doutrina, "o tratamento de informações – positivas ou negativas – pelas entidades de proteção ao crédito é atividade potencialmente ofensiva a direitos da personalidade do consumidor (privacidade e honra). Embora relevantes para o mercado e para o consumidor, as entidades [...] devem observar rigorosamente os limites e requisitos estabelecidos pela lei, sob pena de ofensa a direitos da personalidade e, consequentemente, surgimento do dever de indenizar os danos morais e materiais causados aos consumidores" (Bessa, 2014, p. 53).

---

[27] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.133.261**. Isalete Helena Silva e Boa Vista Serviços S.A […] Credit Scoring. Distinção. Banco de Dados Regido pela Lei Nº 12.414/2011. Tratamento e Abertura do Cadastro sem Consentimento. Possibilidade. Comunicação. Necessidade. Disponibilização dos Dados do Cadastrado. Hipóteses Previstas Na Lei Nº 12.414/2011. Informações Cadastrais e de Adimplemento. Possibilidade de Compartilhamento apenas a outros Bancos de Dados. Restrição Legal quanto aos Dados que podem ser disponibilizados a terceiros Consulentes. Inobservância quanto aos deveres legais de tratamento de dados pelo gestor de banco de dados. Disponibilização indevida de dados do cadastrado. Dano Moral Presumido. Responsabilidade objetiva do gestor de banco de dados [...]. Relator: Minª. Nancy Andrighi, 08 de outubro de 2024. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202401096099&dt_publicacao=10/10/2024. Acesso em: 14 de mai. 2025.

[28] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.115.461**. Aira Alves Pereira Tavares Freitas e SERASA S.A […] Credit Scoring. Distinção. Banco de Dados Regido pela Lei Nº 12.414/2011. Tratamento e Abertura do Cadastro Sem Consentimento. Possibilidade. Comunicação. Necessidade. Disponibilização dos Dados do Cadastrado. Hipóteses Previstas Na Lei Nº 12.414/2011. Informações Cadastrais E De Adimplemento. Possibilidade De Compartilhamento Apenas A Outros Bancos De Dados. Restrição Legal Quanto Aos Dados Que Podem Ser Disponibilizados A Terceiros Consulentes. Inobservância Quanto Aos Deveres Legais De Tratamento De Dados Pelo Gestor De Banco De Dados. Disponibilização Indevida De Dados Do Cadastrado. Dano Moral Presumido. Responsabilidade Objetiva Do Gestor De Banco De Dados [...]. Relator: Minª. Nancy Andrighi, 08 de outubro de 2024. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202304537984&dt_publicacao=14/10/2024. Acesso em: 14 de mai. 2025.

> Como se observa daquele precedente, que tratou de hipótese de compartilhamento de dados do cadastrado sem a sua informação, a configuração do dano moral decorre do evidente sentimento de insegurança experimentado pela parte ao perceber que seus dados foram disponibilizados indevidamente para terceiros, favorecendo a prática de atos ilícitos ou contratações fraudulentas por eventuais terceiros de má-fé.
> Ressalta-se que a referida sensação de insegurança não pode ser considerada como mero dissabor, pois se trata de uma situação praticamente irreparável, sendo quase impossível que o titular tenha o real controle sobre o tratamento de seus dados após serem disponibilizados de forma indevida a terceiros. Tal circunstância prejudica, ainda, o próprio exercício dos direitos que o titular tem em relação aos dados."

Assentando por fim, que após captados os dados, perde-se seu controle e a resposta judicial a tal fato resume-se a indenização nos termos dos arts: 42 e 43 da Lei nº 13.709/2018[29] somente:

> "9. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do titular - dentre os quais se incluem 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. Precedente.
>
> 10. A disponibilização indevida de dados pessoais pelos bancos de dados para terceiros caracteriza dano moral presumido (in re ipsa) ao cadastrado titular dos dados, diante, sobretudo, da forte sensação de insegurança por ele experimentada.
> 11. O gestor de banco de dados que disponibiliza para terceiros consulentes o acesso aos dados do cadastrado que somente poderiam ser compartilhados entre bancos de dados - como as informações cadastrais - deve responder objetivamente pelos danos morais causados ao cadastrado, em observância aos arts. 16 da Lei nº 12.414/2011 e 42 e 43, II, da LGPD."

---

[29] **Lei 13.709/2018:** Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de mai. 2025.

Por se tratarem de decisões colegiadas, já podemos afirmar a superação do mero dessabor quanto ao vazamento de dados, com dano moral presumido, superando-se também a ideia inicial de comprovação do dano, sendo relevante trazer novamente: “Ressalta-se que a referida sensação de insegurança não pode ser considerada como mero dissabor, pois se trata de uma situação praticamente irreparável, sendo quase impossível que o titular tenha o real controle sobre o tratamento de seus dados após serem disponibilizados de forma indevida a terceiros. Tal circunstância prejudica, ainda, o próprio exercício dos direitos que o titular tem em relação aos dados.”

Além da afirmação de um microssistema a ser observado quanto a captação e tratamento de dados, formado pelo Código de Defesa do Consumidor, Lei nº 12.414/2011 (Lei do Cadastro Positivo), Lei nº 12.965/2014 (Marco Civil da Internet) e Lei nº 13.709/2018.

Nesse sentido, duas decisões colegiadas de relatoria do Ministro Ricardo Villas Bôas Cueva, de dezembro de 2024, reaproximaram novamente os tribunais.

No Resp. 2.147.374[30] de relatoria do Ministro Ricardo Villas Bôas Cueva, de dezembro de 2024, ao se manifestar sobre a possibilidade de responsabilização de agente de tratamento por vazamento de dados ocorrido de forma ilícita, fez referência ao decido pelo Supremo Tribunal Federal nas ADIs 6387, 6388, 6389, 6390 e 6393 e registrou:

> “2. Ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), a Emenda Constitucional nº 115/2022 inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa.”

[30] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.147.374**. Eletropaulo Metropolitana Eletricidade de São Paulo S.A e Thayna Nayara da Silva Queiroz […] Lei Geral de Proteção de Dados Pessoais. Direito à Privacidade, à Liberdade e à Autodeterminação Informativa. Agente de Tratamento. Vazamento de Dados não Sensíveis do Titular. Incidente de Segurança. Ataque Hacker. Responsabilidade Exclusiva de Terceiro. Não comprovada. Responsabilidade Civil Proativa. Expectativa de legítima proteção. Compliance e regulação de risco da atividade [...]. Relator: Min. Ricardo Villas Boas Cueva, 03 de dezembro de 2024. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202202209228&dt_publicacao=06/12/2024. Acesso em: 14 de mai. 2025.

Introduzindo na análise, contornos em face do Compliance e limitação tecnológica no momento do tratamento:

> “4. Compliance de dados é o esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados. Referido instrumento assume importância central ao induzir não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade. 5. O tratamento de dados pessoais configurou-se como irregular quando deixou de fornecer a segurança que o titular dele poderia esperar ("expectativa de legítima proteção"), consideradas as circunstâncias relevantes, entre as quais as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, III, da LGPD).”

O tangenciamento entre o conceito de consentimento informado aplicado ao ato médico e à autodeterminação informativa, mencionado no capítulo três, encontra nessa manifestação um ponto em comum na análise quando o relator se refere a tecnologia disponível no momento do tratamento, assim como a tecnologia disponível no momento do ato médico para efeito de responsabilidade.

Trata-se de restringir a responsabilidade de acordo com os mecanismos de segurança disponíveis no momento do tratamento, entendendo que não se pode analisar a responsabilidade com o conhecimento do desenvolvimento atual a ato omissivo ou comissivo praticado em momento passado, porém, exige a demonstração inconteste de que não era possível outra forma de garantir a segurança dos dados. Vejamos:

> “Aliás, a doutrina tem debatido quanto à natureza da responsabilidade civil prevista pela LGDP. Para além da clássica dicotomia entre as vertentes objetiva e subjetiva, há autores que defendem um novo sistema de responsabilização, denominado de responsabilidade civil proativa, conforme consignado pelo TJSP.
> Nessa leitura, "[a] nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de 'prestação de contas'. Esse novo sistema de responsabilidade, que vem sendo chamado de 'responsabilidade ativa' ou 'responsabilidade proativa' encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também 'demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, 'não descumprir a lei, não é mais suficiente'. (...) Exige-se, em síntese, atitudes conscientes, diligentes e proativas por parte das empresas em relação à utilização dos dados pessoais. Assim, a partir de agosto de 2020, quando entra em vigor a LGPD, qualquer empresa que processe dados pessoais, terá não apenas que cumprir a lei, mas também terá que provar que está em conformidade com a Lei. Caberá às empresas, em vez de à Administração Pública, a responsabilidade de identificar os próprios riscos

> e escolher e aplicar as medidas apropriadas para mitigá-los." (Moraes; Queiroz, 2019).”

Não afastando, porém, a necessidade de atualização permanente em consonância com as novas tecnologias, a fim de evitar vazamentos futuros em face dos novos mecanismos tecnológicos.

No Recurso Especial nº 2.147.374[31], também de relatório do Ministro Ricardo Villas Bôas Cueva, de dezembro de 2024, o Superior Tribunal de Justiça deu o tom das responsabilidades e alguns parâmetros genéricos de análise, que no caso sob exame, trouxeram certa clareza, principalmente por se tratar de decisão colegiada.

No caso sob análise, o vazamento de dados teria supostamente ocorrido sem autorização do agente responsável pelo armazenamento e tratamento, fato que não afastou a responsabilidade do agente de tratamento[32].

---

[31] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.147.374**. Eletropaulo Metropolitana Eletricidade de São Paulo S.A e Thayna Nayara da Silva Queiroz. Lei Geral de Proteção de Dados Pessoais. Direito à Privacidade, à Liberdade e à Autodeterminação Informativa. Agente de Tratamento. Vazamento de Dados não Sensíveis do Titular. [...]. Relator: Min. Ricardo Villas Bôas Cueva, 04 de dezembro de 2024. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202202209228&dt_publicacao=06/12/2024. Acesso em: 14 de mai. 2025.

[32] Lei 13.709/2018: Art. 5º Para os fins desta Lei, considera-se: (…) IX - agentes de tratamento: o controlador e o operador; Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. 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. Art. 45. As hipóteses de

Na ocasião o acórdão reafirmou o texto normativa da Lei nº 13.709/2018, sendo expresso ao afirmar que ao se subsumir a categoria de agente de tratamento, as cautelas de segurança exigidas no tratamento dos dados vão além da praxe simplória de armazenamento privado, mas exigem camadas de segurança e acesso restrito, estruturado de forma a atender aos requisitos de segurança, padrões de boas práticas, de governança, princípios gerais da LGPD e demais normas regulamentares, trazendo, como já afirmamos um tom mais elucidativo:

> 2. Ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), a Emenda Constitucional nº 115/2022 inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa.
> 3. A empresa recorrente, pelo fato de se enquadrar na categoria dos agentes de tratamento, tinha a obrigação legal de tomar todas as medidas de segurança esperadas pelo titular para que suas informações fossem protegidas, e seus sistemas utilizados para o tratamento de dados pessoais deveriam estar estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares.
> 4. Compliance de dados é o esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados. Referido instrumento assume importância central ao induzir não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade.
> 5. O tratamento de dados pessoais configurou-se como irregular quando deixou de fornecer a segurança que o titular dele poderia esperar ("expectativa de legítima proteção"), consideradas as circunstâncias relevantes, entre as quais as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, III, da LGPD).
>
> (…)
>
> 7. Assim, correta a conclusão do TJSP de concretizar os direitos do titular ao condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, bem como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD).

---

violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de mai. 2025.

O que se percebe é que a garantia da autodeterminação informativa, nestes termos, atribui ao agente de tratamento um ônus de prova absoluto, quando as empresas passam a explorar os dados pessoais.

E aqui há uma alteração de referencial relevante, diante da relação de forças que se estabelece entre a aquele que faz a captação de dados e seu tratamento, e a pessoa que fornece. A autodeterminação informativa é um ônus de prova no qual estão presentes condições a serem demonstradas para sua legitimidade:

> 1. No que diz respeito ao Compliance de dados:
>
>   - demonstrar as técnicas de tratamento;
>   - consonância com os princípios da LGPD;
>   - declaração expressa de consonância com a finalidade do tratamento e para cada compartilhamento.
>
> 2. Ausência de vicio de vontade.
> 3. Tempo de tratamento;
> 4. Comprovação e notificação sobre a extinção dos dados.

E por que assim se faz necessário, porque o tratamento de dados pessoais, como afirma o relator, particularmente em processos automatizados é uma atividade de risco, não estando distante de um limiar de exposição deliberada e abusiva.

Quando parecia que o Superior Tribunal de Justiça e o Supremo Tribunal Federal tratavam do tema de forma uniforme, o Resp. 2.121.904[33], de relatória da Ministra Nancy Andrighi, julgado em fevereiro de 2025, tendo como tema o vazamento de dados sensíveis por operadora de seguro, mais uma vez restringe a análise a divisão estática entre dados não sensíveis e dados sensíveis nos termos da Lei nº 13.709/2018:

> "6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, caput e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º).
> 7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação,

[33] BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.121.904**. Prudential do Brasil Seguros de Vida S.A e Pedro Henrique Camiloti […] Contrato de Seguro de Vida. Relação de Consumo. Código de Defesa do Consumidor. Lei Geral de Proteção de Dados. Vazamento de Dados Sensíveis. Responsabilidade Objetiva. Dano Moral Presumido [...]. Relator: Minª. Nancy Andrighi, 11 de fevereiro de 2025. Disponível em: scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202400312927&dt_publicacao=17/02/2025. Acesso em: 14 de mai. 2025.

> sobretudo os que incidem sobre “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico” (art. 5º, II, da LGPD).
> 8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD).”
>
> (...)
>
> 15. O art. 2º da LGPD aponta entre os fundamentos da disciplina da proteção dos dados pessoais o respeito à privacidade, a autodeterminação informativa e a inviolabilidade da intimidade, da honra e da imagem.
>
> (...)
>
> 21. Sobre o art. 44 da LGPD, inclusive, Bruno Miragem esclarece que “a regra coloca em destaque, assim como ocorre em relação à responsabilidade do fornecedor no CDC, a questão relativa aos riscos do desenvolvimento, uma vez que delimita a extensão do dever de segurança àquela esperada em razão das 'técnicas de tratamento de dados disponíveis à época em que foi realizado' e, considerando “a previsibilidade de uma atualização e avanço técnico em atividades vinculadas à tecnologia da informação, mais veloz do que em outras atividades econômicas” (Miragem, 2019).
>
> (...)
>
> 51. Desse modo, se esta Terceira Turma, como visto, possui entendimento de que, mesmo no contexto de dados não sensíveis, a transferência a terceiros, sem o consentimento do titular, gera a responsabilização do fornecedor, com ainda mais razão tal conclusão se aplica na hipótese de vazamento de dados pessoais sensíveis do consumidor.
> 52. Portanto, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera a responsabilização objetiva da seguradora e a caracterização de dano moral presumido, o que demonstra, na hipótese, a inexistência de elementos para a reforma do acórdão recorrido.”

Todavia, com uma percepção mais uniforme quando afirma: “Desse modo, se esta Terceira Turma, como visto, possui entendimento de que, mesmo no contexto de dados não sensíveis, a transferência a terceiros, sem o consentimento do titular, gera a responsabilização do fornecedor, com ainda mais razão tal conclusão se aplica na hipótese de vazamento de dados pessoais sensíveis do consumidor.”

5. CONSIDERAÇÕES FINAIS

O que se percebe, é que durante muito tempo os dados pessoais foram fornecidos pelos seus titulares em atos cotidianos e de forma contínua, sem que se tivesse dimensão que se pudesse chegar a um estágio tão avançado e preocupante de tratamento automatizado de dados. Fato inconteste é que uma vez fornecidos esses dados nessas relações cotidianas, perde-se totalmente o controle sobre eles.

A percepção e apropriação do conceito de Direito da Personalidade e de seu viés da Autodeterminação Informativa em relação a captação e tratamento de dados, passam a ser relevantes na tentativa de resguardar um mínimo de privacidade e autonomia dentro dessa nova realidade.

A princípio, este trabalho partiu da hipótese de que o centro da discussão jurídica estaria na autodeterminação informativa e na privacidade, compreendida como a autonomia do titular na conformação do direito à proteção de dados, como prerrogativa de impedir intromissões indevidas em sua intimidade e vida privada. Todavia, no curso da pesquisa, identificou-se que a autodeterminação informativa representa apenas uma das variáveis do problema, sendo o objeto real de atenção os próprios bancos de dados, enquanto estruturas de poder que organizam, armazenam e direcionam o uso dos dados.

As manifestações do Supremo Tribunal Federal parecem ir de encontro a essa percepção, por mais que se observe o cuidado do Supremo Tribunal Federal em trazer as discussões à autodeterminação informativa como conceito direcionador de todo tratamento de dados, suas decisões demonstram que o foco tende a se deslocar da autonomia do indivíduo para a conformação jurídica da formação, circulação e destinação dos dados pessoais. Como destacam Sarlet e Ruaro (2021), o problema central não reside apenas na proporcionalidade do tratamento, mas no próprio compartilhamento inicial dos dados.

Não se pode chegar a conclusão diversa, senão daquela que afirma que no momento em que estamos não há mecanismos suficientes para garantir a privacidade dos dados, para garantir a intimidade, e resguardar o direito da personalidade. É uma grande ilusão acreditar que no atual momento do desenvolvimento tecnológico de captação de dados, há uma correspondência nos mecanismos de segurança suficiente para impedir a exploração dos dados sem autorização dos titulares. A

comparação com o estágio de desenvolvimento da energia nuclear antes de Chernobyl é pertinente: evoluiu-se exponencialmente na capacidade de fissão, sem o devido avanço nos sistemas de contenção, com consequências previsíveis.

A apropriação de dados pessoais tem ocorrido à margem de uma regulação eficaz, permitindo-se que informações pessoais sejam convertidas em dados sensíveis, por meio de práticas como o perfilamento automatizado, muitas vezes sem consentimento real e informado do titular. Uma vez capturados, os dados escapam ao controle individual, e as salvaguardas previstas nas normas que formam, segundo o Superior Tribunal de Justiça, o microssistema de proteção do banco de dados, formado pelo Código de Defesa do Consumidor, Lei nº 12.414/2011 (Lei do Cadastro Positivo), Lei nº 12.965/2014 (Marco Civil da Internet) e Lei nº 13.709/2018 se mostram insuficientes diante de uma realidade muito mais dinâmica. O tratamento de dados revela fragilidades profundas, não só compromete a privacidade e a intimidade, como também abre espaço para interferências comportamentais e exploração de vulnerabilidades.

Os mecanismos de reparação, por sua vez, posteriores e indenizatórios, ocorrem quando o dano, muitas vezes irreversível, já foi causado na memória daquele que teve os dados expostos ou na memória daqueles que ficaram, pela sensação de insegurança permanente, inerente a sua divulgação incerta e não sabida. Sendo na verdade de somenos importância, caracterizando-se mais como perdas e danos do que de fato como objeto principal, uma vez que o que se requer é o desaparecimento do referido dado daquele universo.

Diante disso, pode-se afirmar que o foco da proteção jurídica precisa migrar da autodeterminação informativa para os bancos de dados, compreendidos como estruturas dinâmicas de poder que exigem controle, uma vez que a autodeterminação informativa, como categoria jurídica já está razoavelmente regulada pelos princípios do direito civil, da autonomia da vontade, dos vícios de consentimento e do consentimento informado. Há um exaurimento dentro dessa perspectiva da legitimidade da manifestação da vontade, e é possível observar isso quando as decisões dos tribunais superiores mencionam como fundamento inicial, mas sem aprofundar sobre o tema, dando a entender que é algo sobre o qual não há controvérsias relevantes, ao contrário da formação, tratamento e objeto dos bancos de dados, sobre os quais as decisões navegam com avanços e retrocessos, sempre

a procurado de uma referência normativa mais explicita ou suficiente.

O que permanece sem resposta é o tratamento dos dados após sua captação. O verdadeiro campo de disputa é o tratamento, armazenamento e circulação dos dados dentro de sistemas cada vez mais complexos, a ponto de impedirem o conhecimento mediano de os alcançar, principalmente quanto ao estágio de desenvolvimento da mineração de dados com uso da inteligência artificial.

Além disso, mostrou-se equivocada e inicialmente também assumida por este trabalho, a confiança na eficácia da distinção normativa entre dados pessoais e dados sensíveis. A realidade demonstrou que, com a atual capacidade tecnológica, qualquer dado pode adquirir sensibilidade em função de sua combinação com outros, possibilitando inferências profundas sobre a identidade do indivíduo.

O risco do processamento se encontra na finalidade e nas possibilidades do processamento, e não na natureza do dado pessoal, não apenas no núcleo íntimo, como a narrativa comercial quer construir, mas também nas demais informações que lhe dizem respeito. Assim, a divisão normativa entre dados não sensíveis e dados sensíveis se torna irreal, como a percepção de proteção de dados nos termos propostos pelos normativos existentes. Desconsiderar isso significa aplicar uma proteção insuficiente, expondo as pessoas à exploração econômica de sua existência virtual e à violação de sua dignidade.

O que se alerta, é que a divisão entre dados pessoas e dados pessoais sensíveis não consegue resistir a capacidade tecnológica de tratamento de dados existente, e desconsiderar esse fato, nos leva a uma proteção deficiente e insuficiente da privacidade com ofensa direta a dignidade das pessoas, e abertura para a exploração desses dados.

A promulgação da Emenda Constitucional nº 115/2022, por sua vez, ao elevar expressamente a proteção de dados ao patamar de direito fundamental, representa um marco importante, ao reafirmar a linha jurisprudencial já delineada nas ADIs 6387 e 6649. Essa mudança constitucional autoriza uma nova interpretação do sistema jurídico, mais atenta à fluidez dos riscos e às transformações tecnológicas em curso, permitindo superar a visão estática da Lei 13.709/2018.

Somando-se a ideia de um direito geral de personalidade fundamental de conceito aberto visando a proteger o indivíduo como um todo, inclusive perante novos

perigos (Ody; Cunha, 2021, p. 5).[34] A proteção de dados precisa ser entendida como um desdobramento do direito geral de personalidade, um direito fundamental de natureza aberta, voltado à defesa integral do ser humano diante dos novos riscos impostos pela tecnologia. A proteção efetiva exige uma vigilância constante e uma revisão dinâmica dos marcos normativos.

O controle dos dados já não está nas mãos do titular, e o simples consentimento tornou-se insuficiente diante da complexidade do tratamento automatizado. A sofisticação dos sistemas de tratamento de dados e o uso intensivo de inteligência artificial demandam uma superação das dicotomias normativas, como a separação rígida entre dados sensíveis e não sensíveis em prol de uma abordagem mais realista e dinâmica. Proteger dados, hoje, é proteger o próprio ser humano contra a coisificação mercadológica. A consagração constitucional e infraconstitucional da proteção de dados foi um marco, mas se observa ser apenas o início de uma jornada de vigilância constante, atualização normativa e, sobretudo, coragem interpretativa.

[34] O desastre de Chernobil ou acidente de Chernobil foi um acidente nuclear ocorrido em 26 de abril de 1986 no reator nuclear nº 4 da Usina Nuclear de Chernobil, perto da cidade de Pripiate, no norte da Ucrânia Soviética, próximo da fronteira com a Bielorrússia Soviética. O acidente ocorreu durante um teste de segurança que simulava uma falta de energia da estação, durante a qual os sistemas de segurança de emergência e de regulagem de energia foram intencionalmente desligados. Uma combinação de falhas inerentes no projeto do reator, bem como dos operadores dos reatores que organizaram o núcleo de uma maneira contrária à lista de verificação para o teste, resultou em condições de reação descontroladas. A catástrofe de Chernobil é considerada o acidente nuclear mais desastroso da história, tanto em termos de custo quanto de baixas. Disponível em: https://pt.wikipedia.org/wiki/Acidente_nuclear_de_Chernobil. Acesso em: 04 de mai. 2025.

REFERÊNCIAS

ALBERS, M. Realizing the Complexity of Data Protection. *In:* GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Edit.). **Reloading Data Protection:** Multidisciplinary Insights and Contemporary Challenges. Berlin: Springer, 2014.

ADJEI, J. K. **Monetization of Personal Identity Information:** Technological and Regulatory Framework. IEEE Computer Society Washington, Washington DC/EUA, 14 dez. 2015.

ALEXY, R. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2012.

AMARAL, F. **Direito Civil:** introdução. 5. ed., Rio de Janeiro: Renovat, 2003.

BALKIN, J. M. Fixing Social Media's Grand Bargain. **Hoover Working Group on National Security Technology**., Law, Aegis Paper Series, n. 1814, October, 2018.

BARACAT, E. M.; FERREIRA, J. B.; NEPOMUCENO, T. L. L. Arregimentação e precarização do trabalho humano via plataformas digitais. **Diké (Uesc)**, v. 23, n 25, p.194-225, jan./jun, 2024.

BERGSTEIN, L. G.; TRAUTWEIN, J. R. A proibição de discriminação e os critérios do cálculo atuarial nos contratos de seguro. **Revista ABCD**, v. 4, p. 53-67, 2022. ISSN: 2318-602X | DOI: https://doi.org/10.56119/rcabdc.v4.51.

BERGSTEIN, L. G.; KIRCHNER, F. A proteção do consumidor na União Europeia com a formação de um mercado único digital. **Campos Neutrais – Revista Latino-Americana de Relações Internacionais**., Santa Vitória do Palmar – RS, v. 2, n. 2, p. 25-46, mai./ago. 2020.

BERGSTEIN, L. G. **O tempo do consumidor nas relações de consumo: pela superação do menosprezo planejado nos mercados**. 2018., 288p. Tese (Doutorado em Direito) - Programa de Pós-graduação em Direito da Universidade Federal do Rio Grande do Sul. Porto Alegre, 2018.

BERGSTEIN, L.; MARQUES, C. L. Socialização de riscos e reparação integral do dano no direito civil e do consumidor no Brasil. **Conpedi Law Review**, ISSN - 2448-3931., Costa Rica, v. 3, n. 1, p. 250 – 278, jan./jun, 2017.

BILLIER, J. C.; MARYIOLI, A. **História da filosofia do direito**. Barueri: Manole, 2005.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BITTAR, C. A. **Os direitos da personalidade**. 8 ed. São Paulo: Saraiva, 2015.

BOBBIO, N. **A era dos direitos**. 2.ed. Rio de Janeiro: Elsevier, 2004.
BORGES, R. C. B. **Direitos de personalidade e autonomia privada**. 2.ed. São Paulo: Saraiva, 2007.

BVERFGE 65, 1. pp. 239-240. *In:* SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Konrad-Adenauer-Stiftung, 2005. Disponível em http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudenciase-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_ tribunal_constitucional_federal_alemao.pdf/view. Acesso em: 12 fev. 2025.

BRANCO, S. **Memória e esquecimento na internet**. Porto Alegre: Arquipélago Editorial, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasil: [s. n.], 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 12 fev. 2025.

BRASIL. **Lei nº 10.406, de 2002 (Código Civil).** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 12 fev. 2025.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm. Acesso em: 12 fev. 2025.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 2019.

BRASIL. **Medida provisória n. 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística. Diário Oficial da União. Brasília, DF, 17 abr. 2020a, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 23 fev. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade (ADI) 6837**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil (CFOAB). Relatora: Ministra Rosa Weber. Brasília, DF, 24 abr. 2020b. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 23 fev. 2025.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental (ADPF) 722**. Requerente: Rede Sustentabilidade. Relatora: Ministra Cármen Lúcia. Brasília, DF, 20 ago. 2020c. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354. Acesso em: 23 fev. 2025.

BRASIL. Supremo Tribunal Federal. **ADI 6387 MC-Ref**. […] Medida Provisória Nº 954/2020. Emergência de Saúde Pública de Importância Internacional decorrente do Novo Coronavírus (Covid-19). Compartilhamento de Dados dos Usuários do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal, pelas Empresas Prestadoras, com o Instituto Brasileiro de Geografia e Estatística. [...]. Relatora: Minª.Rosa Weber, 07 de maio de 2020. Acesso em: 12 de fevereiro de 2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1123008775. Acesso em: 14 de mai. 2025.

BRASIL. Supremo Tribunal Federal. **MS nº 37.968**. […] 1. Hélio Angotti Neto formalizou mandado de segurança, com pedido de liminar, contra ato do Presidente da CPI da Pandemia mediante o qual determinada a quebra de seus sigilos telefônico e telemático. [...]. Relator: Min. Nunes Marques, 11 de novembro de 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1319475725/inteiro-teor-1319475728. Acesso em: 14 de mai. 2025.

BRASIL. Supremo Tribunal Federal. **ADPF 722**. Rede Sustentabilidade e Ministro de Estado da Justiça e Segurança Pública. [...] Produção e disseminação de dossiê com informações de servidores federais e estaduais integrantes de movimento antifascismo e de professores universitários. Desvio de finalidade. Liberdades de expressão, privacidade, reunião e associação. [...]. Relatora: Min. Cármen Lúcia, 16 de maio de 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1535843211/inteiro-teor-1535843319. Acesso em: 14 de mai. 2025.

BRASIL. Supremo Tribunal Federal. **ADI 6649**. […] Tratamento de Dados Pessoais pelo Estado Brasileiro. Compartilhamento de Dados Pessoais entre Órgãos e Entidades da Administração Pública Federal. [...]. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1869237633. Acesso em: 14 de mai. 2025.

BRASIL. Supremo Tribunal Federal. **ADI 5545**. Procurador-Geral da República e Assembleia Legislativa do Estado do Rio de Janeiro. [...] Lei estadual que obriga a adoção de medidas de segurança que evitem, impeçam ou dificultem a troca de recém-nascidos nas dependências de hospitais públicos ou privados, casas de saúde e maternidades e que possibilitem a posterior identificação através de exame de DNA. Coleta do material genético de todas as mães e filhos na sala de parto [...]. Relator: Min. Luiz Fux, 13 de abril de 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=505601. Acesso em: 14 de mai. 2025.

BRASIL. Supremo Tribunal Federal. **ADI 6561**. Ação direta de inconstitucionalidade. Lei 3.528 de 2019 do Estado do Tocantins. Cadastro Estadual de usuários e dependentes de drogas. [...]. Relator: Min. Edson Fachin, 04 de setembro de 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=452449&ori=1. Acesso em: 14 de mai. 2025.

BRASIL. Supremo Tribunal Federal. **HC 222141 AgR**. […] Provedores e plataformas dos registros de conexão e registros de acesso a aplicações de Internet. 4. Congelamento do conteúdo de comunicações privadas e de dados pessoais da paciente, com base no art. 13, § 2º, do Marco Civil da Internet, por determinação do Ministério Público, sem prévia autorização judicial. Ilegitimidade. [...]. Relator: Min.Gilmar Mendes, 06 fevereiro de 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/2311573797. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. Edcl. **No Resp. 1.630.889**. […] Bancos de Dados. Proteção ao Crédito. Privacidade e Intimidade. Autodeterminação Informativa. Direitos Fundamentais. Eficácia Horizontal. Princípio da Máxima Efetividade. [...]. Relatora: Min. Nancy Andrighi, 27 de novembro de 2018. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/661802846/relatorio-e-voto-661802876. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **RMS 61302**. […] Direito a Privacidade e a Intimidade. Identificação de Usuários em determinada localização geográfica. [...]. Relator: Min. Rogerio Schietti Cruz, 26 de agosto de 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1718870495. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Resp. 1.758.799**. […] Ação de Compensação de Dano Moral. Banco De Dados. Compartilhamento de Informações Pessoais. Dever de Informação. Violação. Dano Moral. IN RE IPSA. [...]. Relatora: Minª. Nancy Andrighi, 12 de novembro de 2019. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28RESP.clas.+e+%40num%3D%221758799%22%29+ou+%28RESP+adj+%221758799%22%29.suce.&O=JT. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **A Resp. 1.673.128**. […] Apelação Cível. Ação Ordinária. Venda de Dados Sigilosos e Acesso Ilegal aos Dados do DENATRAN. [...]. Relator: Min. Herman Benjamin, 16 de junho de 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=acesso+a+dados+sigilosos. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **AResp. 2.130.619**. Eletropaulo Metropolitana Eletricidade de São Paulo S.A e Maria Edite de Souza. […] Indenização por Dano Moral. Vazamento de Dados Pessoais. Dados Comuns e Sensíveis. Dano Moral Presumido. Impossibilidade. Necessidade de Comprovação do Dan [...]. Relator: Min. Francisco Falcão, 07 de março de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=2.130.619. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.077.278**. Daniela Ferreira Ramos e BV Financeira S.A Crédito Financiamento e Investimento. […] Ação declaratória de Inexigibilidade de Débito por Vazamento de Dados Bancários Cumulada com Indenização por Danos Morais E Repetição De Indébito. Golpe Do Boleto. Tratamento De Dados Pessoais Sigilosos De Maneira Inadequada.

Facilitação da Atividade Criminosa. [...]. Relatora: Minª. Nancy Andrighi, 03 de outubro de 2023. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=211820560&tipo=5&nreg=202301909798&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20231009&formato=PDF&salvar=false. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.104.036**. Claudovir Marcasso […] Entidade mantenedora de cadastros protetivos do crédito - inclusão de dados em cadastro de proteção ao crédito - alegação de violação da lei geral de proteção de dados (LGPD) por suposta comercialização de informações - informações mantidas pela ré que não se relacionam com a intimidade da parte, tampouco abrangem dado pessoal de maior repercussão - inteligência dos ARTS. 5º, E 7º DA LEI 13.709/2018 - Exercício regular do direito - autorização do consumidor que não se mostra necessária - ilicitude não configurada [...]. Relator: Min. João Otávio de Noronha, 14 de novembro de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=art+7+lgpd. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Tema 710**. I - O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). II - Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/cdc-na-visao-do-tjdft-1/inscricao-do-nome-do-devedor-em-cadastro-de-inadimplentes-1/sistema-credit-scoring-x-plataforma-201cserasa-limpa-nome201d. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.122.613**. Elton Nascimento de Souza […] Ação de obrigação de fazer cumulada com indenização por danos morais - divulgação de dados pessoais sem prévia autorização ou consentimento - informações relacionadas aos serviços de proteção de crédito - dispensa legal de prévio consentimento do titular dos dados - art. 7º, X da Lei Geral de Proteção de Dados - inexistência de indícios de comercialização ou divulgação de dados de forma ilícita. [...]. Relator: Minª. Maria Isabel Gallotti, 12 de abril de 2024. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=993180&nreg=201000161913&dt=20120201&formato=HTML. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.132.461**. […] Manutenção de cadastro, disponível apenas para associados e com finalidade exclusiva de fornecer subsídios para proteção do crédito encontra amparo no artigo 7º, X, da Lei Geral de Proteção de Dados - Ausência de comprovação de indevida comercialização de dados - Dano moral não configurado. Precedente desta E. Corte. Inteligência da Súmula nº 550 do C. STJ e do Tema nº 710 dos Recursos Repetitivos - Litigância de má-fé não caracterizada [...]. Relator: Min. Antonio Carlos Ferreira, 29 de maio de 2024. Disponível em:

https://www.jusbrasil.com.br/jurisprudencia/busca?q=art+7+lgpd. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.146.806**. Maria do Rosário Correia dos Santos. […] Ação cominatória c/c indenizatória. Banco de dados. Compartilhamento de informações pessoais. Dever de informação. Violação. Dano moral in re ipsa. Precedente da corte superior [...]. Relator: Min. Marco Aurélio Bellizze, 01 de julho de 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=a%C3%A7%C3%A3o+cominat%C3%B3ria+cumulada+com+compensa%C3%A7%C3%A3o+por+dano+moral. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.133.261**. Isalete Helena Silva e Boa Vista Serviços S.A […] Credit Scoring. Distinção. Banco de Dados Regido pela Lei Nº 12.414/2011. Tratamento e Abertura do Cadastro sem Consentimento. Possibilidade. Comunicação. Necessidade. Disponibilização dos Dados do Cadastrado. Hipóteses Previstas Na Lei Nº 12.414/2011. Informações Cadastrais e de Adimplemento. Possibilidade de Compartilhamento apenas a outros Bancos de Dados. Restrição Legal quanto aos Dados que podem ser disponibilizados a terceiros Consulentes. Inobservância quanto aos deveres legais de tratamento de dados pelo gestor de banco de dados. Disponibilização indevida de dados do cadastrado. Dano Moral Presumido. Responsabilidade objetiva do gestor de banco de dados [...]. Relator: Minª. Nancy Andrighi, 08 de outubro de 2024. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202401096099&dt_publicacao=10/10/2024. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.115.461**. Aira Alves Pereira Tavares Freitas e SERASA S.A […] Credit Scoring. Distinção. Banco de Dados Regido pela Lei Nº 12.414/2011. Tratamento e Abertura do Cadastro Sem Consentimento. Possibilidade. Comunicação. Necessidade. Disponibilização dos Dados do Cadastrado. Hipóteses Previstas Na Lei Nº 12.414/2011. Informações Cadastrais E De Adimplemento. Possibilidade De Compartilhamento Apenas A Outros Bancos De Dados. Restrição Legal Quanto Aos Dados Que Podem Ser Disponibilizados A Terceiros Consulentes. Inobservância Quanto Aos Deveres Legais De Tratamento De Dados Pelo Gestor De Banco De Dados. Disponibilização Indevida De Dados Do Cadastrado. Dano Moral Presumido. Responsabilidade Objetiva Do Gestor De Banco De Dados [...]. Relator: Minª. Nancy Andrighi, 08 de outubro de 2024. Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/10/STJ_202304537984_tipo_integra_275287318.pdf. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.147.374**. Eletropaulo Metropolitana Eletricidade de São Paulo S.A e Thayna Nayara da Silva Queiroz […] Lei Geral de Proteção de Dados Pessoais. Direito à Privacidade, à Liberdade e à Autodeterminação Informativa. Agente de Tratamento. Vazamento de Dados não Sensíveis do Titular. Incidente de Segurança. Ataque Hacker. Responsabilidade Exclusiva de Terceiro. Não comprovada. Responsabilidade Civil Proativa. Expectativa de legítima proteção. Compliance e regulação de risco da atividade [...].

Relator: Min. Ricardo Villas Boas Cueva, 03 de dezembro de 2024. Disponível em: https://camposthomaz.com/comunicado-ct/stj-decide-sobre-responsabilidade-civil-em-incidentes-de-seguranca/#:~:text=O%20julgamento%20no%20caso%20(REsp,43%2C%20III%2C%20da%20LGPD. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.147.374**. Eletropaulo Metropolitana Eletricidade de São Paulo S.A e Thayna Nayara da Silva Queiroz. Lei Geral de Proteção de Dados Pessoais. Direito à Privacidade, à Liberdade e à Autodeterminação Informativa. Agente de Tratamento. Vazamento de Dados não Sensíveis do Titular. [...]. Relator: Min. Ricardo Villas Bôas Cueva, 04 de dezembro de 2024. Disponível em: https://camposthomaz.com/comunicado-ct/stj-decide-sobre-responsabilidade-civil-em-incidentes-de-seguranca/#:~:text=O%20julgamento%20no%20caso%20(REsp,43%2C%20III%2C%20da%20LGPD. Acesso em: 14 de mai. 2025.

BRASIL. Superior Tribunal de justiça. **Recurso Especial nº 2.121.904**. Prudential do Brasil Seguros de Vida S.A e Pedro Henrique Camiloti […] Contrato de Seguro de Vida. Relação de Consumo. Código de Defesa do Consumidor. Lei Geral de Proteção de Dados. Vazamento de Dados Sensíveis. Responsabilidade Objetiva. Dano Moral Presumido [...]. Relator: Minª. Nancy Andrighi, 11 de fevereiro de 2025. Disponível em: https://www.conjur.com.br/wp-content/uploads/2025/02/voto-Nancy-STJ-indenizacao-seguradora-vazamento-dados-sensiveis-segurado.pdf. Acesso em: 14 de mai. 2025.

CABANES, P. **Introdução à história da antiguidade**. Petrópolis: Vozes, 2009.

CACHAPUZ, M. C. **Intimidade e vida privada no novo Código Civil brasileiro:** uma leitura orientada no discurso jurídico. Porto Alegre: Sergio Antonio Fabris Editor, 2006.

CASTAÑEDA, I. M. H. **El concepto jurídico de persona**. Pamplona: Ediciones Universidad de Navarra, 1989.

CAVALIERI FILHO, S. Os Danos Morais no Judiciário Brasileiro e sua evolução desde 1988. *In:* TEPEDINO, Gustavo (org.) **Direito Civil Contemporâneo:** novos paradigmas à luz da legalidade constitucional. São Paulo: Atlas, 2008.

COHEN, J. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, p. 1373-1438, 2002.

CORRAL, H. T. **Derecho civil y persona humana:** cuestiones debatidas. Santiago: Legal Publishing Chile, 2009.

CUPIS, A. **Os direitos da personalidade**. 1.ed. Campinas, S.P.: Romana jurídica, 2004.

CHIUSI, T. A dimensão abrangente do direito privado romano: observações sistemático-teoréticas sobre uma ordem jurídica que não conhecia “Direitos

Fundamentais". *In:* MONTEIRO, António Pinto; NEUNER, Jörg; SARLET, Ingo (org.). **Direitos fundamentais e direito privado:** uma perspectiva de direito comparado. Coimbra: Almedina, 2007.

CHINELATO, S. J. A. Direito de arena, direito de autor e direito à imagem. *In:* BITTAR, Eduardo C. B.; CHINELATO, Silmara Juny (Coord.). **Estudos de direito de autor, direito da personalidade, direito do consumidor e danos morais**. Rio de Janeiro: Forense, 2002.

DAVENPORT, T. H. **Big data at work:** dispelling the myths, uncovering the opportunities. Boston: Harvard Business Review Press, 2014

DIMOULIS, D.; MARTINS, L. **Teoria geral dos direitos fundamentais**. 2.ed. São Paulo: Revista dos Tribunais, 2009.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, D. **Da privacidade à proteção de dados pessoais:** fundamentos da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters, 2020.

DRAY, G. M. **Direitos de personalidade:** anotações ao código civil e ao código do trabalho. Coimbra: Almedina, 2006.

FLUMIGNAN, S. J. G.; FLUMIGNAN, W. G. G. **Princípios que regem o tratamento de dados no Brasil**. *In:* Comentários à Lei Geral de Proteção de Dados Lei nº. 13.709/2018, com alteração da Lei nº. 13.853/201. LIMA, Cíntia Rosa Pereira de (coordenadora). São Paulo: Almedina, 2020.

GAGLIANO, P. S.; PAMPLONA FILHO, R. **Novo Curso de Direito Civil**. volume VI, Direito de Família: As famílias em perspectiva constitucional, 2. ed. São Paulo: Saraiva, 2012

GONÇALVES, C. R. **Direito civil brasileiro:** parte geral. 8.ed. São Paulo: Saraiva, 2010.

GUIMARÃES, J. A. S. A.; GUIMARÃES, A. J. S. A. A Liberdade de Expressão e o Direito ao Esquecimento. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ**. Rio de Janeiro, v. 4 n. 1, jan./abr., 2021.

GUNTHER, L. E.; MACEI, D. N.; DONATE, G. M. H. B. A relação entre os direitos fundamentais e os tributos. **Rev. Campo Jurídico**. Barreiras-BA, v.8, n.1, p.82-95, jan./jun, 2020.

HIRATA, A. **Direito à privacidade**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

HESSE, K. **Elementos de direito constitucional da República Federal da Alemanha**. Tradução: Luís Afonso Heck. Porto Alegre: Sergio Antonio Fabris Editor, 1998.

JAPIASSÚ, H. O racionalismo cartesiano*. In:* RESENDE, Antonio (org.). **Curso de filosofia: para professores e alunos dos cursos de segundo grau e de graduação**. 12.ed. Rio de Janeiro: Jorge Zahar, 2004.

KAISER, B. **Manipulados:** como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. Tradução Roberta Clapp; Bruno Fiuza. Rio de Janeiro: Harper Collins, 2020.

KELLOGG, K.; VALENTINE, M.; CHRISTIN, A. Algorithms at work: the new contested terrain of control. **Academy of Management Annals**, Reino Unido, v. 14, n. 1, p. 366-410, 2020.

KORKMAZ, M. R. D. C. C. **Dados sensíveis na lei geral de proteção de dados pessoais:** mecanismos de tutela para o livre desenvolvimento da personalidade. 2019; p. 118. Dissertação (Mestrado em Direito e Inovação) - Universidade Federal de Juiz de Fora, 2019.

LEONARDI, P. M.; TREEM, J. W. Behavioral visibility: a new paradigm for organization studies in the age of digitization, digitalization, and datafication. **Organization Studies**, Reino Unido, v. 41, n. 12, p. 1601- 1625, 2020.

LIMBERGER, T. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LUÑO, A. E. P. **Los derechos humanos em la sociedad tecnologica**. Madrid: Universitas, 2012.

MARCACINI, A. T. R. **Regras Aplicadas ao Tratamento de Dados Pessoais**. *In:* Comentários à Lei Geral de Proteção de Dados Lei nº. 13.709/2018, com alteração da Lei nº. 13.853/201. LIMA, Cíntia Rosa Pereira de (coordenadora). São Paulo: Almedina, 2020.

MACEI, D. N. **O princípio da verdade material no processo tributário**. 2012 188p. Tese (Doutorado em Direito Tributário) – Pontíficia Universidade Católica de São Paulo. São Paulo, 2012.

MACEI, D. N.; SILVA, R. S. D. R. Moralidade Tributária - Instrumentos Para Análise. **ANIMA: Revista Eletrônica do Curso de Direito das Faculdades OPET**. Curitiba-PR. Ano X, n. 17, jul/dez-2017. ISSN 2175-7119.

MACHADO, A. C. C.; CHINELLATO, S. J. A. (Coord.). **Código Civil interpretado: artigo por artigo, parágrafo por parágrafo**. 6. ed. Barueri: Manole, 2013.

MARQUES, C. L.; MIRAGEM, B. **O Novo Direito Privado e a Proteção dos Vulneráveis**. São Paulo: Revista dos Tribunais, 2012.

MELLO, C. A. Contribuição para uma teoria híbrida dos direitos de personalidade. *In:* SARLET, Ingo Wolfgang (org.). **O novo código civil e a constituição**. 2.ed. Porto Alegre: Livraria do Advogado, 2006.

MENDES, L. S. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. 2008. Tese de Mestrado em Direito – Universidade de Brasília. Brasília, 2008.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva Educação, 2014. (Série IDP: linha de pesquisa acadêmica).

MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. **Pensar: Revista de Ciências Jurídicas**. Fortaleza. v. 25, n. 4, p. 1-18, out./dez, 2020.

MORAES, M. C. B. Apresentação. *In:* RODOTÁ, Stefano. **A vida na sociedade de vigilância:** privacidade hoje. Rio de Janeiro: Renovar, 2008.

MORAES, M. C. B. **Na medida da pessoa humana:** estudos de direito civil. Rio de Janeiro: Renovar, 2010.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de Direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **R. Dir. Gar. Fund.**, Vitória, v. 19, n. 3, p. 159-180, set./dez, 2018.

NASCIMENTO, D. M. **Conceito de Dados Pessoais abarcados pela Lei Geral de Proteção de Dados Pessoais (LGPD)**, [s. l.], 5 jul. 2019. Disponível em: https://advocaciadeboramn.jusbrasil.com.br/artigos/728965462/conceito-de-dadospessoais-abarcados-pela-lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em: 12 fev. 2025.

ODY, L. F. W.; CUNHA, A. S. A **Construção Jurisprudencial de um direito fundamental de proteção de dados:** análise do volkszählunsurteil e seus reflexos na ADI 6.387. Teoria Jurídica Contemporânea. Rio de Janeiro. v. 6. 2021.

OHLIN, J. Is the concept of the person necessary for human rights? **Columbia Law Review**, v. 104-105, 2005.

OLSON, E. **Personal Identity**. The Stanford Encyclopedia of Philosophy, 2010. Disponível em: http://plato.stanford.edu/archives/win2010/entries/identity-personal/. Acesso em: 14 fev. 2025.

O'NEIL, C. **Weapons of math destruction:** how big data increases inequality and threatens democracy. London: Penguin Books, 2018.

PINHEIRO, P. P. **Proteção de Dados Pessoais**. Comentários à nº Lei 13.709/2018. 3. ed. São Paulo, Saraiva, 2020.

PECCICACCO, M.; SOUZA, D. A. A preservação da dignidade da pessoa humana por meio do uso ponderado dos dados pessoais regido pelos limites da razoabilidade e proporcionalidade. *In:* WALDMAN, Ricardo Libel; BARRETO, Waldman (orgs.). **Direitos humanos, ética e democracia na sociedade da informação II**. - São Paulo: Ed. dos Autores, 2021.

PECES-BARBA, M. G. **Curso de derechos fundamentales:** teoría general. Madrid: Boletín Oficial del Estado, 1995.

QUEIROZ, R. M. R.; PONCE, P. P. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**., São Paulo, n.1, v. 1, p. 64-90, 2020.

REALE, M. **Lições preliminares de direito**. 27. ed. São Paulo: Saraiva, 2009.

RODOTÀ, S. **A vida na sociedade da vigilância – A privacidade hoje**. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 92.

SARLET, I. W. A influência dos direitos fundamentais no direito privado: o caso brasileiro. *In:* MONTEIRO, António Pinto; NEUNER, Jörg; SARLET, Ingo (org.). **Direitos fundamentais e direito privado:** uma perspectiva de direito comparado. Coimbra: Almedina, 2007.

SARLET, I. W. Direitos fundamentais em espécie. *In:* MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfang. **Curso de direito constitucional**. (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2013.

SARLET, G. B. S.; RUARO, R. L. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Rev. direitos fundam. democ**., v. 26, n. 2, p. 81-106, mai./ago, 2021.

SILVA, J. A. **Curso de direito constitucional positivo**. 34.ed. São Paulo: Malheiros, 2011.

SOLOVE, D. J. Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, v. 126, pp. 1880-1903, 2013.

SOUSA, R. V. A. C. **O direito geral de personalidade**. Coimbra: Coimbra, 2011.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário 1.010.606 – RJ, de 11 fev. 202**1. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755910773. Acesso em: 20 de fev. 2025.

SCHWABE, J. **50 anos de jurisprudência do Tribunal Federal Constitucional Alemão**. Tradução: Beatriz Hennig et al. Montevidéu: Fundacion Konrad-Adenauer, 2005.

STANKEVECZ, R. V.; BARACAT, E. M. Responsabilidade civil e as novas tecnologias aplicadas à área médica. **Revista Percurso Unicuritiba**., v.2, n.50, p.37-57, abr./jun, 2025.

SZANIAWSKI, E. **Direitos de personalidade e sua tutela**. 2.ed. São Paulo: RT, 2005.

TEFFÉ, C. S.; MEDON, F. Responsabilidade civil e regulação de novas tecnologias: questões acerca de inteligência artificial na tomada de decisões empresariais. **REI - Revista Estudos Institucionais**., Rio de Janeiro, v. 6, n. 1, p. 301-333, abr, 2020.

TEFFÉ, C. S.; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**. Rio de Janeiro, v. 9, n. 1, 2020.

TEPEDINO, G.; TEFFÉ, C. S. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil – RBDCivil**. Belo Horizonte, v. 25, p. 83-116, jul./set., 2020.

UNITED NATIONS. **Declaração Universal dos Direitos Humanos**. Disponível em: https:// www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por. Acesso em: 20 de fev. 2025.

UNITED NATIONS. **International Covenant on Civil and Political Rights**. Disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civiland-political-rights. Acesso em: 20 de fev. 2025.

TEPEDINO, G, **Temas de direito civil**. 3.ed. Rio de Janeiro: Renovar, 2004.

ZANATTA, R. A. F. A proteção de dados entre leis, códigos e programação: os limites do Marco Civil da Internet. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito & Internet III:** Marco Civil da Internet. São Paulo: Quartier Latin, 2015.

ZUBOFF, S. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. London: Profile Books, 2019.

Sites:

www.uol.com.br. Disponível em: https://www.uol.com.br/. ROSSI, Amanda. **Vitamina usada para tentar engravidar pode direcionar até anúncio de carro**. São Paulo, SP, [2023]. Disponível em:https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2023/09/01/remedio-para-engravidar-pode-direcionar-ate-propaganda-de-carro.htm. Acesso em: 01 setembro 2023.

www.uol.com.br. Disponível em: https://www.uol.com.br/. ROSSI, Amanda. **Ministério da Justiça notifica RaiaDrogasil após reportagem do UOL**. São Paulo, SP, [2023]. Disponível em:

https://economia.uol.com.br/noticias/redacao/2023/10/23/ministerio-da-justica-notificaraiadrogasil-apos-reportagem-do-uol.htm. Acesso em: 23 outubro 2023.

www.uol.com.br. Disponível em: https://www.uol.com.br/. GOMES Helton Simões, CORTIZ Diogo, OLIVEIRA Ruam. **72 mi de dados coletados até os 13 anos:** como rede social espreme seu filho. São Paulo, SP, [2024]. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2024/09/03/72-mi-de-dados-coletados-ate-os-13-anos-como-rede-social-espreme-seu-filho.htm. Acessado em: 03 de setembro de 2024.

www.agenciamestre.com. SOUZA, Daniele. **Guerra dos Dados – Empresas Vendem Seus Dados que São Usados em Marketing Digital**. [02.2020]. Disponível em: https://www.agenciamestre.com/marketing-digital/guerra-dos-dados-empresas-vendem-seus-dados-que-sao-usados-em-marketing-digital/. Acesso em: 01 de fevereiro de 2025.

www.intercept.com.br. DIAS, Tatiana. **VIGIAR E LUCRAR Nós identificamos dois clientes dos dados de localização "anônimos" vendidos pela Vivo**. [04.2020]. Disponível em: https://www.intercept.com.br/2020/04/13/vivo-venda-localizacao-anonima/. Acesso em: 01 de fevereiro de 2025.

www.infomoney.com.br. Estadão Conteúdo. **Startup lança serviço que inaugura comércio de dados pessoais**. [2022]. Disponível em: https://www.infomoney.com.br/negocios/drumwave-lanca-servico-que-inaugura-comercio-de-dados-pessoais/. Acesso em: 01 de fevereiro de 2025.

www.cnnbrasil.com.br. MIIANEZI, Gabriela. **Empresa paga cerca de R$ 500 por escaneamento de íris; entenda como é feito**. São Paulo, SP, [2025]. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/sp/empresa-paga-cerca-de-r-500-por-escaneamento-de-iris-entenda-como-e-feito/. Acesso em: 01 de fevereiro de 2025.