UNIVERSIDADE DE BRASÍLIA
Faculdade de Direito
Programa de Pós-Graduação em Direito

Ana Luisa Tarter Nunes

REGIME DUAL DE RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Brasília
2023

Ana Luisa Tarter Nunes

REGIME DUAL DE RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Tese de doutorado apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de Brasília (UnB) para obtenção do título de Doutora no curso de Doutorado em Direito, sob orientação do Professor Fabiano Hartmann Peixoto.

Brasília
2023

NUNES, Ana Luisa Tarter.

Regime Dual de Responsabilidade civil dual na Lei Geral de Proteção de Dados / Ana Luisa Tarter Nunes; orientador: Fabiano Hartmann Peixoto. Brasília, 2023.

Tese (Doutorado – Doutorado em Direito) – Universidade de Brasília (UnB), 2023.

I. Correlações entre a inovação tecnológica e o desenvolvimento do direito à tutela de dados pessoais; II. Do regime dual de responsabilidade civil e proteção de dados pessoais; III. Responsabilidade civil na proteção de dados pessoais frente a novas tecnologias: integração normativa e Inteligência Artificial.

NUNES, Ana Luisa Tarter. *Regime dual de responsabilidade civil na LGPD*. 2023. 296 f. Tese (Doutorado em Direito) – Universidade de Brasília (Unb). 2023.

RESUMO

Objeto. O trabalho tem por objeto o exame da responsabilidade civil extracontratual disciplinada pela Lei Geral de Proteção de Dados. **Objetivo**. O objetivo é detalhar o regime de responsabilidade civil regulado pela normativa, qual é a extensão de sua tutela; de que forma a interpretação sistemática de fontes normativas diversas, como o Código de Defesa do Consumidor, complementam ou influenciam na análise de casos concretos e examinar a aplicabilidade desse quadro normativo frente a danos causados por tecnologias autônomas, como a Inteligência Artificial. **Metodologia**. Parte-se da identificação dos direitos tutelados e das distinções conceituais necessárias para o propósito de descrever o que qualifica um tratamento de dados pessoais como regular. O trabalho prossegue com a análise das consequências de um tratamento irregular de dados pessoais. Identifica-se o regime dual de responsabilidade civil extracontratual da LGPD. Por fim, analisa-se a correlação do emprego de dados pessoais com as características descritivas da Inteligência Artificial (IA) – tomada como elemento representativo das inovações tecnológicas disruptivas – com o propósito de demonstrar a adequação da tutela normativa de dados pessoais frente aos potenciais danos causados pelo emprego dessa tecnologia. **Resultado**. Propõe-se uma construção teórica do regime dual de responsabilidade civil na Lei Geral de Proteção de dados a partir da interpretação dos dispositivos da normativa. Fundamenta-se o caráter instrumental da Inteligência Artificial como elemento necessário para avaliar a responsabilidade civil por danos causados por essa tecnologia, em especial, quando da utilização de dados pessoais para o seu processamento. **Contribuição**. O trabalho contribui com a consolidação do regime de responsabilidade civil por danos ao direito fundamental de proteção de dados pessoais em coerência com as disposições normativas da LGPD e com outros diplomas normativos (como o Código de Defesa do Consumidor e o Marco Civil da Internet). Demonstra-se a adequação do atual quadro normativo de responsabilidade civil em face de danos causados mediante o emprego de tecnologias autônomas (IA) e a necessária consideração da natureza jurídica dessa tecnologia como instrumento a serviço de quem a emprega. **Utilidade**. O esclarecimento das regras, regimes e consequências, nos moldes apresentados, tem o potencial de garantir segurança jurídica ao titular e ao agente de tratamento, de modo a abrir a possibilidade para que a tutela aos dados pessoais seja compatível e harmônica com o incentivo ao desenvolvimento e progresso tecnológico.

PALAVRAS-CHAVE: Direito fundamental à tutela de dados pessoais. LGPD. Responsabilidade civil. Regime dual. Tecnologias autônomas. Inteligência Artificial.

ANA LUISA TARTER NUNES

REGIME DUAL DE RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Banca Examinadora da tese apresentada ao Programa de Pós-Graduação em Direito da Universidade de Brasília, para obtenção do Título de Doutora em Direito.

ORIENTADOR: _____.
Professor Dr. Fabiano Hartmann Peixoto – Faculdade de Direito [FD]
Universidade de Brasília.

1ª EXAMINADORA: _____.
Professora Dra. Fernanda de Carvalho Lage – Faculdade de Direito [FD]
Universidade de Brasília.

2ª EXAMINADORA: _____.
Professora Dra. Amanda Flávio de Oliveira – Faculdade de Direito [FD]
Universidade de Brasília (UnB).

3º EXAMINADOR: _____.
Professor Dr. Diógenes Faria de Carvalho – Faculdade de Direito [FD]
Universidade Federal de Goiás (UFG)

4º EXAMINADOR: _____.
Professor Dr. Leonardo Roscoe Bessa – Faculdade de Direito [FD]
Centro Universitário de Brasília (UniCEUB).

Para Milton, Rose, Pedro, Júlia e Elisa.

Per aspera ad astra.

Throught the thorns, to the stars.

Pelos ásperos caminhos, até os astros.

AGRADECIMENTOS

A citação de Aldous Leonard Huxley marcou meu percurso no desenvolvimento dessa tese. O filósofo inglês afirma que, depois de mais de quarenta e cinco anos de intensa pesquisa e estudo, o melhor conselho que pode dar às pessoas é ter um pouco de bondade umas com as outras. No literal, o autor afirma: "*it's a little embarrassing that after 45 years of research & study, the best advice I can give people is to be a little kinder to each other*."

Nos encontros e casualidades da vida, tive a sorte de encontrar essa experiência de Huxley na orientação de Fabiano Hartmann. Mais do que um professor e orientador, foi o responsável por reunir algumas das melhores pessoas que poderia conhecer. Amigos e amigas que acrescentam à lição do filósofo a necessidade de ter bondade com nosso próprio ser, diante das cobranças pessoais excessivas para atender às nossas expectativas.

Avançar por caminhos longos, como no desenvolvimento desse trabalho, implicou na passagem por muitas experiências paralelas, dificuldades e eventos supervenientes que, por vezes, tornaram o trabalho mais árduo do que eu imaginava poder enfrentar. Nesse ponto, tive a sorte de encontrar o carinho e paciência da família – sentimentos que se transformaram em incentivo e apoio para me encorajar a prosseguir em passo firme e sempre em frente.

A construção de uma tese é um trabalho individual, mas nem sempre solitário. Agradeço a todos que, das mais diversas formas, me ajudaram a desenvolver ideias, a prosseguir, a construir e a continuar. As palavras são insuficientes para descrever a importância e o carinho que desenvolvi por cada pessoa e por cada momento. A vocês, minha gratidão!

SUMÁRIO

ÍNDICE DE IMAGENS

ÍNDICE DE TABELAS

INTRODUÇÃO

A integração da Inteligência Artificial (IA) na vida cotidiana é acompanhada por intensos debates sobre suas potencialidades e seus possíveis impactos. Títulos de matérias e posts com *clickbaits* e chamadas sensacionalistas são atrativas para os leitores de notícias e usuários de aplicativos, mas acabam por gerar receios por vezes infundados sobre as capacidades e supostos perigos pelo emprego dessa tecnologia. Em meio a um cenário de descrições *hollywoodianas*, o caráter disruptivo e o funcionamento autônomo da IA suscitam conclusões (por vezes precipitadas) sobre a inadequação das atuais normativas do ordenamento jurídico para tratar de danos causados por sua utilização. Nesse ponto, exsurge a necessidade de buscar posicionamentos coerentes sobre o tratamento jurídico que deve ser dado à IA, em especial pelos danos causados pelo seu emprego. É importante diferenciar o que é dano de mero receio e que consequências devem ser toleradas como incidentes inerentes à vida cotidiana e quais são tuteladas pela norma jurídica.

Na disseminação do emprego da Inteligência Artificial, despontam preocupações com a privacidade das pessoas bem como sobre a sua relevância como instrumento para analisar o comportamento do consumidor com o propósito de atender às suas preferências mediante a oferta de produtos e serviços personalizados. Nessa perspectiva, das situações danosas que envolvem o emprego dessa tecnologia desdobram-se questionamentos sobre a aplicação da Lei Geral de Proteção Dados – Lei de nº 13.709/2018. A complexidade dessa análise envolve a incidência concomitante de normas especiais, como a aplicação do Código de Defesa do Consumidor.

Por essas considerações, ganha relevância a análise da incidência dos artigos 42 a 45, da LGPD, às situações danosas causadas pelo emprego da Inteligência Artificial. Cuidam-se dos dispositivos específicos que disciplinam a responsabilidade civil pelo tratamento irregular de dados pessoais. Nesse ponto, tem-se o questionamento central deste trabalho: como o regime de responsabilidade civil da LGPD incide sobre danos causados pelo tratamento irregular de dados pessoais que envolvam o emprego da Inteligência Artificial?

Na análise dos dispositivos elencados em capítulo específico na Lei Geral de Proteção de Dados – arts. 42 a 45 – vislumbra-se que a normativa realiza distinções sobre o tratamento irregular. O artigo 44 da LGPD é claro em indicar que o tratamento de dados será irregular tanto quando descumprir a legislação como quando não fornecer a segurança que o titular de dados dele pode esperar. Em consideração aos outros dispositivos da LGPD que tratam sobre o tema de responsabilidade civil e em conformidade com a interpretação sistematizada e integrada

(diálogo das fontes) dos demais diplomas que integram o quadro normativo brasileiro de tutela aos dados pessoais, o aprofundamento da análise do tema revelou uma necessidade de sistematização do regime de responsabilidade civil prevista na LGPD.

A par do tríplice regime de responsabilidade civil do Código de Defesa do Consumidor – composto por uma cláusula geral de responsabilidade civil (art. 6º, VI) e pela disciplina do fato e do vício do produto e do serviço – no percurso deste trabalho foi constatada a ausência de classificação, estruturação ou enumeração aprofundada dos tipos de tratamento irregular que o art. 44, da LGPD, enuncia. Com o propósito de suprir essa lacuna, este trabalho apresenta a construção teórica de um regime dual de responsabilidade civil pelo tratamento irregular de dados pessoais a partir da interpretação dos dispositivos da LGPD.

O regime dual de responsabilidade civil pela LGPD é pautado pela distinção entre duas hipóteses de tratamento irregular de dados pessoais: 1) o tratamento irregular por inobservância à legislação; e 2) o tratamento irregular por não fornecer a segurança que o titular dele possa esperar. O tema é aprofundado para apresentar a diferenciação entre tratamento ilícito de tratamento indevido, ambos fundamentados como modalidades do tratamento irregular por inobservância à legislação.

A proposta corrobora com a identificação de dois propósitos distintos para a disciplina da responsabilidade civil pela LGPD: um voltado a regular a atuação dos agentes de tratamento e o outro com o foco na proteção da pessoa natural. Esses propósitos são extraídos do regime dual de responsabilidade civil pelo tratamento irregular, respectivamente, por violação à legislação *stricto sensu* e pelo não atendimento à legítima expectativa de segurança do titular.

Diante da intensa correlação do tratamento de dados pessoais na execução e no desenvolvimento de tecnologias cada vez mais integradas às relações da sociedade contemporânea, a utilidade prática dessa classificação é colocada em prova para avaliar a adequação do atual o regime normativo de responsabilidade civil frente aos danos causados por tecnologias cada vez mais autônomas, como a Inteligência Artificial.

O detalhamento do atual quadro normativo e da extensão do regime de responsabilidade civil por danos ao direito fundamental de tutela aos dados pessoais tem por propósito contribuir com a segurança jurídica no balanceamento de interesses para, de um lado, garantir a efetivação dos direitos da personalidade do titular de dados e, de outro, compatibilizar tal proteção com o incentivo ao desenvolvimento e progresso tecnológico.

Para cumprir com esses objetivos, a presente análise é estruturada em três partes, enumeradas e ordenadas da seguinte forma:

Parte I:	Correlações entre a inovação tecnológica e o desenvolvimento do direito à tutela de dados pessoais.
Parte II:	Do regime dual de responsabilidade civil e proteção de dados pessoais.
Parte III:	Responsabilidade civil na proteção de dados frente a novas tecnologias: integração normativa e Inteligência Artificial.

Tabela 1 - Estrutura da tese em três partes.

A Parte I ocupa-se do detalhamento das correlações entre a inovação tecnológica e o desenvolvimento do direito à tutela de dados pessoais. Demonstra-se ser inerente à formação dos diversos marcos regulatórios de proteção de dados o reconhecimento de que a utilidade dos dados pessoais vinculada ao progresso tecnológico torna necessária a atualização de garantias fundamentais pelos Tribunais – especialmente diante das mudanças constantes de contextos tecnológicos. Decisão de 1983, pelo Tribunal Constitucional Alemão, é representativa nesse sentido, pois inovou ao reconhecer uma garantia constitucional específica relacionada à proteção de dados pessoais e a existência de um direito à autodeterminação informativa como resposta aos avanços tecnológicos – os quais tornaram possível o processamento de dados em proporção (até então) jamais imaginadas[1].

Demonstra-se que a centralidade dos dados para o funcionamento da sociedade da informação provoca o delineamento de novos contornos da tutela aos direitos da personalidade da pessoa humana. Para esse propósito, são abordados os seguintes questionamentos:

Parte I		
Correlações entre a inovação tecnológica e o desenvolvimento do direito à tutela de dados pessoais		**Capítulo.**
•	Por que os dados importam para o desenvolvimento tecnológico?	Capítulo 1.
•	Qual é o papel dos dados pessoais perante a sociedade da informação?	
•	Como a tecnologia influencia no desenvolvimento de direitos de tutela à pessoa humana?	Capítulo 2.
•	Qual é a correlação entre os dados pessoais e a privacidade?	

[1] Reclamação Constitucional contra ato normativo – Lei do Censo (*Volkszählungsgesetz*) de 1983. BVERFGE, 65, 1. SCHWABE, Jügen; MARTINS, Leonardo. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Konrad-Adenauer-Stiftung, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf p. 233 a 235.

•	Qual é o fundamento jurídico para a proteção dos dados pessoais?	Capítulo 3.
•	Qual é a diferença de sua conformação como direito fundamental e direito da personalidade?	
•	Qual é o atual quadro normativo que tutela os dados pessoais no ordenamento jurídico brasileiro com o potencial de influenciar a análise da responsabilidade civil prevista na LGPD?	Capítulo 4.
•	Quais os parâmetros utilizados para definir qual norma incidirá sobre um caso concreto?	

Tabela 2 - Aspectos abordados nos capítulos da Parte 1.

O Capítulo 1 aborda a relação do dado pessoal como insumo da sociedade da informação. Demonstra-se que o direito à proteção de dados pessoais não surge de um ambiente acadêmico estéril, mas dos papéis que o dado e a informação assumem nas relações sociais contemporâneas.

O Capítulo 2 acolhe os preceitos e posicionamentos expostos no capítulo antecedente para tratar do desenvolvimento do conceito jurídico de dados pessoais: sua gênese, transformações e convergência com a privacidade e direitos correlatos.

Evidencia-se que a busca de delimitação conceitual estanque dos direitos da personalidade não se sobrepõe à importância da identificação do que se pretende alcançar com a tutela desses direitos. Mais importante do que definir *o que* se protege é conhecer *o que se pretende* proteger com a tutela de um direito. Nessa linha de raciocínio, a maior contribuição do capítulo é definir o que se almeja alcançar com a tutela jurídica aos dados pessoais.

A par da delimitação dos objetivos pretendidos com a proteção desse direito, o Capítulo 3 aprofunda o enquadramento da tutela de dados pessoais como direito fundamental e da personalidade, bem como as implicações que decorrem do reconhecimento desse *status*. O Capítulo 4 apresenta o quadro normativo de tutela dos dados pessoais efetivado pelo ordenamento jurídico brasileiro considerando-se o ambiente em diálogo das fontes para a análise da responsabilidade civil extracontratual, regulada pela LGPD, perante os potenciais danos causados a esse direito.

Na Parte II desenvolve-se a contribuição mais representativa do trabalho: a construção dogmática e estruturada do regime de responsabilidade da LGPD, com a indicação de suas espécies e modalidades. Para a classificação defendida, "tratamento irregular" é gênero de duas espécies: por violação à legislação e pelo não atendimento à legítima expectativa de segurança do titular. Diferencia-se tratamento ilícito de tratamento indevido como modalidades do tratamento irregular que não atende à legislação *lato sensu*: o primeiro por violar a legislação *stricto sensu* e o segundo pela inobservância das medidas de segurança definidas pela ANPD.

A estruturação da classificação atende à seguinte representação visual sintetizada pela figura a seguir:

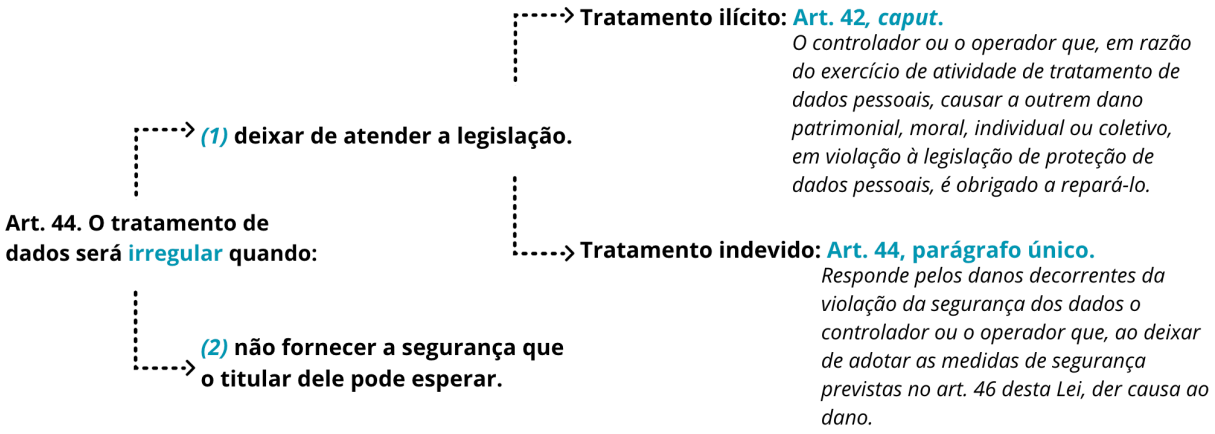

Figura 1 - Espécies de tratamento irregular e modalidades de tratamento irregular por violação à legislação. Distinção de tratamento irregular, ilícito e indevido. Figura elaborada pela autora.

Atualmente, a despeito de ser possível identificar na doutrina o reconhecimento de uma dupla opção normativa para a responsabilidade civil (MARQUES, MIRAGEM; 2023), não se verificou um detalhamento estruturado do que se considera um tratamento irregular e como os demais dispositivos da LGPD (em especial, os artigos 42, 43, 45 e 46) se relacionam de forma diferenciada a depender da espécie de tratamento irregular em evidência. Tampouco se verificou distinções a respeito da "adoção de medidas de segurança" (art. 44, parágrafo único c/c art. 46, §1º, da LGOD) e da "expectativa de segurança" (art. 44, *caput*, segunda parte) como as realizadas no presente trabalho.

Para cumprir com esses propósitos, na Parte II, são abordados os seguintes questionamentos:

Parte II		
Responsabilidade Civil e Proteção de Dados Pessoais		**Capítulo.**
•	Qual é a natureza jurídica da responsabilidade civil adotada pela LGPD?	Capítulo 6.
•	Quais são as espécies do gênero tratamento irregular de dados pessoais?	Capítulo 7.
•	Por que defender a existência de um regime dual de responsabilidade civil na LGPD?	
•	Qual é a primeira espécie de tratamento irregular de dados pessoais?	Capítulo 8.
•	O que significa "medidas de segurança" para fins de apuração de responsabilidade civil, pela LGPD?	

•	Por que defender a diferenciação de modalidades da 1ª espécie de tratamento irregular de dados pessoais?	
•	Qual é a diferença entre tratamento inadequado e ilícito?	
•	Qual é a segunda espécie de tratamento irregular de dados pessoais?	Capítulo 9.
•	Qual é o conteúdo do "dever de segurança" para fins de apuração de responsabilidade civil, pela LGPD?	
•	O que configura uma legítima expectativa de segurança do titular de dados?	
•	Quais situações exemplificativas seriam representativas da aplicação dessa espécie de responsabilidade civil?	

Tabela 3 - Aspectos abordados na Parte II

No desenvolvimento do trabalho, verificou-se a utilidade da distinção entre tratamento inadequado e ilícito (nomenclaturas utilizadas pela LGPD). Demonstra-se, ademais, que a adoção de "medidas de segurança" não se confunde com a "expectativa de segurança" do titular de dados. O primeiro se relaciona com o "tratamento indevido" (art. 44, parágrafo único e art. 46, §10, da LGPD) – cujo foco é a regulação da conduta do agente – e o segundo se refere à espécie de tratamento irregular caracterizada pelo não fornecimento da segurança que o titular dele pode esperar (art. 44, *caput*, segunda parte) – cujo foco é a tutela da pessoa natural, titular dos dados pessoais.

A importância dessa estrutura tem implicações práticas, como na análise dos elementos da responsabilidade civil, do ônus de prova e das excludentes de responsabilidade.

A convergência interpretativa a respeito dos critérios legais que determinam um tratamento regular (e por consequência, permitem a identificação de um tratamento irregular) é o ponto essencial para a efetivação da tutela normativa aos dados pessoais. O mercado exige segurança jurídica para compreender quais situações legitimam o tratamento de dados e a efetivação da tutela da pessoa natural exige clareza na identificação de pressupostos necessários para gerar o dever de indenizar. É em meio a esse cenário que se confere destaque e se demonstra a importância de aprofundar a análise do regime de responsabilidade civil da LGPD – objeto do presente trabalho.

A Parte III, por fim, aborda a integração normativa do quadro de responsabilidade civil na proteção de dados pessoais frente a tecnologias autônomas, com destaque para a Inteligência Artificial. Esclarecimentos necessários sobre a análise jurídica do tema ocupam boa parte do que se denomina o estudo estratégico do Direito e da IA. O foco dos capítulos desse tópico se voltam a esclarecer e fundamentar a natureza instrumental que a Inteligência Artificial assume na análise de responsabilidade civil decorrente de potenciais danos por quem as emprega.

Na Parte III, são abordados os seguintes questionamentos:

Parte III		
Responsabilidade Civil na Proteção de Dados Pessoais: Integração normativa e Inteligência Artificial.		**Capítulo.**
•	Como a Inteligência Artificial molda o mercado de consumo?	Capítulo 10.
•	Quais são as perspectivas que podem ser adotadas no debate da Inteligência Artificial e o Direito?	Capítulo 11.
•	O que é Inteligência artificial?	Capítulo 12.
•	Qual é a natureza jurídica da Inteligência Artificial?	Capítulo 13.
•	Por que defender o caráter instrumental do emprego da Inteligência Artificial?	
•	Como o caráter instrumental da IA influencia na análise da incidência do regime dual de responsabilidade civil prevista na LGPD?	
•	Em qual hipótese o emprego da IA não atrairia a incidência do regime de responsabilidade civil da LGPD?	Capítulo 14.
•	Quais regimes de responsabilidade recairiam sobre danos causados no exemplo de danos causados por carros autônomos comercializados e em fase de testes?	

Em síntese, a construção teórica do regime dual de responsabilidade civil extracontratual a partir da interpretação dos dispositivos da LGPD e a defesa da natureza instrumental da Inteligência Artificial para fins de apuração da responsabilidade civil por danos causados pelo seu emprego representam a inovação proposta por este trabalho.

A partir do detalhamento da construção teórica do regime de responsabilidade civil dual da LGPD, em interpretação sistemática (em diálogo das fontes) de diplomas normativos diversos, como o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei do Cadastro Positivo, demonstra-se a suficiência do atual quadro normativo frente a danos causados por tecnologias autônomas, como a Inteligência Artificial.

Todo o trabalho é pautado pela busca de fortalecimento da *segurança jurídica*. Ainda que a *justiça* seja o fundamento filosófico que compõe a base do Direito, considera-se que o conceito de *justo* é a base axiológica no *desenvolvimento* de normas de responsabilidade, ao passo que a *segurança jurídica* é a base valorativa da *aplicação* das normas de imputação da responsabilidade. A construção teórica do regime dual de responsabilidade civil extracontratual prevista na LGPD e a fundamentação da natureza instrumental da Inteligência Artificial representam a inovação proposta por este trabalho cujo objetivo é auxiliar na convergência de

posicionamentos a fim de garantir segurança jurídica para todas as partes que integram uma relação de tratamento de dados pessoais.

PARTE I – CORRELAÇÕES ENTRE A INOVAÇÃO TECNOLÓGICA E O DESENVOLVIMENTO DO DIREITO À TUTELA DE DADOS PESSOAIS

1. EFEITOS JURÍDICOS DA CENTRALIDADE DOS DADOS COMO INSUMO NA SOCIEDADE DA INFORMAÇÃO.

Na segunda metade do século XX, o crescimento econômico mundial fixou seus alicerces no desenvolvimento tecnológico e no alto fluxo de dados (ROZA, 2020). As transformações geraram (e ainda geram) impactos simultâneos sentidos nas esferas sociais, políticas, econômicas e culturais. Essas profundas transformações estruturais da sociedade marcam um novo paradigma técnico-econômico baseado em uma conformação organizacional dinâmica e dependente da infraestrutura disponível de informações (TAKAHASHI, 2000). Várias expressões são utilizadas para correlacionar a influência das inovações tecnológicas na organização social, dentre as quais ganha destaque a designação *sociedade da informação* (LASTRES, 1999).

Na dimensão econômica da sociedade da informação, os dados assumem centralidade na atividade financeira, na produção de riqueza e no desenvolvimento de novos negócios e empreendimentos. É o caso da ampliação do empregos de bancos de dados para avaliação de crédito dos consumidores – instrumento que surgiu a partir da necessidade de otimizar o mercado de crédito ao proporcionar um conhecimento rápido e detalhado do histórico de compras do consumidor que postula um financiamento.

Pela perspectiva social, a informação assume posição cada vez mais integrada ao cotidiano das pessoas. À medida que novas tecnologias se incorporam ao convívio social, mais dados são utilizados – e gerados – na prestação de serviços, em um processo de retroalimentação no qual as próprias pessoas espontaneamente disponibilizam suas informações tanto para fortalecer relações existentes como para formar novos laços. Não são coletados apenas dados estáticos – que descrevem uma pessoa ou um fato. Há uma nova dinâmica na formação de bancos de dados caracterizada não pelo mero acúmulo, mas pelo *fluxo*, *instantaneidade* e *variedade* de informações coletadas, processadas e distribuídas – ao que é referido como o fenômeno ou instrumentalização do *Big data*.

Dos efeitos sociais da sociedade da informação desdobram-se efeitos monetários da utilização de dados. É o caso de redes sociais, em que os dados de interação dos usuários com a plataforma são utilizados como remuneração indireta na prestação de serviços. A capitalização de empresas que prestam serviços de redes sociais – como a Meta (antigo Facebook) e o LinkedIn – é majoritariamente realizada pela comercialização de propagandas direcionadas aos usuários da plataforma. Em regra, o fornecimento dos serviços de conectividade é oferecido de forma gratuita aos usuários – o que corrobora para a incorporação das plataformas de redes sociais para intermediar o relacionamento social no cotidiano das pessoas.

Com a habilidade de atingir audiências específicas, a efetividade dos anúncios incentiva outras empresas a investir cada vez mais nesse formato de publicidade. Os algoritmos empregados são elaborados com a finalidade de maximizar o tempo do usuário nas plataformas justamente para maximizar os lucros dessas empresas. Por isso fala-se que tais companhias atuam em uma "economia de atenção", pois as plataformas competem pela captura e manutenção da atenção de seus usuários.

Além da publicidade direcionada, outra forma de capitalização das plataformas de redes sociais ocorre pela "*venda*" de dados pessoais. Não se trata propriamente da comercialização de informações sobre a identidade dos usuários (como e-mail, números de telefone ou endereços), mas da comercialização de dados agregados para empresas os utilizarem como subsídios para descrições analíticas de comportamento de mercado (com a intenção de formar um novo produto, por exemplo) ou para análises estatísticas (como para verificar qual é o melhor horário ou as melhores datas em que o consumidor se mostra mais suscetível às propagandas a ele direcionadas – a exemplo do dia das mães).

Tanto para a publicidade direcionada como para a venda de dados agregados, as informações dos usuários são a peça-chave da capitalização das empresas. Esse cenário justifica a referência aos dados pessoais como insumos da Sociedade da Informação.

Os efeitos jurídicos da monetização a partir de dados pessoais não são inéditos, pois há tempos já são reconhecidos. Como exemplo, o Superior Tribunal de Justiça reconheceu a formação da relação de consumo entre usuários e uma plataforma de redes sociais em 2012. Ainda que o art. 3º, §2º, do CDC[2], exija que a prestação de serviços ocorra mediante

[2] A relação de consumo exige o preenchimento de três elementos: o subjetivo (consumidor e fornecedor); o objetivo (produto ou serviço) e o finalístico (destinatário final). A maior questão pontuada sobre o reconhecimento da relação de consumo no caso refere-se à exigência do art. 3º, §2º pois exige-se que os serviços prestados sejam realizados mediante remuneração: "*serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das*

remuneração (elemento objetivo da relação de consumo), o Tribunal esclareceu que os usuários não precisam prestar uma compensação em dinheiro pelos serviços utilizados. A forma de capitalização dessas empresas representa uma remuneração indireta do fornecedor, apta a permitir a formação de uma relação de consumo, conforme se verifica na ementa do julgado:

> CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. DESNECESSIDADE. RESTRIÇÃO DOS RESULTADOS. NÃO-CABIMENTO. CONTEÚDO PÚBLICO. DIREITO À INFORMAÇÃO.
> 1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90.
> 2. **O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo**, pois o termo "mediante remuneração", contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o **ganho indireto do fornecedor**´ (…)
> (STJ – REsp: 1316921 RJ 2011/0307909-6, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 26/06/2012, T3 – TERCEIRA TURMA, Data de Publicação: DJe 29/06/2012) – grifos da autora.

A utilização de dados pessoais pelas plataformas de redes sociais não esgotam as mais diversas formas pelas quais tais informações são processadas. Os diferentes cenários jurídicos nos quais os dados são utilizados (em especial os pessoais) atraem a aplicação de diplomas normativos diversificados a depender da situação fática enfrentada.

O Código de Defesa do Consumidor, por exemplo, disciplina outra forma de emprego de dados pessoais. Trata-se da regulação da atividade de bancos de dados e cadastros do consumidor para a avaliação de concessões de crédito (arts. 43 e 44). A Lei do Cadastro Positivo amplia a gama de dados que podem ser utilizados para o que se denominou como a formação do *score* de crédito do consumidor. O Marco Civil da Internet, por sua vez, regula a forma, prazos e meios de transferência de dados mantidos por provedores. Há, também, o *habeas data* (art. 5º, LXII, da CF/1988) que se apresenta como uma garantia individual para assegurar o direito ao conhecimento e retificação de dados de seu titular.

No cenário de tutela setorizada de dados pessoais, a Lei Geral de Proteção de Dados surge como norma de alcance nacional que centraliza disposições sobre o tratamento de dados pessoais – ou seja, qualquer operação realizada com informações que identifiquem ou tornem identificável uma pessoa, tais como as que se referem a "*coleta, produção, recepção,*

---

relações de caráter trabalhista." Em tese, se o serviço é gratuito, não há preenchimento do elemento objetivo e, portanto, não há a figura de fornecedor. A solução encontrada pelo STJ foi o reconhecimento da remuneração indireta dos serviços prestados. (STJ – REsp: 1316921, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 26/06/2012, T3 – Terceira Turma, Data de Publicação: DJe 29/06/2012)

classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X, da LGPD). Os exemplos enunciados pela norma demonstram que sua aplicação é ampla: alcança a tutela de dados pessoais de todas as pessoas naturais, seja o tratamento realizado por pessoa física ou jurídica, de direito público ou direito privado (art. 1º, da LGPD), seja em meio físico ou digital.

A LGPD não entra em conflito com as normas que também tutelam dados pessoais. Pelas soluções tradicionais de confronto de normas, aplica-se a lei superior em detrimento da inferior (*lex superior derogat lex inferior*), a lei especial em detrimento da geral (*lex specialis derogat lex generali*) e a lei posterior em lugar da anterior (*ex posterior derogat lex priori*). Não foi essa a solução que o legislador adotou. Pelos arts. 45 e 64, da LGPD[3], as normas de tutela à pessoa são aplicadas de forma concomitante e integrada, ou seja, em *diálogo das fontes* (MARQUES, 2020).

Na miríade de relações formadas na Sociedade da Informação, é frequente uma atividade de tratamento de dados pessoais ocorrer em (ou formar) uma relação de consumo. Nesses casos, há a incidência tanto das disposições da LGPD quanto as da legislação de consumo. A aplicação em diálogo das fontes beneficia a tutela da pessoa humana, pois amplia a cartela de direitos do titular de dados/consumidor. Ocorre que esse cenário torna ainda mais complexo o quadro normativo que deve ser interpretado pelo aplicador do direito.

Os desafios jurídicos sobre a identificação do objeto de tutela nas relações formadas na sociedade da informação são variáveis. Discussões sobre a tutela à intimidade, privacidade, honra, direito de imagem e direito à informação permeiam o debate sobre o que se entende por proteção de dados pessoais. O conceito de privacidade, por exemplo, é debatido há mais de cem anos e não há uma perspectiva de uma delimitação precisa de sua abrangência (WARREN; BRANDEIS, 1890). Conceituar dado ou informação também é objeto de debate para aferir a incidência de normativas específicas.

Quanto aos limites de tutela da LGPD e da legislação de consumo, exsurge a possibilidade de aplicação do Código Civil para amparar danos causados pelo surgimento de novos tipos relações. O desenvolvimento tecnológico expande os horizontes sobre a questão da responsabilização por danos decorrentes de máquinas cada vez mais autônomas. O

[3] LGPD. Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.
LGPD. Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

processamento de dados com intervenção mínima ou sem intervenção humana já é realidade para aplicações práticas da Inteligência Artificial (IA). É o caso, por exemplo, de avaliações de crédito realizadas de forma automática pelo processamento de algoritmos aplicados a uma grande base de dados para pormenorizar o comportamento de um consumidor. Nesse campo, o desafio inicial do intérprete também recai sobre os conceitos a serem utilizados para descrever essa aplicação tecnológica. É determinante identificar ou compreender a forma como a tecnologia funciona e influencia a análise jurídica. É criticável compreender que cada inovação tecnológica deve vir acompanhada de uma correspondente tutela normativa específica. Há tempos se abandou a pretensão de que o legislador deve regular ou rotular todos os aspectos do convívio social.

Diante de danos decorrentes da utilização de tecnologias, cabe ao intérprete verificar se há o tratamento de dados pessoais aptos a atrair a incidência da LGPD; a formação de uma relação de consumo que induza a aplicação da legislação de consumo; ou a possibilidade de conformação da situação fática a alguma das cláusulas de responsabilidade previstas no Código Civil.

A questão não é constatar a ausência de uma lei específica, mas conformar a aplicação do regime de responsabilidade ao que se objetiva alcançar com a tutela a um direito de dados pessoais, devendo-se, ainda, considerar um cenário de relações complexas disciplinados por legislações diversas e aplicadas de forma concomitante.

Para a aplicação da LGPD, exige-se a compreensão do que se entende por *dado*; o objeto de tutela da normativa (os dados pessoais) e sua correspondente conexão com conceitos análogos (como privacidade); o âmbito de incidência da norma e os deveres exigidos para configurar um tratamento de dados como regular – afinal, o regime de responsabilidade civil da LGPD pressupõe um tratamento irregular de dados pessoais (art. 44, *caput*, LGPD).

Compreendidas essas questões, é possível ao intérprete verificar as correlações de regimes de responsabilidade disciplinados por legislações diversas para uma necessária convergência de suas disposições.

Passa-se à análise dos desafios propostos, como a conceituação de dados; a caracterização de dados pessoais; a correspondência destes com conceitos conexos (como a privacidade e intimidade) e à identificação de qual é o objetivo normativo de alçar a proteção de dados pessoais como direito fundamental e direito da personalidade.

1.1 Dado e informação

Dado e informação são conceitos rotineiramente utilizados de forma intercambiável. Por outro lado, há setores que defendem que cada termo possui peculiaridades próprias.

O fundamento para a diferenciação dos termos visa, em geral, qualificar os processos de conhecimento humano ou representar o aumento de valor agregado de categorias diversas. *Dado*, por essa perspectiva, é a representação de um fato ou de determinado aspecto da realidade em estado anterior à *informação*. Trata-se de uma informação em estado potencial, uma pré-informação, uma representação do aspecto de um fato antes de uma interpretação ou de um processo de associação. A *informação*, por sua vez, representa a depuração do conteúdo de um dado, o resultado de sua interpretação, a redução de um estado de incerteza que chega ao limiar da *cognição* (DONEDA, 2021).

A tentativa de hierarquizar as percepções humanas no processo de transformação dos dados para gerar conhecimento ou desenvolver a sabedoria remontam ao final dos anos 1980, como nos trabalhos de Ackoff (1989). Cabe ressaltar que nenhum dos trabalhos representativos dos processos cognitivos da mente humana dessa época fizeram referência a uma representação gráfica para ilustrar a hierarquia da percepção humana no processo de aumento de valor agregado na transformação de dados (MENDONÇA, DENNER, 2020). Ainda assim, tais trabalhos serviram de base para descrever a aquisição de conhecimento por diagramas, como o conhecido modelo DIKW (*data, informations, knowledge, wisdom*), representado pela pirâmide do conhecimento:

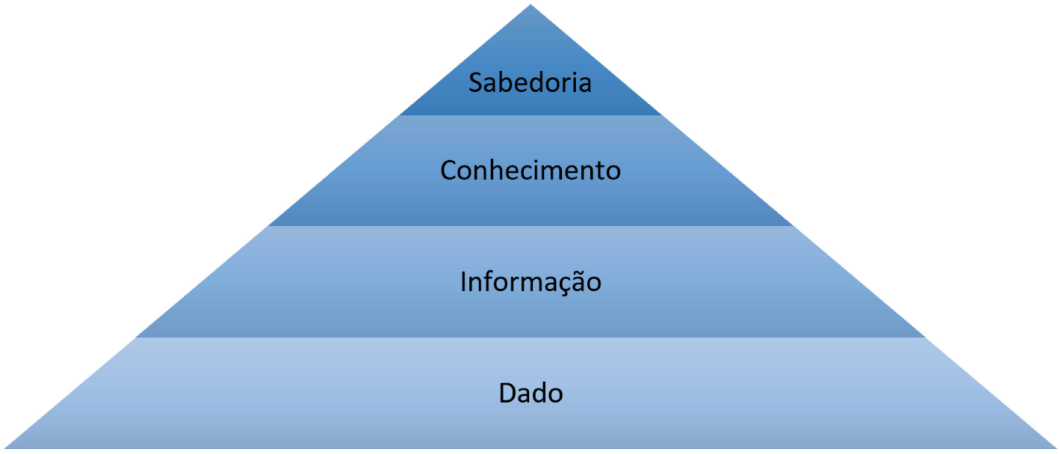

Figura 2- Pirâmide DIKW. Fonte: (RIBEIRO; SANTOS, 2020)

Por essa classificação, cada camada representa um *refinamento* da anterior. Para Ackoff (1989) a categoria *dados* descreve símbolos que representam propriedades de objetos ou eventos. *Informação*, por sua vez, consiste no incremento de utilidade aos dados a partir de seu processamento ou interpretação. Para o autor, a diferença ente dados e informação é eminentemente funcional e não propriamente estrutural (ou seja, uma mudança a partir de uma interpretação que agrega valor ao dado sem que ocorra uma modificação na sua representação ou estrutura). A camada compreensão ou conhecimento (*knowledge*) representa a extração de *explicações* para o que foi descrito pela informação (como respostas às perguntas: quem, quando, porque, onde e quanto). Sabedoria (*wisdom*), por fim[4], é a habilidade de, a partir do conhecimento, incrementar a *funcionalidade* ou *efetividade* do objeto ou evento representado pelo dados.

O modelo piramidal chegou a ser aprimorado para uma representação em cadeia para reforçar o relacionamento sinérgico dos elementos do processo cognitivo humano:

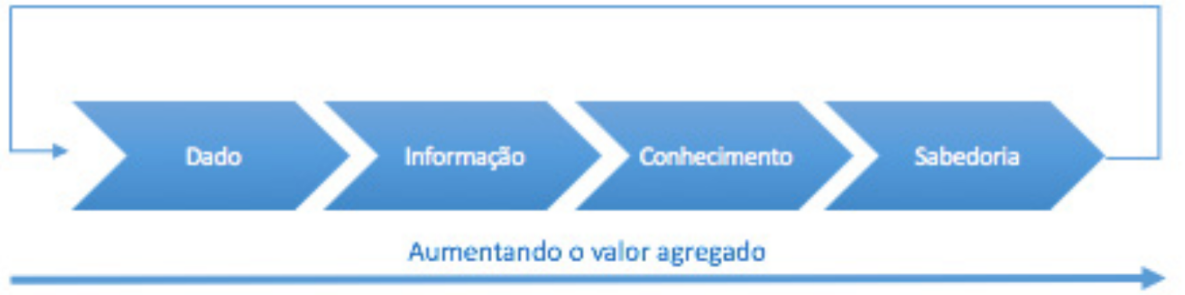

Figura 3 - Cadeia de Valor agregado DIKW. Fonte: (RIBEIRO; SANTOS, 2020)

A despeito de seu caráter didático, a adoção de modelos criados para ilustrar o processo cognitivo humano é alvo de críticas ante a ausência de verificações empíricas para sua validação como modelos teóricos (RIBEIRO; SANTOS, 2020). De fato, não há um índice para a quantificação do valor agregado necessário para passar de uma categoria à outra, tampouco um acordo sobre a parametrização de níveis ou sobre a organização hierárquica para diferenciar as classes de conhecimento.

[4] A disseminação do modelo piramidal em quatro classificações é umas representações mais tradicionais. No entanto, outros autores acrescentam outras categorias ou descrições distintas. O próprio Ackoff (1989), por exemplo, acrescenta outras etapas, como compreensão (como elemento distinto de conhecimento) e inteligência (como última categoria).

Em uma perspectiva jurídica (DONEDA, 2021), o termo *informação* é associado a uma ordem de valor, como a liberdade de informação (liberdade de imprensa) e o direito à informação (art. 5º, XIV e XXXIII, CF/88)[5]. Danilo Doneda (2021) destaca que o termo também possui um significado histórico para representar a maior capacidade de desenvoltura qualitativa e quantitativa na sua manipulação, especialmente em decorrência da inovação tecnológica. A tecnologia, nesse sentido, é tomada como vetor determinante para o incremento do número de formas pelas quais as informações podem ser apropriadas ou utilizadas, justamente por ser o elemento que proporciona o aumento da capacidade de armazenamento e de comunicação de dados.

A diferenciação de dado e informação, por essa perspectiva, seria a evidência de uma cisão de momentos históricos proporcionada pela tecnologia. O aspecto diferencial promovido pela tecnologia, nesse cenário, se refere a sua capacidade de transformar dados desorganizados em informações organizadas ou estruturadas.[6]

Danilo Doneda (2021) sustenta que a diferenciação de termos também tem utilidade para valorizar a *informação* como fenômeno jurídico em si. O autor leva em consideração o fato de que boa parcela das liberdades individuais são concretamente exercidas em plataformas nas quais a circulação de informações assume papel relevante.

Por uma abordagem tradicional, a tutela jurídica trata a *informação* a partir de manifestações específicas, como no exercício da liberdade de expressão, do direito de requisição de informações, da propriedade intelectual e da livre circulação de dados. Para o autor (DONEDA, 2021), essa perspectiva de análise setorizada desconsidera focos de tensão sobre interesses conflitantes e constitucionalmente legitimados. Reconhecer a *informação* como fenômeno jurídico em si, por outro lado, proporciona uma abordagem mais funcional dos diversos direitos a ela relacionados

A despeito das diferenciações apresentadas, cabe apontar que as normas jurídicas brasileiras utilizam os termos dado e informação de modo intercambiável. A título de exemplo, a LGPD conceitua *dado* pessoal como uma *informação* relacionada à pessoa natural identificada ou identificável (art. 5º, X). O Código de Defesa do Consumidor refere-se a *dados*

[5] Art. 5º. XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

[6] Inclusive, cabe mencionar que, no âmbito do Sistema Brasileiro de Inteligência, inteligência é conceituada como a atividade que tem por objetivo a obtenção e análise de dados para a produção de conhecimentos (Lei nº 9.883/1999, art. 1º, §2º).

pessoais como uma das *informações* que devem ser disponibilizadas em formatos acessíveis aos consumidores (art. 43, *caput* e §6º) [7]. O Marco Civil da Internet associa *dados* pessoais como uma das *informações* que possam contribuir para a identificação do usuário ou mesmo de um terminal (art. 10, §1º)[8].

Em termos práticos, constata-se que a utilização intercambiável dos termos *dado* ou *informação* não diminui a tutela necessária aos direitos a eles correlacionados. Isso porque o impacto tecnológico é sentido no âmbito jurídico há tempos que remontam ao emprego da máquina fotográfica (WARREN; BRANDEIS, 1890). O aumento do fluxo de dados em meios de comunicação e no desenvolvimento tecnológico reforçam, mas não inauguram preocupações com as potenciais consequências danosas do emprego de novas tecnologias.

Não se olvida da importância da conceituação de institutos jurídicos para a aplicação e a efetivação de direitos. No entanto, a par do percurso histórico da privacidade e dos conceitos a ela atrelados, sua tutela sofreu modificações de acepções que não necessariamente indicam uma instabilidade, mas sim uma característica de adaptação circunstancial que fortalece a conclusão de que a importância do instituto não é propriamente a sua conceituação, mas a centralidade da proteção do indivíduo – o que aproxima o instituto à acepção de um direito existencial (TEPEDINO, 1999), conforme tutelado pelo art. 1º, III, da CF/1988.

Esse argumento não dispensa a importância de uma Lei de Proteção de Dados Pessoais de âmbito nacional. O diploma normativo consagra o reconhecimento da essencialidade da tutela de dados pessoais para a proteção da personalidade das pessoas. Ademais, centraliza a disposição de regras de forma a abranger o tratamento de dados tanto no âmbito físico como no digital, o que soluciona problemas relacionados à disciplina setorizada do tema, como nas relações de consumo ou pelos serviços prestados por provedores de internet – respectivamente tutelados, em especial, pelo Código de Defesa do Consumidor e pelo Marco Civil da Internet.

---

[7] Lei 8.078/1990. Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

[8] Lei 12.965/2014. Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .

De fato, a LGPD não tem o escopo de regular as informações como fenômeno jurídico – ao menos não na forma proposta por Danilo Doneda[9]. Sem dúvida, não é possível regular todas as acepções e situações sociais que tem como ponto central a tutela à informação. O reconhecimento de diferentes diplomas normativos de acordo com casos concretos ainda é uma necessidade – mas não necessariamente representa um ponto prejudicial à tutela da pessoa humana frente a danos relacionados ao uso de seus dados ou informações.

Outro argumento que afasta (ou ao menos dirime) os prejuízos pela utilização indistinta dos termos "dados" e "informação" se refere ao fato de que o esforço hermenêutico do intérprete não pode ser avaliado fora de seu tempo, o que abre a possibilidade para adequações de acordo com as circunstâncias avaliadas (TEPEDINO, 1999). Esse ponto assume especial relevância na análise dos impactos jurídicos da evolução tecnológica – marcadamente disruptiva e dinâmica.

A diferenciação dos conceitos de *dados* e *informação* deve ser avaliada a partir de sua utilidade. Em uma perspectiva didática, é relevante para diferenciar momentos históricos marcados pelos efeitos disruptivos da tecnologia – compreendida como instrumento adequado para transformar dados desorganizados em informações ordenadas. No entanto, os efeitos disruptivos da tecnologia ainda são sentidos, ou seja, a mudança se tornou traço perene da sociedade da informação. O esforço hermenêutico do intérprete não cessaria ainda que contasse com um acordo terminológico momentâneo sobre dado e informação.

Para a tutela da pessoa humana frente a novas tecnologias, a diferenciação entre dados e informação não foi adotada pela lei brasileira. Por essa perspectiva, o foco é a efetivação de direitos e a prevenção de danos, de modo que o esforço hermenêutico do intérprete se volta *ao que* se pretende efetivar ou proteger – e não, propriamente, à busca de um consenso estanque sobre a diferenciação entre os conceitos de dados e informação.

1.2 Dos dados pessoais segundo a LGPD.

A LGPD optou por tutelar os direitos da pessoa humana (pessoa física). Não haveria óbice – do ponto de vista legal, jurisprudencial ou doutrinário – para que a disciplina da LGPD também alcançasse a tutela de dados da pessoa jurídica. À pessoa jurídica são atribuídos direitos da personalidade (art. 52, do Código Civil) e esta pode, inclusive, ser ressarcida a título de dano

[9] A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) surge como diploma que centraliza as regras para o tratamento de dados pessoais, por pessoa física ou jurídica, em meio analógico ou digital, com o objeto de tutelar a liberdade, privacidade e o desenvolvimento da personalidade da pessoa natural (art. 1º, da LGPD). Nota-se que a LGPD tutela apenas os direitos da pessoa natural. A atividade por ela regulada, por outro lado, alcança qualquer pessoa – física ou jurídica – que a realize.

moral (Súmula-STJ 227)[10]. No entanto, a normativa é clara ao limitar sua aplicação à tutela de pessoas naturais.

Para a LGPD, dado pessoal é aquele que identifica ou torna identificável uma pessoa (necessariamente) natural (art. 5º, I, da LGPD). A proteção de dados da pessoa jurídica deve seguir outros meios de tutela – tais como a ofertada pela Lei de Proteção à Propriedade Intelectual (Lei nº 9.279/1996).

O artigo 1º, da LGPD, revela o titular dos direitos por ela tutelados (pessoa natural); o seu propósito (regular a atividade de tratamento de dados pessoais); o seu objeto de tutela (tratamento de dados pessoais) e aqueles que estão sujeitos à sua regulação (pessoa física ou jurídica).

Lei Geral de Proteção de Dados	
Titular de direitos:	Pessoa (*necessariamente*) natural.
Propósito:	Regulação da atividade de tratamento de dados pessoais
Objetivo:	Proteger direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Objeto de tutela:	Atividade de tratamento de dados pessoais.
Sujeitos à regulação:	Pessoa física ou jurídica.

Tabela 4 - Objeto, objetivo e propósitos da LGPD.

Aduz o art. 5º, I, da LGPD que dado pessoal é qualquer "*informação relacionada a pessoa natural identificada ou identificável*". No entanto, a mera referência a uma pessoa não qualifica essa informação como pessoal. Opiniões alheias ou produções pessoais (como de obras ou escritas intelectuais) não constituem dados pessoais – ao menos não como ponto de tutela da LGPD (DONEDA, 2021).

A LGPD reforça a exigência de que é preciso constatar um vínculo da dado à identificação de uma pessoa para que o dado possa ser considerado pessoal. Se um titular de um dado não puder ser identificado, o dado será anônimo (art. 5º, III) e, como tal, não será considerado pessoal para os fins disciplinados pela Lei de Proteção de Dados (art. 12, *caput*).

O dado será pessoal quando seu objeto for um sujeito de direito. Tratando-se de um sujeito de direito, o dado pessoal assumirá a relevância como um atributo de sua personalidade.

[10] STJ, Súmula n. 227:"A pessoa jurídica pode sofrer dano moral"

Dado pessoal é, portanto, aquele que revela ou possa revelar algum aspecto da personalidade de uma pessoa.

1.2.1 Dados Anônimos, dados insignificantes e os riscos da perfilização: casos práticos.

Dado anônimo é aquele que se refere a uma pessoa indeterminada (DONEDA, 2021). Trata-se de instrumento útil para os casos em que a relevância de uma informação se refere a uma coletividade, a exemplo da produção de estatísticas para o desenho de políticas públicas. A utilização de grandes quantidades de dados por Governos não é inédita. Dentre as experiências anteriores, há a Lei do Censo (Volkszählungsgesetz), de 1983, a qual foi declarada inconstitucional pelo Tribunal Constitucional Alemão, em reconhecimento à autodeterminação informativa dos indivíduos bem como diante dos riscos que o processamento autônomo de informações poderia gerar aos titulares (mediante a criação de perfis detalhados da personalidade do indivíduo).

No plano internacional, antes mesmo desse julgamento paradigmático, o Conselho Europeu para a Proteção de Dados, em 1981, editou a **Convenção 108, de Strasbourg**, o qual trouxe, em seu art. 2º, a relevância do controle ao tratamento automatizado de dados, estipulando que a informação pessoal é considerada como "*qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação*" e, ao mesmo tempo, consagrou a imprescindibilidade de sua proteção.

Medidas preventivas adotadas para enfrentamento da pandemia do COVID-19 são representativas da utilidade dos dados anônimos. Para produção de estatísticas, algumas ações de iniciativa do Poder Executivo utilizaram dados dos sistemas de localização de celulares para coordenar ações de incentivo ao isolamento social.

No estado de São Paulo, por exemplo, foi implementado o Sistema de Monitoramento Inteligente (SIMI-SP) pelo qual operadoras de telefonia (VIVO, TIM, CLARO e OI) possibilitaram a consulta pública de dados georreferenciados agregados[11] para a elaboração de políticas públicas. O tratamento desses dados permitiu a elaboração de conteúdos visuais, como

[11] O próprio informativo do programa indica que, em respeito à proteção de dados, as informações sobre deslocamentos das pessoas são aglutinadas e anonimizadas. Disponível em: https://www.saopaulo.sp.gov.br/coronavirus/isolamento/ Acesso em 31/03/2023.

a indicação de índices de adesão ao isolamento social de acordo com cada município, sem que houvesse a identificação de seus titulares, como demonstrado abaixo:

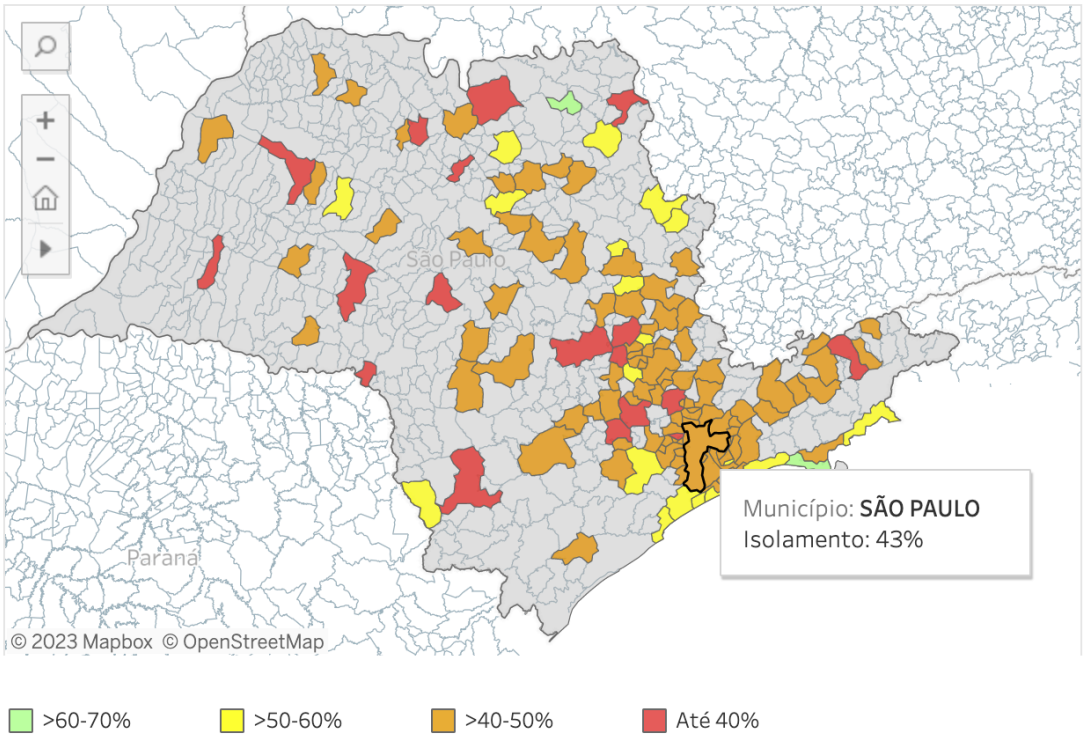

Figura 4. Mapa do Estado de São Paulo. Indicação da adesão ao isolamento social do Município de SP em 31/03/2023: 43%.

No contexto do tipo de tratamento de dados pessoais para essa finalidade, foram empregados meios para que não fosse possível a associação da informação à identificação de um indivíduo. Os dados de localização são agregados, ou seja, passam por um processo analítico de tratamento estatístico. No acordo firmado, os números telefônicos, nomes e números de IP dos aparelhos móveis não são compartilhados. Ademais, os dados de geolocalização não são disponibilizados de forma individualizada, mas transmitidos em bloco e em tempo real.

A constitucionalidade e a legalidade do programa SIMI-SP foram reconhecidas pelo Tribunal de Justiça do Estado de São Paulo. Destacam-se trechos do teor do acórdão que elencam os argumentos e posicionamentos adotados pelo tribunal:

> [...] não se verifica na impetração *qualquer elemento que induza à clara identificação do usuário* pelo sistema SIMI, que não seja a aplicação quantitativa referente à circulação das pessoas, para fins de constatação do cumprimento, pela população, do distanciamento social anteriormente determinado.
> [...]

> Ademais, é fato notório que a central de inteligência apenas analisa os dados de telefonia móvel para indicar tendências de deslocamento e apontar a eficácia das medidas de isolamento social. Com isso, é possível apontar em quais regiões a adesão à quarentena é maior e em quais as campanhas de conscientização precisam ser intensificadas, inclusive com apoio das prefeituras. *Os dados de georreferenciamento servem para aprimorar as medidas de isolamento social para enfrentamento da grave pandemia*.
> (TJ-SP - Mandado de Segurança Coletivo (MSC) n.º 2073871-34.2020.8.26.0000. Relator: Moreira Viegas, Data de Julgamento: 01/07/2020, Órgão Especial, Data de Publicação: 02/07/2020). – *grifos da autora.*

Um dos propósitos da anonimização é evitar a criação de perfis dos titulares. Nesse ponto, as práticas empregadas no programa SIMI-SP também amparam o princípio da não discriminação, pelo qual se proíbe o tratamento de dados para fins discriminatórios ilícitos ou abusivos (art. 6º, IX, LGPD). Este dispositivo é determinante para amparar preocupações de que o compartilhamento de dados não seja utilizado para a prática de *profiling* – também conhecida como perfilização: prática que traduz a ideia de criação de perfis, para esboçar, descrever ou antecipar traços e propensões das pessoas (SARTOR, 2020).

Note-se que a perfilização (*profiling*) não é um método, em si, proibido. No entanto, o compartilhamento de grandes volumes de dados gera receios e é visto com cautela. Especial atenção vem sendo dada ao tema desde a revelação de que informações de viés psicológico de mais de 50 milhões de usuários do Facebook foram utilizados pela empresa *Cambrigde Analytica* para a realização de propaganda política nas eleições dos Estados Unidos em 2016 – e, possivelmente, também para induzir posicionamento de cidadãos quanto ao referendo do Brexit, no mesmo ano.

Para melhor compreensão sobre como foram elaborados milhões de perfis com os traços psicológicos e comportamentais das pessoas, o tratamento de dados pessoais para a construção de perfis pela *Cambrigde Analytica* pode ser visualizada segundo o seguinte esquema:

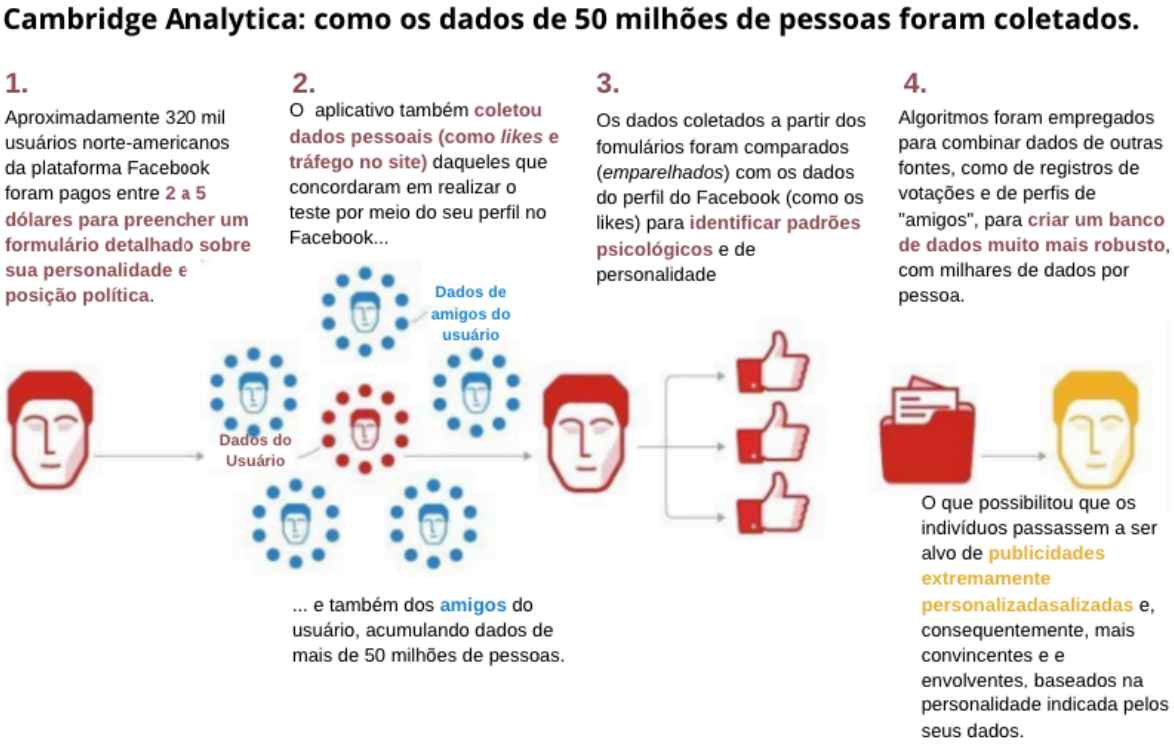

Figura 5. Simplificação do processo de construção de personalidades a partir de perfis de plataforma social.[12]

Ainda sobre a preocupação com a utilização de dados para a prática de *profiling*, cabe citar a decisão tomada pelo Supremo Tribunal Federal, na ADI nº 6387 que teve como objeto a análise da constitucionalidade da Medida Provisória nº 954/2020. Essa normativa determinou que operadoras de telefonia móvel fixa compartilhassem, com o IBGE, as listas de nomes, telefones e endereços tanto de consumidores como de pessoas jurídicas para fins de produção estatística oficial durante a situação de emergência de saúde pública internacional decorrente do coronavírus.

Note-se que tanto o SIMI-SP quanto a MP nº 954/2020 têm o propósito comum de possibilitar a produção de estatísticas para fins de enfrentamento da pandemia. Ocorre que a conclusão do STF foi pela inconstitucionalidade da medida provisória. Pode-se adiantar que as diferenças de desfechos na análise constitucional e legal entre os dois exemplos reforçam que o *contexto* no qual os dados anônimos são compartilhados é relevante para aferir a legitimidade de seu processamento.

[12] Trata-se de esquema traduzido e adaptado a partir do apresentado por Giovanni Sartor, em 2020, a respeito dos impactos da GDPR na Inteligência Artificial – página 24. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf Acesso em 31/03/2023.

O objeto da análise da constitucionalidade da medida provisória referiu-se à transferência de dados pessoais de consumidores de telefonias ao IBGE com o propósito de realizar o PNAD (Pesquisa Nacional por Amostra de Domicílios). A questão jurídico-constitucional envolveu o cotejo entre dois aspectos: (i) a importância da produção estatística para o desenho de políticas públicas no combate ao coronavírus e (ii) os direitos fundamentais à proteção de dados, à autodeterminação informativa e à privacidade.

Em outras palavras, a questão jurídica enfrentada colocou em jogo a ponderação de dois valores. De um lado, a estatística, que não se trata de um valor em si, mas de um instrumento indispensável para o desenvolvimento de soluções e políticas públicas adequadas às necessidades da população. De outro, figuram os direitos fundamentais elencados nos incisos X e XII, do art. 5º, da Constituição Federal, notadamente o direito à intimidade e à vida privada, bem como o direito de privacidade – à época, o direito à proteção dos dados pessoais não constava expressamente na Constituição Federal e a Lei Geral de Proteção de Dados encontrava-se em *vacatio legis*.

A decisão tomada na ADI 6387 é paradigmática para a proteção de dados no Brasil, pois suscitou a oportunidade de o Supremo Tribunal Federal reconhecer a privacidade, a proteção de dados e a autodeterminação informativa como direitos fundamentais autônomos. O resultado do julgamento da referida ação constitucional foi além de reconhecer a legalidade desses direitos, pois os alçou à categoria de direitos fundamentais ainda que não expressos no texto constitucional. A Corte Suprema compreendeu que estão albergados, de forma implícita, pela leitura conjunta dos incisos X e XII do art. 5º da Constituição Federal.

O STF não se limitou a reconhecer a autonomia de direitos não expressos na Constituição Federal, como também definiu parâmetros para a sua relativização. Afinal, direitos fundamentais são absolutos quanto à extensão de seus efeitos (ou seja, são de observância obrigatória por toda a coletividade), mas não são absolutos quanto à sua aplicação em casos concretos. Admitem, em outras palavras, a relativização de seus preceitos quando em confronto com outros direitos fundamentais – tais como o direito à informação e à liberdade de imprensa.

A Corte Suprema admitiu a importância da realização de retratos estatísticos pelo IBGE na condução de quaisquer políticas públicas. No entanto, declarou como excessiva a exigência de compartilhamento de dados pessoais nos moldes previstos na MP 954/2020. Em seu posicionamento, defendeu que a prevenção de riscos aos direitos fundamentais não permitiria a mitigação da proteção de dados pessoais no caso analisado.

Note-se que a ADI 6387 retratou uma preocupação que antecedeu danos efetivos – o que reforça a função de prevenção de uma eventual imputação de responsabilidade cível – e, de forma expressa, estabeleceu que o tratamento dos dados em si não era proibido. Inclusive, nas razões de voto, o Ministro Edson Fachin se posicionou acerca da importância das informações formuladas pelo IBGE para a qualidade da vida democrática:

> Em primeiro lugar, não restam dúvidas de que os estudos demográficos e os métodos estatísticos são parte essencial de uma ideia democrática de Governo e de Administração Pública. As políticas públicas, quando amparadas por evidências (sejam elas de natureza quantitativa ou qualitativa), garantem não somente a efetiva realização das funções do Estado, ou o apuro técnico dos serviços públicos, mas também o justo controle político dos Poderes republicanos. Porque as políticas públicas podem ser analisadas racionalmente, elas também podem ser objeto do escrutínio dos cidadãos nos "fluxos de formação discursiva da opinião e da vontade"[...]
> Em outras palavras, *Demografia e Estatística contribuem de forma decisiva para a racionalização do debate público e, neste sentido, são essenciais para o pleno exercício da cidadania*.
> (STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020) – Voto do Exmo. Ministro Edison Fachin.

À época da decisão da ADI n.º 6387, o STF relatou sua preocupação com a situação da pandemia global e da adoção de medidas excepcionais utilizadas como justificativas para realizar políticas de vigilância e de coleta de dados de cidadãos. Não se pode desconsiderar que, em muitas realidades, a relativização de direitos para realizar políticas de vigilância tendem ao enfraquecimento de direitos individuais (LONG, 2020).

Para o STF, a ausência de diploma legislativo e de autoridade administrativa específicos para a proteção de dados evidenciou os riscos do compartilhamento e usos ilícitos dos dados em detrimento do titular. O vazamento de dados da empresa de Previdência Privada do Banco do Brasil que, por uma falha de segurança, causou a publicização de dados de 153 mil clientes foi utilizado como exemplo da periculosidade do compartilhamento de dados. No caso do Banco do Brasil, a falha relatada possibilitou o acesso a todos os dados pessoais de clientes por terceiros, os quais podiam editar e cadastrar beneficiários em nome do próprio cadastrado.

A decisão do STF enfatizou muito mais a insuficiência da estrutura física e organizacional do IBGE do que uma proibição em caráter geral de transferência de dados nos termos previstos na MP 954/2020. O que se definiu é que a coleta e compartilhamento de dados pessoais, ainda que em cenários de crise, devem seguir parâmetros constitucionais e legais que atendam, em síntese, a relação de necessidade e adequação. Para o Supremo, a intervenção

prevista na MP n.º 954/2020 somente seria possível com o reforço das garantias de natureza procedimental – ou seja, apenas com um incremento do conjunto de filtros e salvaguardas relativos aos dados dos usuários poderia, a priori, justificar tal ingerência.

Pela conclusão do STF, é possível concluir que o compartilhamento de informações diretamente ligadas à identidade do indivíduo (como nome e número de telefone) em muito se distancia do compartilhamento de dados anonimizados, agregados e em bloco, como o realizado na iniciativa do Governo de São Paulo (SIMI-SP). Para a Corte Suprema, o nível de precisão na identificação dos usuários foi preocupante a ponto de direcionar a conclusão de que a influência negativa no nosso cotidiano seria mais do que apenas potencial.

Os dados de milhões de pessoas são chave de acesso com alto valor para execução de políticas públicas, mas também carregam um alto risco de adoção de expedientes prejudiciais ao indivíduo. Este risco se caracteriza pela possibilidade de tratamento irregular destes elementos individualmente descritivos, ou de sua utilização por terceiros que não eram, em princípio, os destinatários daquelas informações. Nesse sentido, cabe destacar o que o Ministro Ricardo Lewandowski considera como riscos da sociedade da informação:

> A atuação do IBGE, assim, é inegavelmente necessária para que os objetivos traçados na Carta Maior sejam alcançados. Ela identifica os potenciais e as carências dos diversos setores da sociedade, coletando dados que servirão de base para a elaboração das políticas públicas voltadas ao desenvolvimento nacional e à melhoria da qualidade de vida dos brasileiros [...]
> É preciso ficar claro, portanto, que não se está a falar de informações insignificantes, mas da chave de acesso a dados de milhões de pessoas, com alto valor para execução de políticas públicas, é verdade, mas também com provável risco de adoção de expedientes, por vezes, dissimulados, obscuros, que possam causar desassossego na vida diária do indivíduo. Este risco se caracteriza pela possibilidade do tratamento indevido destes elementos individualmente descritivos, ou de sua utilização por terceiros que não eram, a princípio, os destinatários daquelas informações. Estes são os chamados riscos da sociedade da informação, [...]
> (STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020) – Voto do Exmo. Ministro Ricardo Lewandowski.

Apesar de a especificidade do caso envolver a realização de políticas públicas no combate à pandemia do COVID-19, é possível verificar a ênfase no aspecto preventivo pela Corte Superior em sua análise voltada a efetivar a proteção de dados pessoais. Esse fator pode ser indicativo de uma tendência de futuras decisões, o que tem um impacto não apenas na interpretação de leis específicas – a exemplo do Código de Defesa do Consumidor (CDC) e da Lei Geral de Proteção de Dados (LGPD) – como também nas tecnologias que fazem uso de

dados pessoais, com especial destaque para a Inteligência Artificial (ciência que visa dotar programas e computadores com a capacidade de realizar atividades que são tradicionalmente consideradas como prerrogativas de humanos).

A potencial influência negativa da utilização de dados evidencia que o ponto determinante de uma utilização indevida de informações depende do *cenário* no qual está inserido. Nomes, telefones e endereços, por exemplo, são comumente disponibilizados pelos próprios titulares em cadastros para realização de uma compra. A questão que se coloca é a possibilidade de sua utilização para propósitos lesivos diante da vulnerabilidade de sistemas que podem reverter a anonimização de dados ou admitir o acesso indevido. A decisão do Supremo evidencia que não é o tipo de dado em si que carrega periculosidade, mas o potencial lesivo do *contexto* no qual pode ser utilizado. A exemplo do caso de enfrentamento do Coronavírus, a utilização de dados, ao mesmo tempo que útil para conter avanços do vírus, somente é legítima a depender do ambiente em que se insere.

O benefício prático do reconhecimento da tutela de dados, da autodeterminação informativa e da privacidade como direitos fundamentais também tem o benefício de indicar que tempos de crise não são uma carta em branco para ferir a Constituição. Conforme afirmam Andrej Zwitter e Oskar Gstrein (2020, *online*), em tradução livre:

> Embora uma crise como a pandemia do coronavírus exija medidas dedicadas, rápidas e eficazes, não devemos esquecer que os *dados são contextuais*. Um mesmo conjunto de dados pode ser sensível em diferentes contextos, e precisamos de estruturas de governança para garantir que esses dados sejam gerados, analisados, armazenados e compartilhados em sistemas legítimos e formas responsáveis. À luz da pandemia COVID-19 dados de localização podem ser muito úteis para análises epidemiológicas. *No contexto de uma crise política, os mesmos dados de localização podem ameaçar o estado de direito, a democracia e o gozo dos direitos humanos*. *– grifos da autora*.

Por esse raciocínio, interessante a crítica de Daniel Solove (2011) para se opor à ideia de que a privacidade deve ou pode ser mitigada em tempos de crise a título de beneficiar a segurança (ou outro valor da coletividade)[13]. Para o doutrinador, há uma falsa dicotomia entre

[13] Daniel Solove critica a ideia de que a privacidade deve ser mitigada em tempos de crise, a título de beneficiar a segurança. Para o doutrinador, há uma falsa dicotomia entre privacidade e segurança, como se ambos os valores fossem mutualmente excludentes. Cuida-se do "argumento do pêndulo", segundo o qual, em tempos de crise o pêndulo vai em direção à segurança e, em tese, permite o sacrifício de direitos, enquanto em tempos de paz, o pêndulo volta para a valorização da liberdade e da proteção de direitos. Nas palavras do doutrinador, "*sacrifícios de direitos e liberdades civis devem ser feitos somente quando o governo justifica adequadamente por que esses sacrifícios são necessários. É preciso submeter tais restrições a um escrutínio meticuloso, especialmente porque, em tempos de crise, o medo distorce nosso julgamento. (...) devemos ser extremamente cautelosos ao fazer sacrifícios desnecessários*" (tradução da autora).

privacidade e segurança, como se ambos os valores fossem mutualmente excludentes. Cuida-se do "argumento do pêndulo", segundo o qual, em tempos de crise o pêndulo vai em direção à segurança e, em tese, permite o sacrifício de direitos, enquanto em tempos de paz, o pêndulo volta para a valorização da liberdade e da proteção de direitos. Nas palavras do doutrinador, em tradução da autora:

> sacrifícios de direitos e liberdades civis devem ser feitos somente quando o governo justifica adequadamente por que esses sacrífícos são necessários. É preciso submeter tais restrições a um escrutínio meticuloso, especialmente porque, em tempos de crise, o medo distorce nosso julgamento. [...] devemos ser extremamente cautelosos ao fazer sacrifícios desnecessários"
> [...]
> Não apenas o argumento do pêndulo está errado ao supor falsamente que sacrifícios de direitos e liberdades civis são sempre necessários, mas também ao ignorar a essência do porquê os direitos e as liberdades civis são importantes. A proteção da liberdade é ainda mais importante em tempos de crise, quando ela está sob a maior ameaça. Durante os tempos de paz a necessidade de protegê-la não é tão imperiosa, justamente porque nesse período é menos provável que façamos sacrifícios desnecessários de liberdade. A maior necessidade de salvaguardar a liberdade ocorre nos momentos em que menos queremos protegê-la, quando nosso medo obscurece nosso julgamento. Quando as coisas ficam difíceis é justamente o momento em que nós mais precisamos de direitos.

De fato, eventuais restrições ao direito à privacidade, à proteção de dados e à autodeterminação informativa podem (e devem) ocorrer. Em outras palavras os direitos e garantias fundamentais, tais como a intimidade, vida privada e sigilo de dados, não são absolutos ou ilimitados,[14] mas medidas de mitigação devem ser orientadas por parâmetros constitucionais e legais – e também pela capacidade de segurança que o agente de tratamento pode proporcionar em sua atividade.

Todo esse cenário revela que a simplicidade de conceituação de dados anônimos pela LGPD esconde uma gama de temas complexos – inclusive já enfrentados pela justiça brasileira. O art. 5º, III, desse diploma normativo, define dado anônimo como aquele "*relativo a titular*

[14] Nas razões de voto, o Ministro Alexandre de Moraes se posiciona: "Encontram, obviamente, limites nos demais direitos consagrados pela nossa Carta Magna. É o denominado, pela doutrina, princípio da relatividade ou da convivência das liberdades públicas. Quando houver conflito entre dois ou mais direitos ou garantias fundamentais, deverá o intérprete [como o STF] ... utilizar-se do princípio da concordância prática ou da harmonização, de maneira a coordenar e combinar os bens jurídicos em conflito, para que se evite o sacrifício total de uns em relação a outros, realizando também, quando possível, por óbvio, redução proporcional do âmbito de alcance de cada um e a resolução da chamada contradição de princípio - sempre em busca do verdadeiro significado da norma e, mais do que isso, em tempos confusos, em tempos conflitantes, sempre buscando a harmonia do texto constitucional com sua finalidade precípua. Isso já vem também, todos sabemos, expresso no art. 29 da Declaração dos Direitos Humanos das Nações Unidas, que expõe que a finalidade dos direitos fundamentais é a proteção de toda a sociedade, do bem-estar de uma sociedade democrática."

que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" e conceitua anonimização (art. 5º, XI, da LGPD) como a "*utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo*".

Não há dados insignificantes. Há um risco inerente de um dado anônimo se transformar em um dado pessoal. O próprio art. 12, da LGPD, reconhece a possibilidade de dados anonimizados sofrerem processos de reversão para a identificação de seus titulares[15]. A partir da conjunção de diversas informações que descrevem um sujeito de forma parcial, é possível montar a imagem final do sujeito então anônimo – o que é descrito como um efeito mosaico da disposição dos dados (BIONI, 2020). Tecnologias que empregam inteligência artificial se tornam cada vez mais avançadas, o que reforça o fato de que a caracterização de um dado como anônimo deve ser analisada caso a caso e de acordo com a tecnologia disponível ao tempo de seu tratamento.

Interessante notar que a noção da importância do *contexto* nos quais dados são inseridos é essencial para aferir a constitucionalidade ou legalidade de uma medida não apenas para a utilização de dados anônimos, mas também para a avaliação do uso de dados sensíveis. Para os dados anônimos, a análise do contexto visa avaliar, em especial, a possibilidade de aplicação de processos de reversão para identificação dos titulares dos dados. Para os dados sensíveis, de modo correlato, a avaliação do contexto é determinante para aferir o graus de *riscos* de discriminação a que estão sujeitas as pessoas diante de um tratamento de dados pessoais.

1.2.2 Dados sensíveis: a relevância do contexto.

Dados sensíveis são aqueles que apresentam maior potencial de utilização discriminatória ou lesiva. Em geral, citam-se como sensíveis os dados sobre orientação sexual, etnia, convicção política ou religiosa, históricos médicos ou dados genéticos de um indivíduo. No Brasil, a LGPD conceitua como sensível o dado pessoal "*sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter*

[15] LGPD. 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.

religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II, da LGPD).

A elaboração dessa categoria de "maior importância" ou de classificação hierárquica superior que os diferencia dos tipos "comuns" de dados pessoais não é isenta de críticas. Uma categorização prévia de dados "mais importantes" pode ofuscar a noção de que as capacidades tecnológicas de processamento de dados permitem a construção de um ambiente de discriminação baseado em informações tidas por *comuns*, públicas ou mesmo publicizadas pelos próprios titulares. Como sintetiza Danilo Doneda (2021, p. 147 e 148): "*... cada vez mais é patente que mesmos dados não qualificados como sensíveis, quando submetidos a determinado tratamento, podem revelar aspectos considerados sensíveis sobre a personalidade de alguém, podendo levar a práticas discriminatórias*."

Em outras palavras, é como o dado é processado e em que contexto é inserido que evidencia sua periculosidade. Justamente por compreender a riscos de um tratamento – e não do dado em si – a Alemanha orientou seu posicionamento no sentido de não adotar um regime *a priori* diverso para uma categoria de dados sensíveis (DONEDA, 2021).

O Brasil optou por caminho distinto. A Lei Geral de Proteção de Dados diferencia dados pessoais "comuns" de dados sensíveis (art. 5º, I e II respectivamente). Pela normativa, dado pessoal é todo aquele que identifica ou permite a identificação de uma pessoa. Dado pessoal sensível, por sua vez, é o dado vinculado a uma pessoa natural que dispõe sobre questões étnicas, raciais, religiosas, políticas, sindicais, filosóficas, orientação sexual, de saúde, genéticas ou biométricas (art. 5º, II, da LGPD).

A despeito das críticas, a opção do legislador brasileiro em adotar uma hierarquia classificatória de dados pessoais não é sem fundamento ou despropositada. De fato, qualquer tratamento de dados pessoais pode revelar aspectos sensíveis de uma pessoa e possibilitar tratamentos discriminatórios ou mesmo ilícitos – ainda mais no contexto de evolução tecnológica contínua. Por outro lado, a classificação permite uma visualização prática sobre a dimensão da periculosidade dos dados. Em outras palavras, a utilidade da classificação dos dados sensíveis refere-se a uma parametrização *a priori* de riscos. Nos dizeres de Danilo Doneda (2021, p. 148):

> a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações nas quais a discriminação pode advir sem que sejam utilizados dados sensíveis.

Ainda sobre os aspectos práticos da diferenciação, a LGPD elencou hipóteses mais permissivas da atividade de tratamento de dados "comuns" e mais restritas para os dados pessoais sensíveis. O art. 7º da normativa elenca dez hipóteses nas quais o tratamento de dados pessoais "comuns*"* (art. 5º, I, LGPD) pode ser realizado:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Por outro lado, o art. 11, da LGPD, elenca oito hipóteses nas quais as informações pessoais sensíveis podem ser objetivo de uma atividade de tratamento de dados:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Note-se que o rol apresentado pela LGPD é taxativo, conforme a disposição expressa tanto do *caput* do art. 7º quanto do *caput* do art. 11, os quais mencionam que o tratamento de dados pessoais "*somente poderá ocorrer*" quando se enquadrar em alguma das alternativas apresentadas. No entanto, ao se analisar as hipóteses permissivas descritas pela LGPD, nota-se uma grande abertura de fundamentos que podem ser utilizados para legitimar as mais diversas finalidades de um tratamento de dados. A hipótese de um tratamento amparado no legítimo interesse, por exemplo, é uma das cláusulas mais abertas e maleáveis previstas na LPGD.

Pode-se apontar, em síntese, que o art. 7º, da LGPD, elenca três grandes hipóteses permissivas para a atividade de processamento de dados pessoais: i) pelo consentimento informado, ii) por determinação ou autorização legal e iii) pelo legítimo interesse. A maior diferença no tratamento de dados pessoais sensíveis refere-se ao fato de que o art. 11, da LGPD, não indica, de forma expressa, o legítimo interesse como base legal para o exercício da atividade.

Tanto a análise dos dados anônimos quanto a dos dados sensíveis revelam que não há dados insignificantes para a sociedade da informação. A tecnologia permite formar um mosaico para identificar um indivíduo a partir de dados que passaram por processos de anonimização e é preciso considerar que quaisquer dados pessoais podem ser utilizados para inferir aspectos sensíveis de uma pessoa. Esses fatores revelam a necessidade de aprofundar a extensão do conteúdo normativo que se pretende alcançar com a tutela aos dados pessoais.

Por outro lado, a diferenciação de um conteúdo sensível pela legislação é justificável. Trata-se de um esforço legislativo para proteger dados pessoais que tornam seus titulares mais suscetíveis a riscos, discriminações ou outros tratamentos lesivos. Ademais, o aplicador do direito deve se atentar para as diferentes hipóteses legitimadoras dos tratamentos de dados para os casos de a atividade envolver os dados classificados, *a priori*, como sensíveis.

2. IMPACTOS DA INOVAÇÃO TECNOLÓGICA NA REFORMULAÇÃO DOS DIREITOS À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS.

A sofisticação e a ampliação de capacidades de sistemas de computação recaem, em grande medida, no processamento de dados – cujo fluxo, produção e armazenamento são continuamente impulsionados pelos avanços tecnológicos e pela respectiva incorporação destes no cotidiano das pessoas e empresas. É o que se observa, por exemplo, com a difusão do uso de *smartphones*. A perfilização[16] (*profiling*) e a avaliação de crédito são apenas amostras de atividades que tanto produzem quanto demandam dados no seu processamento.

O impacto na vida privada das pessoas tomadas como alvo do tratamento de dados (a exemplo do sistema de *credit score* e por *data brokers*[17]) ou que envolvam sua interação com esses sistemas (como no caso de redes sociais ou sites de busca) provoca a reflexão sobre desdobramentos jurídicos do emprego da tecnologia nas relações sociais – particularmente as mais polêmicas, como a Inteligência Artificial. O domínio do conceito normativo[18] de privacidade e da proteção de dados pessoais ganha destaque nesse cenário, especialmente quanto à indicação dos seus meios de tutela e modos de compensação por sua violação.

No âmbito do desenvolvimento da tecnologia e inovação, a privacidade é muitas vezes tratada como um subtópico de temas relacionados com a segurança digital. Por esse contexto, a compreensão quanto à efetividade da proteção à privacidade recai sobre medidas relacionadas a obliterar vínculos identificadores de informações (como processos para anonimização de dados pessoais) ou na ocultação de conteúdos por meio de criptografias de ponta a ponta e outras medidas de segurança como o gerenciamento de assinaturas digitais e a implementação de métricas de *K-anonymity*[19].

---

[16] Perfilização é o tratamento de dados que objetiva a análise e predição de comportamentos pessoais, profissionais, de consumo e de crédito. (ZANATTA, 2019).

[17] A expressão *Data brokers* descreve a atividade de entidades que coletam dados pessoais ou de empresas, disponíveis em fontes de natureza pública ou até mesmo provenientes de terceiros (que coletaram os dados de forma legítima) para organizá-las, classificá-las e comercializá-las para terceiros. Normalmente utilizadas para elaborar perfis de consumidores, os propósitos do monitoramento são variados, como avaliação de seguros, prestação de serviços bancários, campanhas publicitárias ou avaliação de crédito.

[18] A privacidade pode ser analisada sob diversos ângulos: como preceito ético (ou seja, como valor, virtude ou dever), por uma perspectiva econômica (como uma utilidade, interesse ou preferência) ou por um viés político (como um bem público ou privado; como política pública ou controle social). O foco no presente trabalho é a perspectiva legal, ou seja, seu conceito normativo que abrange temas como a definição de um direito, limites para seu exercício e tutela em caso de violação.

[19] *K-anonymity* é uma propriedade de uma base de dados (*dataset*) que permite avaliar (medir) o grau de reidentificação da informações armazenadas. Qualquer conjunto de dados tem a probabilidade máxima de 1/K de permitir a reidentificação. Quanto maior o valor de K, menor a probabilidade de referenciar a quem os dados se referem. Ocorre que o anonimato excessivo pode implicar na inutilidade dos dados para os propósitos de seus destinatários em decorrência da distorção nas informações ou na impossibilidade de análises que não reproduzam

Embora a criptografia, processos de anonimização e temas relativos à segurança de dados sejam de fato relevantes para promover a proteção à privacidade, o conceito normativo deste termo não se limita a questões de identificação e de confidencialidade. A representação de uma pessoa a partir de seus dados ressoa em questões relativas às suas próprias decisões: com quem se relaciona, quais conteúdos irá usufruir, quais escolhas poderá tomar. São aspectos do desenvolvimento do seu próprio ser, de sua personalidade, cuja tutela não se limita à ocultação de suas informações.

A busca de uma delimitação teórica de conceitos deve considerar que o significado da privacidade é contextual, histórico e dinâmico. Abrange tanto uma noção de liberdade negativa contra intromissões (dever de que outros se abstenham de interferir na vida privada) como a de liberdade positiva, compreendida como o direito de controlar o modo pelo qual as informações pessoais são adquiridas e processadas – perspectiva que é, por vezes, designada como privacidade informacional[20] (TURKINGTON, 1990).

Ocorre que a dinâmica de transformações sociais revela uma insuficiência de ambas as perspectivas para delimitar o alcance do conceito de privacidade, especialmente quando se leva em consideração a ausência de escolhas do usuário para a utilização de serviços online, a tomada de decisões autônomas independentemente de seu consentimento (ou mesmo de seu conhecimento) e a sensível questão de direcionamento de conteúdos para influenciar sua posição ideológica – por vezes baseadas em argumentos falaciosos.

Sobre a insuficiência da acepção da privacidade como liberdade negativa (dever de abstenção), tem-se o fato de que dados são coletados, produzidos e processados diuturnamente em proporções acima de qualquer controle e independentemente da vontade do indivíduo, o que mitiga a possibilidade de uma ocultação voluntária de informações ou de uma ampla proibição contra intromissões.

Sobre a liberdade positiva (direito de controlar o fluxo ou o tratamento de dados pessoais), o volume, velocidade, variedade e capacidade de processamento de dados (conhecido como o fenômeno do *Big data*), demonstram que o controle de operações por meio do consentimento do titular é, no mínimo, impraticável (se não intangível) na sociedade

---

resultados incorretos ou até mesmo tendenciosos. GOOGLE. Cloud Data Loss Prevention. *Computing k-anonymity for a dataset Guide*. Disponível em: https://cloud.google.com/dlp/docs/compute-k-anonymity#:~:text=K%2Danonymity%20is%20a%20property,people%20also%20in%20the%20dataset. Acesso em: 27/03/2023.

[20] Tradução livre da expressão "Informational privacy" apresentada por Richard Turkington, pela qual o direito à privacidade informacional é suscitado como uma reivindicação contra quem adquiriu ou divulgou informações pessoais ou íntimas sem o respectivo consentimento. Traduz, portanto, uma noção de controle sobre os dados pessoais. (TURKINGTON, 1990)

contemporânea – o que revela a insuficiência de uma perspectiva positiva da privacidade, traduzida como controle sobre os dados por meio da manifestação de seu consentimento.

Como solução a esse impasse, em outra acepção, o refinamento do conceito normativo da privacidade destaca sua relação com a *construção da identidade* do indivíduo – e não apenas com a possibilidade de sua identificação (HILDEBRANDT, 2020). Note-se que a "identificação" de uma pessoa é, em si, um aspecto pontual, próxima à noção da descrição de um fato. A "construção da identidade", por sua vez, é uma característica dinâmica e intrínseca à dignidade da pessoa humana, que abrange a liberdade de pensamento, de ser e de mudar. Nessa perspectiva, a privacidade e a tutela de dados pessoais se revelam como projeções da tutela à dignidade da pessoa humana, como direitos fundamentais e inerentes à personalidade do indivíduo ou como direitos humanos que transcendem limites territoriais. É o que Agre e Rotenberg (1997) retratam como o direito de estar livre de restrições desmedidas[21] na construção de sua identidade[22].

Danilo Doneda (2021) expõe outra linha de raciocínio, pela qual a proteção de dados pessoais é um dos meios pelos quais a conotação contemporânea da privacidade se manifesta, com destaque para uma concepção coletiva (e não apenas individualista) da privacidade, ou seja, um conceito que converge as relações da própria personalidade com o mundo exterior. Pode-se inferir, por essa perspectiva, que a privacidade remete à um desenvolvimento do próprio ser enquanto indivíduo, ao passo que a proteção de dados remete ao desenvolvimento da personalidade perante a coletividade. Enquanto é possível notar conotações diferentes de ambos os direitos, cabe esclarecer que essa diferenciação foi exposta, mas não defendida pelo autor. Danilo Doneda (2021, p. 44) reconhece a tutela de dados pessoais como a continuação da privacidade por outros meios.

De fato, privacidade e proteção de dados são termos que convergem no objetivo de contemplar a ampla proteção da pessoa humana, tomada como valor máximo do ordenamento brasileiro (art. 1º, III, CF/1988). O esforço diferenciação de ambos em muito recai na vontade (ou mesmo necessidade) epistemológica dos intérpretes, os quais, em grande medida,

[21] Fala-se em "desmedidas" ou desarrazoadas porque uma infração à privacidade de alguém pode ser legalmente justificada, de modo a não ofender o *direito* à privacidade. A título de exemplo, o Estado pode ingressar na residência de um indivíduo no caso de desastre ou flagrante delito (art. 5º, XI, da CF). Trata-se de uma infringência à sua privacidade, mas não uma violação ao direito de privacidade.

[22] Segundo os autores: "*From this perspective, control over personal information is control over an aspect of the identity one projects to the world, and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity*." (1997).

reconhecem a conceituação suficiente de um direito como exigência para a coesão de um sistema.

Ocorre que a tutela da privacidade há muito depende de uma valoração complexa do seu conteúdo mediante o sopesamento das situações concretas de sua aplicabilidade. A proteção dos dados, que ganha destaque crescente à vista dos desenvolvimentos tecnológicos, não segue caminho diverso, pois sua compreensão atende às particularidades frente às situações concretas que contextualizam sua análise.

A gênese dos pressupostos ontológicos da proteção de dados e da privacidade é, de fato, congênere. Se as situações concretas exigirem a tutela de ambos, não há a necessidade de defender uma conceituação estritamente distinta como se a tutela de um ocorresse em detrimento do outro. Seja pelo reconhecimento da tutela de dados pessoais como a continuação, por outros meios, da privacidade (DONEDA, 2021) ou pela compreensão de que há uma zona de convergência e, em certa medida, um conteúdo próprio de cada direito, uma vez que se mostra possível avaliar o atendimento ao conjunto de direitos que tutelam a personalidade de um indivíduo, restará atendido o valor máximo da tutela da pessoa humana. Esse é o propósito principal que deve orientar o intérprete.

2.1 Correlação da acepção de privacidade e direitos conexos.

A distinção conceitual do direito de privacidade marca intensa discussão doutrinária que se estende ao longo de décadas. No final do século XIX, a consideração do impacto de tecnologias como a máquina fotográfica e a divulgação de imagens em tabloides acerca da vida privada de socialites em festas é tomada, pela doutrina majoritária, como o contexto que iniciou a discussão jurídica acerca da necessidade de proteger um direito à privacidade (WARREN; BRANDEIS, 1890).

A privacidade, à época, era vista como garantia de inviolabilidade de aspectos da vida privada do indivíduo. Assumia a natureza de um direito individual negativo cuja aptidão, ao ser invocado, voltava-se a garantir uma imunidade ou defender uma barreira à vida privada de uma pessoa, ao que é sintetizado como o direito de ser deixado em paz ou, no original, *the right to be let alone*. A expressão, que ganhou grande notoriedade, foi empregada pelo magistrado Thomas Cooley para consolidar o posicionamento que já vinha sendo adotado pelos tribunais. No entanto, sua autoria é comumente atribuída ao artigo de Samuel Warren e Louis Brandeis (1890). De toda forma, o texto se revelou paradigmático por inaugurar a possibilidade, a partir

de precedentes da tradição do *common law*, da identificação de um direito de privacidade de natureza pessoal, ou seja, independente da estrutura da tutela da propriedade.

A associação da autoria da expressão "*the right to be let alone*" à Warren e Brandeis e a assunção de que seu conteúdo foi apresentado como o primeiro conceito de privacidade (ou seja, compreendido como o direito de ser deixado só) é relativamente equivocada. Como esclarece Danilo Doneda (2021, p. 104), Warren e Brandeis não chegaram a trabalhar com uma perspectiva fechada (estanque) da privacidade e foi Thomas Cooley o autor da citação viralizada:

> [...] um ponto de vista corriqueiro, que é a menção a um "direito de ser deixado só", tantas vezes sendo apontado como sendo a definição de Warren e Brandeis, não é de todo exato: em seu mencionado artigo, os autores em nenhum momento definem estritamente o *right to privacy*. A associação que geralmente é feita do artigo com o *right to be let alone* deve ser relativizada: essa é uma citação do magistrado Thomas Cooley, que os autores não chegam a afirmar que traduziria propriamente o conteúdo do direito à privacidade – ou seja, Warren e Brandeis não chegaram a trabalhar com uma perspectiva fechada de *privacy*.

De toda forma, a compreensão histórica do direito à privacidade comumente vincula o início de seu desenvolvimento à noção do direito à tranquilidade ou de ser deixado só como um entendimento extraído do artigo paradigmático de Warren e Brandeis "*The Right to Privacy*" (1890). Essa concepção, tomada como tradicional, pressupõe a divisão entre as esferas pública e privada, de modo a definir um direito de resguardo às informações ou aspectos da vida pessoal classificadas como particulares.

Trata-se de um sentido fortemente individualista no qual a proteção à privacidade volta-se a reconhecer uma posição estática e absenteísta do Estado encarregado de garantir o direito do titular de retrair aspectos de sua vida do domínio público (BIONI, 2019). Na classificação dos conceitos da privacidade, esse posicionamento é tomado como o sentido negativo do termo, justamente por retratar essa noção de um dever de abstenção, de não fazer, de não tornar público o que for privado.

No século XX, a concepção de privacidade passou por profundas transformações sobre seu sentido e alcance. A noção de direito subjetivo da privacidade, como um direito de exercer uma "predileção" individual associada a uma tranquilidade ou conforto se mostrou insuficiente para garantir a autonomia privada no desenvolvimento da própria personalidade, especialmente frente aos potenciais de controle e influência atribuídos aos avanços da tecnologia da informação (DONEDA, 2021, p. 131):

> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos.

A imensa dificuldade de enquadrar a privacidade em uma concepção coerente e unitária foi agravada com esse desenvolvimento. Cabe compreender que a busca de uma definição estanque e que reflita um consenso da semântica de privacidade é inerente àqueles que buscam uma coesão de um sistema. Ocorre que a perspectiva epistemológica de análise do termo acaba por gerar um processo de excessiva generalização, o que culmina em uma definição eminentemente abstrata ou tautológica, tais como a definição de privacidade como intimidade; como o direito de manter segredo ou da reserva da vida privada; como um dever de sigilo, de recato ou de confidencialidade.

A gradação de termos para refletir a privacidade foi outra perspectiva defendida por muitos doutrinadores e foi até mesmo adotada pela Suprema Corte alemã – importante esclarecer que foi posteriormente abandonada.

É o caso da teoria dos círculos concêntricos ou teoria das "esferas" da personalidade, detalhada por Heinrich Hubmann (STRÖMHOLM, 1967, pág. 75). O autor desenvolve seu argumento a partir da constatação de que há um direito geral de personalidade que pode ser dividido em três grupos: o direito de *desenvolver uma personalidade*, o direito de *defender a própria personalidade* e o direito de defender a própria *individualidade*.

O primeiro grupo abrange direitos protegidos eminentemente por normas de direito público, como o direito de livre associação ou de expressão. O segundo compreende os direitos tutelados por nomas de cunho privado, como proteção à propriedade intelectual. O terceiro grupo é o que de fato compreende a teoria das esferas por ele defendida. Baseada na distinção entre aspectos públicos e privados, propõe Hubmann a classificação do direito de *individualidade* em três esferas distintas: a da individualidade (em sentido estrito), a da vida privada e a da intimidade (ou do segredo).

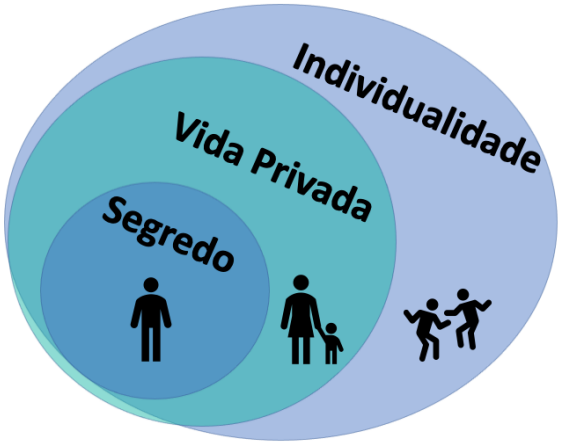

Figura 6 - Representação da Teoria das Esferas (círculos concêntricos) de Henrich Hubmann - 1953. Elaborado pela autora.

A esfera da individualidade compreende o nome de uma pessoa, o nome empresarial e a sua honra. A esfera privada remete à proibição de publicar a imagem de um indivíduo ou de descrições de sua vida, como caligrafias ou comportamentos em meio social. Por fim, a esfera da intimidade (ou do segredo) protege não apenas contra a divulgação ou exposição de informação, mas também contra o mero conhecimento de um tema por terceiros, tais como cartas confidenciais. Stig Strömholm (1967, pág. 56) assim descreve cada esfera dessa categorização de privacidade (em tradução livre, pela autora):

> [...] a esfera da individualidade compreende o nome de uma pessoa, seu nome comercial e a honra; [...] sobre do direito de defender sua "esfera privada", uma pessoa pode proibir a publicação não só de sua imagem, mas também de qualquer "retrato de sua vida" (*Lebensbild*), ou seja, uma descrição ou representação de sua vida, atos, palavras e pensamentos, e de um "*retrato de seu caráter*" (Charakterbild), como pode ser obtido a partir do acesso a palavras, atos, caligrafia e outros elementos passíveis de interpretação por meio de métodos científicos. O direito à "esfera da intimidade" vai além: protege não apenas contra a publicação, mas também contra qualquer ato pelo qual um terceiro pode obter conhecimento tais como acesso a notas pessoais e cartas confidenciais.

A análise das esferas – ou de qualquer categorização de termos conexos à privacidade – tem o eminente propósito de determinar os limites de uma pretensão de defesa ou de identificar em que momento não mais prospera o argumento de proteção à esfera privada de alguém. Aliás, para Hubmann, apenas a esfera da intimidade (terceira e mais restrita categoria) seria protegida contra tentativas de obter informações de um sujeito.

Posteriormente referida como teoria da "cebola passiva" pela doutrina alemã – por conta da noção de camadas de acesso à vida privada de uma pessoa – a segmentação proposta por

Hubmann foi deixada de lado pela jurisprudência constitucional alemã a partir, em especial, da paradigmática decisão que reconheceu o direito à autodeterminação informacional, em 1983. (GERNETT, 2016).

À época, o Tribunal Superior Alemão conjugou dois fundamentos de sua *Basic Law* (Lei Constitucional de 1949) previstos no artigo 2, parágrafo [1] – direito de toda pessoa ao livre desenvolvimento da personalidade – e no artigo 1, parágrafo [1] – inviolabilidade da dignidade humana – para reconhecer o direito à autodeterminação informacional[23]. Essa formulação exigiu a redefinição dos conceitos de personalidade (*Persönlichkeit*) bem como sobre as condições necessárias para propiciar o seu "livre desenvolvimento" – antes marcadas por uma concepção "liberal clássica" da relação entre o indivíduo e o Estado na qual a proteção da personalidade foi inicialmente baseada (GERNETT, 2016).

Em um contexto histórico, os conceitos jurídicos de personalidade e do direito ao seu livre desenvolvimento na Alemanha foram empregados para atender aos propósitos contextuais da época: a restauração de uma cultura jurídico-moral após a cisão dessas acepções entre 1933 e 1945; e o fortalecimento e preservação de uma "jurisprudência estabelecida" (contínua) de modo a consolidar a noção de "segurança jurídica" a partir de 1949 (GERNETT, 2016). É importante constatar a enorme influência dos eventos que marcaram os anos de 1933 a 1945 (ascensão do nazismo) bem como o de 1949 (promulgação da Constituição Alemã) sobre as análises semânticas e argumentativas dos direitos analisados.

Da mesma forma, as terminologias empregadas pela Constituição brasileira devem ser lidas em razão do contexto no qual se encontram os direitos que visa proteger. Historicamente, por "vida privada", compreende-se o estabelecimento de limites, pautados por uma lógica de exclusão, para diferenciar a vida pública da vida privada (o que é privado não é público e vice versa). Ao lado dessa noção dicotômica de público e privado, há o termo "intimidade" que se refere aos eventos mais pessoais de um indivíduo, em uma compreensão próxima ao direito de tranquilidade, do direito de ser deixado só – *the right to be let alone* – (DONEDA, 2021).

A despeito da escolha pelo constituinte por termos diversos (intimidade e vida privada), não estamos diante de duas hipóteses distintas ou com valorações diferentes. Longe do objetivo de alcançar uma precisão dogmática sobre os limites entre ambos os conceitos, o legislador optou pelo excesso, ou seja, pelo desvio da discussão das fronteiras dos termos (ante o seu alto

[23] A numeração se refere à Constituição Alemã atualizada até a emenda prevista no "Act of 28 June 2022", traduzida para o inglês por Christian Tomuschat, David Currie, Donald Kommers e Raymond Kerr em cooperação com o *Language Service of the German Bundestag*, disponível em: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html Acesso em 12/04/2023.

grau de subjetividade) para evidenciar o seu foco principal, qual seja, a aplicação do direito fundamental da pessoa humana (DONEDA, 2021).

Os caminhos percorridos para definir o que se espera de um conceito de privacidade demonstram que a indefinição quanto ao seu conteúdo é uma característica intrínseca da matéria. As particularidades de cada sociedade e de cada contexto histórico são determinantes para justificar as diferentes concepções de privacidade. Há uma manipulação do termo pelo próprio ordenamento jurídico, pois "*não raro* [a privacidade] *é utilizada para suprir algumas de suas necessidades estruturais, assumindo um ou outro sentido em razão de determinadas características de um ordenamento e dificultando ainda mais a sua redução a um sentido comum*." (DONEDA, 2021, p. 102).

De toda forma, a privacidade ainda é o termo mais utilizado (e, talvez, o mais razoável) para se referir a uma qualidade da construção e "defesa da identidade" de uma pessoa. Seja em uma perspectiva de defender um dever de abstenção contra intromissões ou como o direito de controlar informações que descrevem uma pessoa, o conteúdo de privacidade se mantém atualizado justamente por ser contextual. Não há, cabe ressaltar, uma superação de conceitos anteriores, mas um aperfeiçoamento ou acréscimos de novas noções. Tampouco o termo ofusca a especificidade de vocábulos conexos – como intimidade ou vida privada – ou de direitos correlatos – como direito à imagem, à honra e à proteção de dados pessoais.

O termo privacidade se correlaciona, mas não exclui noções ou aplicações de direitos correlatos. Inclusive, sua acepção gera consequências diferenciadas. Sobre a violação à privacidade pela divulgação de dados pessoais (como nomes ou de endereços), por exemplo, os tribunais vêm consolidando o entendimento no sentido de que o dano deve ser comprovado para ensejar um dever de compensar. Em outras palavras, eventual afetação ao direito à privacidade não gera um automático e correspondente dever de indenizar:

> 4 - Responsabilidade civil. Danos morais. Exposição de dados pessoais em site da internet. A Lei de regência não contempla a indenização por danos morais *in re ipsa*. Ao contrário, a inteligência do art. 42 indica a necessidade de demonstração, em concreto, do dano causado pelo tratamento inadequado de dados. Nos cadastros da ré não consta dado sensível (referente a 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, inciso II da Lei) nem há demonstração de que os autores sofreram limitação ou vulneração a qualquer dos interesses essenciais da pessoa natural, como imagem, privacidade, honra, intimidade ou integridade corporal. **A disponibilização do nome, CPF e endereço residencial dos autores em site da rede mundial de computadores, por si só, não enseja a reparação por danos morais**. (...) Na forma do art. 18, inciso VI, da Lei 13.709/2018 (LGPD), o titular dos dados

> pessoais tem direito a obter do controlador, a qualquer momento e mediante requisição, a eliminação dos dados pessoais tratados."
> Acórdão 1434128, 07397589020218070016, Relator: AISTON HENRIQUE DE SOUSA, Primeira Turma Recursal, data de julgamento: 24/6/2022, publicado no DJE: 14/7/2022. – grifos da autora.

Sobre o direito à imagem, por outro lado, é entendimento sumulado que a prova do prejuízo é dispensável pela publicação não autorizada de pessoas com fins econômicos ou comerciais (Súmula-STJ nº 403). Desse modo, o STJ firmou o entendimento de que a mera publicação com propósitos econômicos ou comerciais da imagem de terceiro, sem a sua autorização, configura dano moral *in re ipsa*. Nota-se que, a despeito da intensa correlação entre o direito à privacidade e o direito à imagem, o tratamento jurisprudencial é diferenciado.

Todo o cenário exposto evidencia a possibilidade de convivência da noção contextual da privacidade com as peculiaridades e tratamentos diferenciados a direitos e expressões correlatos. Ainda que teorias como as dos círculos concêntricos de Hubmann não tenham sido suficientes para diferenciar termos como intimidade, vida privada e privacidade, o que se busca ressaltar é que o intérprete não pode olvidar do contexto histórico que justificam a utilização dos termos empregados pelo legislador ou constituinte. Conclui-se, ademais, que a proximidade conceitual de direitos conexos não se confunde com uma obrigação de serem dadas respostas iguais pelos tribunais. A presunção do dano constante da Súmula 403, do STJ, evidencia essa conclusão.

2.2 Convergência da tutela à privacidade e o direito à proteção de dados pessoais.

Historicamente, a tutela conferida pelos direitos fundamentais assumiu um papel pautado na relação verticalizada entre o Estado e o cidadão. Pela perspectiva da proteção contra ingerências externas, a privacidade é tida como dever e atribuição do Estado. Trata-se de uma conotação negativa do termo – ou seja, um dever de não fazer. Essa proteção não foi superada ou substituída. Há exemplos atuais de proteção constitucional nessa perspectiva, como o direito fundamental à inviolabilidade da casa de um indivíduo, ressalvadas as condições expressas e restritas a essa regra – como em caso de flagrante delito ou desastre, para prestar socorro ou, durante o dia, por determinação judicial (art. 5º, XI, CF/1988).

Outro exemplo, que ressalta a proteção contra ingerências externas e se revela a favor de uma noção de proteção aos segredos da vida privada, é o direito fundamental ao sigilo das correspondência e das comunicações telefônicas – o qual somente pode ser excepcionado por

ordem judicial e nas hipóteses legais para fins de investigação criminal ou de instrução processual penal (art. 5º, XII, CF/1988).

O conceito normativo de privacidade em sua perspectiva negativa não perde importância na atualidade. Essa concepção assume especial relevância para ressaltar que a noção subjetiva de privacidade não se confunde com o *direito* de privacidade. Uma mesma situação pode infringir uma *noção* subjetiva de intimidade (como adentrar em uma residência sem anuência do proprietário) mas, ao mesmo tempo, não violar o *direito* de privacidade (como no caso de flagrante delito). Em tais situações, a interferência na vida privada é justificável, de modo que a mitigação da privacidade pela noção subjetiva de alguém não se confunde com uma violação ao seu *direito* de privacidade.

Essa perspectiva pode ser estendida ao direito à proteção de dados pessoais. É o caso da utilização de dados pessoais para fins de desenvolvimento e implementação de políticas públicas; para a supervisão de atividades financeiras pelo Banco Central e pela Receita Federal ou para atender aos deveres de publicidade e transparência impostos ao Estado (como divulgação nominal de folhas de salários de servidores). A privacidade ou os dados pessoais podem até ser turbados em uma percepção subjetiva individual, mas não há violação ao *direito* de privacidade pelo seu conceito normativo (HILDEBRANDT, 2020).

Transcendendo a noção de um dever de não interferência, a proteção de dados é utilizada como justificativa para o ingresso de uma concepção tomada como liberdade positiva da privacidade. Por essa perspectiva, não se trata de salvaguardar a esfera privada de alguém, uma vez que se reconhece que a coleta de dados muitas vezes é realizada independentemente da vontade do indivíduo. Trata-se de um dever de transparência voltado a garantir que o tratamento de dados coletados seja comunicado ao titular e que este tenha a possibilidade de interferir nas finalidades dessa atividade (ou ao menos tomar conhecimento desses propósitos).

Na busca de definir limites que permitam distinguir a privacidade e a proteção de dados pessoais, não há divergência relevante em reconhecer que há áreas de sobreposição entre ambos. É o caso, a título de exemplo, no qual os dados pessoais são utilizados para apoiar atividades como um modelo de negócio, o comércio eletrônico ou a publicidade direcionada – há que se considerar tanto a noção de privacidade quanto a de tutela de dados pessoais (há a necessidade, portanto, de considerar a tutela de ambos os direitos).

Por outro lado, Mireille Hildebrandt (2020) defende que a privacidade engloba matérias que não dizem respeito à proteção de informações pessoais, tais como temas relativos à inviolabilidade do domicílio e da correspondência ou mesmo para o exercício do direito de disposição do próprio corpo (em reforço a esse argumento, cabe acrescentar que a privacidade

já foi utilizada como argumento a favor do direito de escolha ao aborto e para tomar pílula anticoncepcional).

Da mesma forma, seguindo o raciocínio da autora (HIDELBRANDT, 2020), o direito à proteção de dados pessoais concerne à atividade de tratamento de informações que identifiquem ou tornem identificável uma pessoa, o que nem sempre envolve a interferência de um direito à privacidade. É o caso de dados pessoais serem processados por solicitação do próprio titular para finalidades diversas, como abrir contas em bancos, para ingressar em eventos ou para participar de pesquisas censitárias. Nesses exemplos, se houver uma mudança de finalidade no tratamento de dados que se distancie da autorizada pelo titular, não haverá necessariamente uma violação a um dever de sigilo, mas sim, ao direito à proteção de dados pessoais.

Cabe contextualizar que o raciocínio de Mireille Hildebrandt é desenvolvido para promover a compreensão de conceitos jurídicos por profissionais da computação. É inerente a esse ramo a noção exemplificativa e simplificada de termos. De fato, o que importa para a ciência da computação é muito mais o resultado que pode ser alcançado do que a formulação de um conceito amplo o suficiente para abranger todos os aspectos históricos e contextuais nos quais a tutela da privacidade (e dos dados pessoais) são invocados. Nesse sentido, privacidade, para a autora, é tomada como um dever de sigilo enquanto a proteção de dados é abordada como um direito de acesso e de retificação. Trata-se de uma simplificação que auxilia na compreensão dos termos.

Na prática, por outro lado, o desenvolvimento dos conceitos normativos da privacidade e da proteção de dados não ocorreu em um movimento histórico linear. Tampouco há o rigor na divisão estanque dos termos nas disposições normativas brasileiras. No plano constitucional, a tutela de tais direitos encontra proteção implícita nos incisos X e XII, do art. 5º, da Constituição Federal e, a partir da promulgação da Emenda Constitucional 115/2022, a tutela de dados pessoais passou a constar de forma expressa na Constituição (art. 5º, LXXIX).

Aliás, o direito de acesso e o de retificação há muito já são reconhecidos como aspectos da privacidade, o que demonstra que o conceito jurídico do termo de fato ultrapassa a mera noção de sigilo, de um dever de ocultação de informações. A via do habeas data visa (art. 5º, LXXII, da CF/1988), que visa garantir o conhecimento de informações pessoais presentes em registros ou bancos de dados de entidades de caráter público ou para possibilitar anotações ou correções desses registros, também é reconhecida pelo STF como um dos meios à proteção da privacidade do indivíduo (STF - HD: 93 DF, Relator: Min. Ellen Gracie, Data de Julgamento: 03/12/2010, DJe-240).

Pelo exposto, ao menos em uma perspectiva jurídica, constata-se que é intensa a correlação entre os conceitos de privacidade e de proteção de dados pessoais, seja pela similaridade de sua gênese e de seus conteúdos, seja pela necessária valoração contextual para anunciar o *propósito* de sua definição. De fato, é coerente a posição que defende que há uma zona contextual que não diz respeito a ambos, mas a apenas um dos direitos. Por outro lado, também é inegável o reconhecimento de que há uma zona de sobreposição – ou de convergência – entre a tutela ao direito à privacidade e à tutela aos dados pessoais.

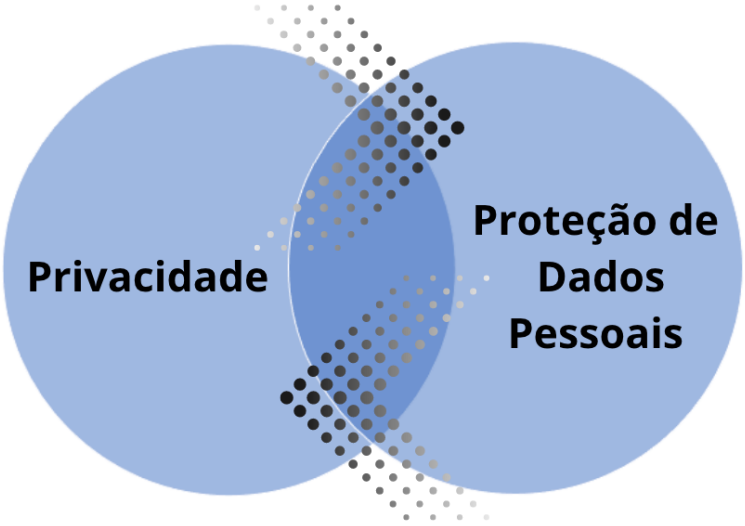

Figura 7. Correlação Privacidade e Proteção de Dados Pessoais. Elaborado pela autora.

Como direitos fundamentais e direitos da personalidade, a privacidade e a proteção de dados pessoais convergem por assumirem características próprias, com destaque para as consequências de sua violação (o dano moral) e os modos de compensação. Ademais, a classificação desses preceitos como direitos da personalidade indica que a conotação de ambos os direitos não se submete a uma lógica de proteção patrimonial, típica do direito privado.

Defende-se que é pela perspectiva de uma *convergência conceitual* que o conteúdo do direito à privacidade e à proteção de dados pessoais deve ser interpretado. A exigência dessa postura hermenêutica é reforçada pelo fato de que as normas do ordenamento jurídico brasileiro preveem a proteção a ambos os direitos de forma concomitante em diversos diplomas normativos, como na Constituição Federal – a qual tutela a privacidade de forma implícita e alça a proteção de dados como direito fundamental explícito (art. 5º, LXXIX) , no Marco Civil da Internet – que elenca como princípios da disciplina do uso da internet no Brasil a proteção

da privacidade (art. 3º, II) e dos dados pessoais (art. 3º, III) – e, em especial, na Lei Geral de Proteção de Dados – a qual dispõe sobre o tratamento de dados pessoais (art. 1º) e tem como um dos fundamentos o respeito à privacidade (art. 2º, I).

3. DO FUNDAMENTO JURÍDICO PARA A PROTEÇÃO DOS DADOS PESSOAIS.

A definição dos limites jurídicos da proteção aos dados pessoais envolve a sua compreensão em face do conteúdo da dignidade da pessoa humana. Isso porque o Estado contemporâneo se justifica na promoção de valores humanísticos, ou seja, não se pode considerar o ser humano como um instrumento para propósitos diversos (quaisquer que sejam), mas sim, como um fim em si mesmo. (BESSA, 2011, pág. 47).

Afirmar que a proteção do conteúdo da dignidade da pessoa humana é o propósito do ordenamento jurídico não é um discurso meramente proselitista. A afirmativa revela uma mudança de desígnio, de finalidade ou de base do próprio ordenamento jurídico. Em simples palavras, o propósito do ordenamento jurídico não se limita a garantir a preservação do patrimônio das pessoas, mas sim dos aspectos existenciais do ser humano, tais como o atendimento a necessidades básicas (saúde, educação, alimentação etc.) ou pela garantia do direito de escolha, de ser, de mudar e de existir, ou seja, da tutela à personalidade de um indivíduo.

A dignidade da pessoa humana é valor nuclear, projetando-se para todo o ordenamento jurídico – o que inclui, obviamente, a orientação da análise dos direitos à privacidade e à proteção dos dados pessoais. Na correlação entre a complexidade de interesse ligados à privacidade e a tutela dinâmica dos dados pessoais, a fundamentação desses direitos não é fracionada: permanece concentrada na dignidade da pessoa humana.

A cláusula geral de tutela à dignidade associa-se à autonomia e à liberdade de uma pessoa, à possibilidade de fazer escolhas, ao respeito aos direitos da personalidade (BESSA, 2011, pág. 48). Sob a denominação de direitos da personalidade estão compreendidos os atinentes à tutela da pessoa humana, considerados essenciais à sua dignidade e integridade. Compreendem o direito ao exercício de características próprias de cada indivíduo, sejam físicas, comportamentais ou psíquicas – ou seja, aquelas que definem sua personalidade. (TEPEDINO, 1999)

Como exemplo representativo sobre a tutela ao direito de definir as características próprias de cada personalidade, tem-se o reconhecimento do direito fundamental subjetivo do transgênero à alteração de seu prenome e de sua classificação no registro civil independentemente de qualquer exigência de aparência ou procedimento cirúrgico. Trata-se de orientação pacificada pelo STF em 2018 no RE 670422/RS (repercussão geral). Para exercer tal direito, basta a manifestação de vontade do indivíduo. Tal posicionamento demonstra o

respeito aos princípios da identidade, inerente à personalidade, o que, em última análise, encontra respaldo na concretização da proteção à dignidade da pessoa humana.[24]

A partir da compreensão no sentido de que o fundamento jurídico para a proteção dos direitos da personalidade reside no princípio constitucional de tutela da dignidade da pessoa humana, previsto no art. 1º, III, da CF/1988, desdobra-se o entendimento de que os direitos da personalidade são projeções, aspectos, vertentes da dignidade da pessoa humana (BESSA, 2011).

Desse argumento se extrai a qualificação da privacidade e da proteção de dados como direitos fundamentais, direitos da personalidade e até como direitos humanos. Tratam-se de direitos inerentes pelos quais a tutela à dignidade da pessoa humana é funcionalizada, se materializa ou se projeta, o que visualmente pode ser assim demonstrado:

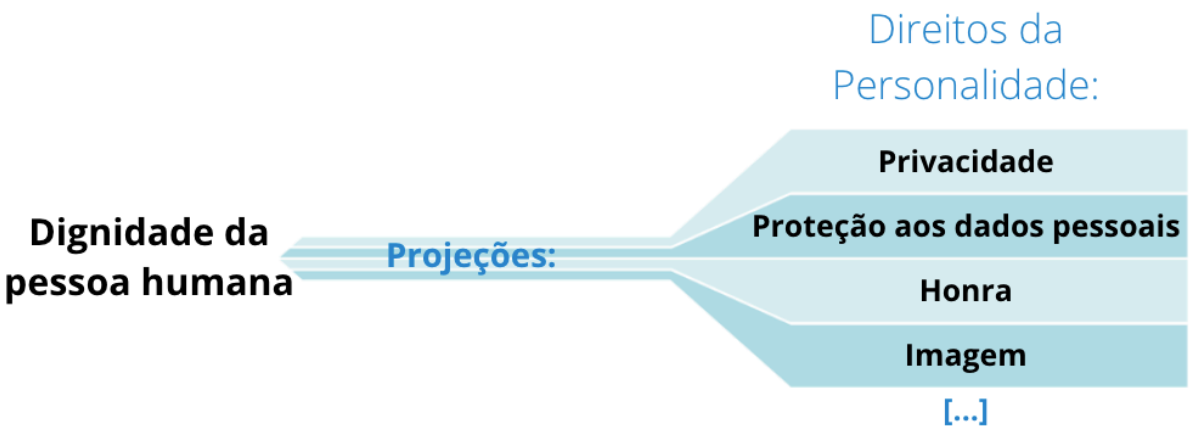

Figura 8 - Representação dos direitos da personalidade como projeções (materializações) da dignidade da pessoa humana. Elaborado pela autora.

Em continuidade a esse raciocínio, cabe demonstrar que as expressões "direitos fundamentais" (conforme empregado na Constituição Federal de 1988), "direitos humanos" (adotada pela Declaração das Nações Unidas, de 1948) e "direitos da personalidade" (nos

[24] A decisão do STF foi fundamentada nas seguintes premissas: 1) O direito à igualdade sem discriminações abrange a identidade ou a expressão de gênero; 2) A identidade de gênero é uma manifestação da própria personalidade da pessoa humana. O Estado não diz o gênero da pessoa, ele deve apenas reconhecer o gênero que a pessoa se enxerga; 3) A pessoa não deve provar o que é, e o Estado não deve condicionar a expressão da identidade a qualquer tipo de modelo, ainda que meramente procedimental. Tal entendimento flexibiliza o entendimento de imutabilidade do prenome tomado como regra, conforme definido em entendimento jurisprudencial, do STJ: "*a regra no ordenamento jurídico é a imutabilidade do prenome, um direito da personalidade que designa o indivíduo e o identifica perante a sociedade, cuja modificação revela-se possível, no entanto, nas hipóteses previstas em lei, bem como em determinados casos admitidos pela jurisprudência*." STJ. Jurisprudência em Teses, edição nº 138 - Direitos da Personalidade – II. Tese nº 5, respectivamente. Disponibilizada em 29/11/2019. Disponível em: https://processo.stj.jus.br/SCON/jt/doc.jsp?livre=%27138%27.tit. Acesso em 16/03/2023

termos utilizados em capítulo próprio no Código Civil) têm o objetivo comum de contemplar os atributos da personalidade humana sob a proteção jurídica (SCHREIBER, 2014).

Quanto aos direitos fundamentais, o contexto de sua formulação e consolidação ocorreu no período do pós II Guerra Mundial, momento no qual a relevância dada à proteção do indivíduo, para além das disposições normativas expressas, culminou na declaração de direitos que ultrapassaram uma dogmática construída para os direitos patrimoniais. Tais declarações surgiram a partir da necessidade de proteger o cidadão contra o arbítrio do Estado totalitário – para o qual a proteção conferida pelo direito público limitava-se à tutela da integridade física de garantias políticas. Os direitos fundamentais, em sua gênese, portanto, se referiam à proteção do indivíduo em face do Estado. Nota-se que, nesse momento, não existia nas relações de direito privado um sistema de proteção fora dos limites dos tipos penais (TEPEDINO, 1999).

No contexto do surgimento da categoria dos direitos subjetivos privados, os direitos humanos são, em princípio, os mesmos da personalidade. Direitos humanos referem-se aos direitos essenciais do indivíduo em relação ao direito público, voltados ao propósito de protegê-los em um plano internacional contra arbitrariedades do Estado – independentemente deste disciplinar ou não matéria. Direitos da personalidade, por sua vez, são os mesmos direitos, porém sob o ângulo privado, nas relações entre particulares, ou seja, situações nas quais o propósito é defendê-los de atentados perpetrados por outras pessoas. (TEPEDINO, 1999)

Para Anderson Schreiber (2014, p. 13), as diferentes designações para contemplar a proteção jurídica aos atributos da personalidade humana referem-se tão somente à mudança de plano no qual tais expressões são empregadas:

> Assim, a expressão direitos humanos é mais utilizada no plano internacional, independentemente, portanto, do modo como cada Estado nacional regula a matéria. Direitos fundamentais, por sua vez, é o termo normal- mente empregado para designar "direitos positivados numa constituição de um determinado Estado". É, por isso mesmo, a terminologia que tem sido preferida para tratar da proteção da pessoa humana no campo do direito publico, em face da atuação do poder estatal. Já a expressão direitos da personalidade é empregada na alusão aos atributos humanos que exigem especial proteção no campo das relações privadas, ou seja, na interação entre particulares, sem embargo de encontrarem também fundamento constitucional e proteção nos planos nacional e internacional.

Todo o raciocínio exposto sustenta a tese de que a perspectiva constitucional dos direitos da personalidade, guiada pelo fundamento da dignidade da pessoa humana (art. 1º, III, CF/1988), orienta a proteção da privacidade e dos dados pessoais como a garantia ao livre desenvolvimento de sua personalidade. Esse objetivo é reforçado pela própria Lei Geral de

Proteção de Dados, a qual elenca, em seu art. 1º, que a disciplina do tratamento de dados pessoais tem por objetivo não apenas os direitos fundamentais de liberdade e de privacidade, mas também a garantia do livre desenvolvimento da personalidade da pessoa natural.

A noção de proteger o livre desenvolvimento da personalidade por meio da proteção aos dados pessoais revela o objetivo elementar que deve guiar a adequação da normatividade da LGPD às exigências contextuais da coletividade contemporânea. Na sociedade da informação, as pessoas são reconhecidas pela representação de sua personalidade formada a partir de seus dados pessoais, o que ressalta a importância de sua tutela para garantir a proteção da identidade e personalidade de cada indivíduo.

Nesse sentido, o conteúdo da proteção dos dados pessoais, pautada como projeção da dignidade da pessoa humana, abrange o direito ao sigilo; o direito de controlar o fluxo dos dados; o poder de influenciar como sua personalidade é representada perante a coletividade e, também, de que modo sua identidade é ou será moldada pelo tratamento de seus dados pessoais.

Em outras palavras, garante-se o direito à tranquilidade, ao sigilo (ser deixado só); o poder de controle sobre as informações pessoais (aspecto positivo da privacidade e proteção de dados) e sobre a forma como a representação de sua personalidade será formada e retratada perante a sociedade (em uma expressão da autodeterminação informativa).

3.1 Proteção de dados pessoais como direito fundamental.

O valor central da proteção da dignidade do indivíduo pelo ordenamento jurídico orienta a compreensão de que as disposições normativas elencadas em diplomas próprios não são taxativas. Os direitos fundamentais não precisam estar expressos no texto constitucional para o reconhecimento de sua existência, exercício ou tutela.

A teor do §2º, do art. 5º, da Constituição Federal[25], a ordem jurídico-constitucional brasileira abrange direitos fundamentais sediados fora do título próprio (ou seja, em outras partes do texto constitucional bem como em tratados internacionais ratificados) e também os não expressamente positivados, na condição de direitos implícitos, conquanto deduzidos dos princípios ou preceitos fundamentais.[26]

[25] O dispositivo aduz que "*os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte*."

[26] Acerca do reconhecimento do direito à proteção de dados e à autodeterminação informativa como direitos fundamentais implícitos, Ingo Wolfgang Sarlet afirma que "*para uma compreensão constitucionalmente adequada, é preciso recordar que a inter-relação entre o direito internacional dos direitos humanos (e um direito*

Na Constituição Federal, não há uma previsão expressa que alça a privacidade como direito fundamental e, até a promulgação da EC 115/2022, também não a havia para a proteção de dados pessoais. Seus conteúdos foram extraídos a partir da leitura dos incisos X e XII, do art. 5º, da Carta Maior, os quais expressam, respectivamente que "*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*" e que "*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*". Tais previsões expressam a concepção tradicional do direito à privacidade, tomada um direito ao sigilo.

A subsunção da privacidade à função negativa de um direito fundamental refletiu na limitação do reconhecimento da proteção constitucional do sigilo (art. 5º, XII) ao conteúdo das comunicações. Esse entendimento orientou posições jurisprudenciais, como no julgamento do Recurso Extraordinário (RE) nº 418.416-8/SC, em 2006 (DJ 19.12.2006). Nesse julgado, foi estabelecida a diferença entre a interceptação das comunicações e a apreensão da base física na qual se encontravam os dados. No último caso, não foi reconhecida a violação ao preceito fundamental uma vez que não teria ocorrido quebra do sigilo das comunicações (ou seja, uma intercepção das comunicações), mas mera apreensão do aparato físico no qual se encontravam os dados. Esse raciocínio toma a privacidade como escudo contra o exterior em uma lógica de exclusão, de tudo ou nada.

A reconceptualização do direito à privacidade coincidiu com o desenvolvimento jurisdicional do conceito de autodeterminação informacional, cujo marco paradigmático é atribuído à decisão tomada pelo Tribunal Constitucional Alemão em 1983 – *Volkszählungsurteil* (BVerfGE 65, 1). No caso, a Corte Constitucional Alemã declarou a inconstitucionalidade da denominada Lei do Censo alemã, a qual possibilitava que o Estado realizasse o tratamento cruzado de informações sobre os cidadãos para mensuração estatística da distribuição espacial e geográfica da população pelos endereços, tipos de profissões e locais de trabalho.

No julgado, o Tribunal Alemão situou a proteção de dados pessoais como projeção de um direito geral de personalidade para além de uma proteção ao sigilo, mas como um direito de poder decidir sobre a divulgação e o uso de seus dados pessoais; sobre os limites de sua vida

---

humano à proteção dos dados pessoais) e a ordem jurídico-constitucional doméstica brasileira guarda uma conexão com o problema da assim chamada expansividade (não taxatividade e exaustividade) do catálogo constitucional dos direitos fundamentais". (SARLET. 2021, p. 27).

pessoal que podem ser revelados e sobre o direito a tomar conhecimento sobre quem sabe e o quanto sabe sobre as informações que lhes digam respeito. A Corte Constitucional Alemã compreendeu que o processamento automatizado dos dados, ainda que para os propósitos legítimos (como desenvolvimento de estatísticas úteis ao desenho de políticas públicas), colocaria em risco o poder do indivíduo em decidir por si mesmo sobre como ele deseja fornecer seus dados pessoais a terceiros.

Os riscos reconhecidos pelo Tribunal referem-se à possibilidade de que as informações fornecidas a respeito das profissões, moradias e locais de trabalho poderiam ser processadas por meio de sistemas automatizados a ponto de habilitar a formação de um perfil completo da personalidade dos cidadãos. A abordagem revelou-se paradigmática por não ter se pautado em uma dicotomia entre o que é considerado público e excluir o que for classificado como privado, mas sim em uma análise atenta aos múltiplos contextos de uso nos quais os dados podem ser processados e os riscos que deles podem advir.

A exemplo da paradigmática decisão tomada pelo Tribunal Constitucional Alemão, em 1983, o Supremo Tribunal Federal chancelou, no julgamento das ADIs nº 6.387, 6.388, 6.389, 6.390 e 6.393, a autonomia do direito fundamental à autodeterminação informativa, à privacidade e da proteção de dados pessoais. Posteriormente, em fevereiro de 2022, a Emenda Constitucional nº 115, de 2022, incluiu a tutela de dados pessoais no rol de direitos fundamentais do art. 5º (inciso LXXIX), tornando expresso tal direito fundamental que, até então, era reconhecido de forma implícita a partir dos incisos X e XII do mesmo dispositivo.

Alçar a privacidade como um direito constitucional autônomo, ainda que implícito, importou no reconhecimento de que a proteção às informações pessoais não se restringe ao momento de sua comunicação (art. 5º, XII, CF/1988) ou da intimidade (art. 5º, X, CF/1988).

A perspectiva constitucional dos direitos da personalidade (art. 1º, III, CF/1988) volta-se à proteção da privacidade como a garantia ao livre desenvolvimento da pessoa humana – o que em muito é associada a uma prevenção de riscos de uma atividade. Em outras palavras, a análise é pautada pela identificação das potenciais ofensas e perigos de um processamento de informações que possam influir na autonomia de um indivíduo.

Nota-se que essa perspectiva ultrapassa a consideração da privacidade apenas como um direito ao sigilo, no qual impera a lógica dicotômica que diferencia o público do privado, tutelando a exclusão do conhecimento externo de informações privadas e desconhecendo de ofensas para os casos que envolvam o emprego de informações públicas ou tornadas públicas. Para além do sigilo comunicacional, o STF reconheceu que a disciplina jurídica do

processamento de informações afeta o sistema de proteção de garantias individuais como um todo.

A tutela à formação da própria personalidade não se dá apenas em um contexto no qual o indivíduo é autossuficiente, centralizado e isolado, mas em um ambiente relacional, necessariamente social e cultural. O ambiente no qual o sujeito se insere deve ser considerado de modo que o desenvolvimento de seus valores – individuais ou culturais – não ocorram com travas. É preciso garantir que as pessoas possam navegar por espaços sociais, de modo que a privacidade não seja tomada como uma negação à participação social, mas como uma das condições para que esta ocorra. Pela perspectiva interpretativa de proteção ao direito de autodeterminação, a proteção do direito fundamental à proteção de dados pessoais recai não na classificação de uma dimensão privada ou não do dado (ou seja, na publicidade ou sigilo do dado), mas nos *riscos* atribuídos ao seu tratamento por terceiros.

Adentra nessa fórmula a preocupação com decisões automatizadas por meio da utilização do Big Data, cujo processamento não gera saídas (*outputs*) necessariamente mais "justas" ou "mais corretas". A precisão e correção de uma decisão tomada de forma automatizada depende da precisão do algoritmo que orienta o processamento dos dados e, no mesmo nível de importância, da qualidade dos dados tomados como entrada (*input*). A tutela da pessoa humana, por essa perspectiva, não considera a natureza privada ou pública do dado. Visa, em realidade, garantir o poder participar ou tomar medidas que garantam sua participação na tomada de decisões que influenciam a sua forma de relacionar com o mundo externo.

Tanto a privacidade quanto a proteção de dados são reconhecidas como direitos fundamentais, expressão de direitos da personalidade e concebidas como projeções da dignidade da pessoa humana.

Há consequências práticas da caracterização de tais direitos como fundamentais – que independem de sua previsão expressa (como a proteção de dados pessoais, explícita no art. 5º, LXXIX) ou implícita (caso do direito à privacidade). Ambos são alçados à categoria de cláusulas pétreas (art. 60, §4º, da CF/1988), o que os tornam insuscetíveis de se tornarem objeto de deliberação de propostas tendentes a aboli-los. Ademais, garante-se a proibição do retrocesso e, em caso de violação, abre-se a possibilidade para o reconhecimento de um dever de compensação (a título de danos morais). Outrossim, não são direitos absolutos, pois admitem mitigação, desde que respeitados os respectivos núcleos essenciais.

Por outro lado, o reconhecimento inicial da tutela de dados pessoais como direito fundamental implícito (na ADI 6.387) não retira a importância de sua previsão expressa no rol de direitos fundamentais previstos na Constituição Federal. A Emenda Constitucional nº 115,

de 2022 conferiu a condição de norma de eficácia limitada ao tema – dependente, portanto, de regulação normativa infraconstitucional para poder exercer todos os seus efeitos.

Ademais, foi definida a competência exclusiva da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais (art. 21, XXVI, da CF/1988) bem como a sua competência privativa para legislar sobre a proteção e tratamento de dados pessoais. Tais previsões reforçam o caráter nacional da Lei 13.709/2018 (LGPD), ou seja, o dever de sua observância não apenas no nível federal, mas também estadual e municipal – e retira a possibilidade de os Estados ou Municípios legislarem sobre o tema[27].

O diferencial de qualificar a proteção de dados pessoais como direito fundamental expresso na Constituição Federal demonstra que há maior segurança jurídica quanto ao conteúdo normativo da proteção de dados pessoais, especialmente quando se consideram as dinâmicas político-institucionais voltadas a sua concretização. Saber as "regras do jogo" por meio de uma lei nacional e formar balizas de previsibilidade para decisões judiciais são essenciais especialmente para a convergência regulatória no caso do fluxo internacional de dados ou para fomentar o mercado a adotar iniciativas e negócios que operacionalizem o devido tratamento de dados pessoais.

Ademais, a previsão expressa dos dados pessoais como direito fundamental mitiga possíveis brechas legais que possibilitem a violação de direitos inerentes à dignidade e existência da pessoa humana. Há grande relevância quanto a esse aspecto, especialmente quando se considera o fato de que as leis e regulamentos não possuem a capacidade de acompanhar a velocidade das mudanças disruptivas decorrentes do implemento de novas tecnologias.

É o caso da Inteligência Artificial. Independentemente de leis específicas, seu emprego deve respeitar o livre desenvolvimento da personalidade das pessoas. Em síntese, a previsão expressa da proteção de dados como direito fundamental reforça a obrigação do Poder Judiciário em garantir que o progresso da ciência não crie condições para a violação da

[27] Cabe ressaltar, por outro lado, que há decisões do STF que reconhecem a constitucionalidade de leis estaduais que tangenciam a disciplina do tema dos dados pessoais. É o exemplo do caso em que lei estadual, considerada constitucional pela Corte Suprema, determinou que prestadoras de serviço telefônico são obrigadas a fornecer, sob pena de multa, os dados pessoais dos usuários de terminais utilizados para passar trotes aos serviços de emergência. STF. Plenário. ADI 4924/DF, Rel. Min. Gilmar Mendes, julgado em 4/11/2021 (Info 1036). Por outro lado, o Supremo Tribunal Federal considera que o interesse público na prestação de serviços de tecnologia da informação a órgãos como a Secretaria do Tesouro Nacional e a Secretaria da Receita Federal (integrantes da estrutura do Ministério da Economia), sejam prestados com exclusividade por empresa pública federal criada para esse fim, como é o caso da Serpro. STF. Plenário. ADI 4829/DF, Rel. Min. Rosa Weber, julgado em 20/3/2021 (Info 1010). As decisões não são conflitantes ou antagônicas, mas sua análise demonstra que não é possível, a priori, determinar os limites ou o grau de relevância que será dado caso a caso para verificar a constitucionalidade da atuação legislativa dos entes políticos estaduais ou mesmo municipais.

Constituição (DONEDA, 2023), independentemente de modificações disruptivas nos contextos sociais.

3.2 Proteção de dados pessoais como direito da personalidade.

Para a doutrina brasileira especializada (TEPEDINO, 1999), os direitos da personalidade possuem como características a originalidade, a extrapatrimonialidade, o caráter absoluto, a inalienabilidade, a imprescritibilidade e a intransmissibilidade. A originalidade (também conhecida como generalidade) indica que são inerentes ao ser humano, ou seja, sua aquisição independe da capacidade civil ou da vontade do indivíduo: são concedidos a todos pelo só fato de *ser*, de estar vivo.

São extrapatrimoniais pois não podem mensurados em valores monetários – o que não impede que sua lesão gere reflexos econômicos (como a compensação financeira por sua violação). São absolutos no sentido de serem oponíveis *erga omnes*, impondo-se o dever de respeitá-los não apenas pelo Estado[28] mas por toda a coletividade – o que, cabe ressaltar, não se confunde com a impossibilidade de sofrerem conformações ou mitigações em casos práticos.

São indisponíveis pois seu exercício não pode sofrer limitações voluntárias (art. 11, do Código Civil), o que também os torna irrenunciáveis e impenhoráveis. A imprescritibilidade impede que a lesão a um direito convalesça com o passar do tempo – como uma decorrência ao perecimento da pretensão ressarcitória. São, por fim, intransmissíveis e irrenunciáveis (art. 11, do Código Civil), de modo que seu titular não pode transferi-los ou delegá-los.

Cabe notar que, a despeito das características inerentes aos direitos da personalidade (em especial a indisponibilidade), tais direitos não são absolutos. Seu exercício admite limitações. A título de exemplo, a inviolabilidade da vida privada da pessoa natural (tutelada pelo mencionado art. 21, do Código Civil) foi mitigada na ADIN 4815, a qual dispensou a

[28] Conforme enuncia Gustavo Tepedino (1999, p. 14), "a concepção dos direitos da personalidade teve sua gênese ligada, inicialmente, às teorias jusnaturalistas, como forma de proteção do homem contra o arbítrio do totalitarismo, e, de forma geral, do poder público. Daí a concepção desses direitos como direitos inatos, invulneráveis, portanto, ao arbítrio do Estado-legislador." Cabe apontar, no entanto, que o autor critica a concepção jusnaturalista como fonte dos direitos da personalidade. Isso porque as circunstâncias ou razões metajurídicas de criação de um direito do homem não autoriza a construção de uma categoria de direitos impostos à sociedade de forma independente de sua própria formação cultural, social e política. Ao citar a lição de Adriano de Cupis, Gustavo Tepedino defende que a suscetibilidade de ser titular de direitos da personalidade é tão vinculada ao ordenamento jurídico quanto os demais direitos e obrigações. Em outras palavras, qualquer situação jurídica só pode nascer do dado positivo, ou seja, de uma lei. Nesses termos, cabe sua citação (1999, p. 17): "No Estado de Direito, a ordem jurídica serve exatamente para evitar os abusos cometidos por quem, com base em valores supralegislativos, ainda que em nome de interesses aparentemente humanistas, viesse a violar garantias individuais e sociais estabelecidas, através da representação popular, pelo direito positivo."

necessidade de autorização prévia para a edição de biografias em vista da preponderância do direito à informação e à liberdade de expressão em relação a uma noção de privacidade do indivíduo, conforme se extrai da leitura de trechos da ementa:

> 2. O objeto da presente ação restringe-se à interpretação dos arts. 20 e 21 do Código Civil relativas à divulgação de escritos, à transmissão da palavra, à produção, publicação, exposição ou utilização da imagem de pessoa biografada.
> 3. A Constituição do Brasil proíbe qualquer censura. O exercício do direito à liberdade de expressão não pode ser cerceada pelo Estado ou por particular.
> 4. O direito de informação, constitucionalmente garantido, contém a liberdade de informar, de se informar e de ser informado. O primeiro refere-se à formação da opinião pública, considerado cada qual dos cidadãos que pode receber livremente dados sobre assuntos de interesse da coletividade e sobre as pessoas cujas ações, público-estatais ou público-sociais, interferem em sua esfera do acervo do direito de saber, de aprender sobre temas relacionados a suas legítimas cogitações.
> 5. Biografia é história. A vida não se desenvolve apenas a partir da soleira da porta de casa.
> 6. Autorização prévia para biografia constitui censura prévia particular. O recolhimento de obras é censura judicial, a substituir a administrativa. O risco é próprio do viver. Erros corrigem-se segundo o direito, não se coartando liberdades conquistadas. A reparação de danos e o direito de resposta devem ser exercidos nos termos da lei.
> 7. A liberdade é constitucionalmente garantida, não se podendo anular por outra norma constitucional (inc. IV do art. 60), menos ainda por norma de hierarquia inferior (lei civil), ainda que sob o argumento de se estar a resguardar e proteger outro direito constitucionalmente assegurado, qual seja, o da inviolabilidade do direito à intimidade, à privacidade, à honra e à imagem.
> 8. Para a coexistência das normas constitucionais dos incs. IV, IX e X do art. 5º, há de se acolher o balanceamento de direitos, conjugando-se o direito às liberdades com a inviolabilidade da intimidade, da privacidade, da honra e da imagem da pessoa biografada e daqueles que pretendem elaborar as biografias. STF - ADI nº 4.815/DF, Relator: Min. Carmem Lúcia, Data de Julgamento: 10/06/2015.

As primeiras tratativas adotadas para transformar a pessoa como um referencial normativo de valor para além de uma concepção instrumental acompanhou o desenvolvimento, no direito privado, da categoria dos direitos da personalidade (DONEDA, 2021). Nesses primeiros momentos, a multiplicação de direitos subjetivos referentes a aspectos da personalidade fomentaram diversas tentativas de sistematizar um inventário sobre quais seriam os direitos da personalidade previstos pelo ordenamento. A insuficiência de uma manifestação mecânica desse formalismo é revelada pela fato de que o respeito e a tutela da pessoa humana não podem ser fracionados sem afrontar o seu valor em si.

No momento em que se reconhece a vinculação do ordenamento jurídico ao valor máximo de tutela à pessoa humana, a denominação de direitos da personalidade previstos em

capítulo próprio do Código Civil não deve ser lida de forma a excluir outras hipóteses ali não previstas.[29] Ao intérprete não incumbe descrever a estrutura de um direito da personalidade de modo circunscrito a um diploma normativo, mas sim desenvolver os parâmetros pelos quais cada expressão da personalidade se projeta a partir de seu valor unitário. Nesse cenário, ao mesmo tempo em que se observa "*o franco esvaziamento das possibilidades do Código Civil de enunciar propriamente direitos subjetivos, por outro ganham importância ao fornecer critérios para a ponderação e a interpretação*." (DONEDA, 2021, pág. 99)

Aberta a possibilidade de enunciação de direitos da personalidade fora do capítulo próprio do Código Civil, a centralidade do ser humano como valor em si também incentivou a elaboração de regimes normativos específicos para as diversas situações nas quais se fez presente a necessidade de promover a proteção da pessoa. "*Esse é, aliás, um aparente paradoxo com o qual nos deparamos: a unidade do ordenamento e do valor da pessoa humana coexiste com uma multiplicação sem precedentes dos campos nos quais é realizada sua tutela*." (DONEDA, 2021, pág. 99). É o caso dos desdobramentos da tutela da pessoa pela sua qualidade de consumidor (pelo CDC), de titular de dados (pela LGPD) e por outras normativas setorizadas que operacionalizam a tutela de aspectos da personalidade de um indivíduo.

A par da unidade da personalidade, o sujeito não pode ser tomado de forma fragmentada, como diversas faces frente às suas necessidades e garantias sob o pretexto de funcionalizar o sistema jurídico. Nesse contexto, o consumidor, o titular de dados, o cadastrado em um banco de dados (segundo a Lei do Cadastro Positivo), o usuário da Internet (Marco Civil da Internet) e qualquer outra face atribuída à pessoa devem ser unificados pelo valor que pretendem assegurar: a dignidade do indivíduo como um valor em si.

Nesse sentido, a perspectiva de tutela dos dados pessoais deve ser tomada como manifestação de um valor unitário (a dignidade da pessoa humana), ainda que funcionalizado por diversos diplomas normativos, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei 14.414/2011), o Marco Civil da Internet e, com especial destaque, para a Lei Geral de Proteção de Dados.

O Código de Defesa de Consumidor conferiu proteção aos dados pessoais de forma expressa, ainda que não de modo amplo, ao regular a atividade dos bancos de dados e de cadastros de consumidores (arts. 43 e 44). A Lei do Cadastro Positivo (Lei 14.414/2011)

[29] IV Jornada de Direito Civil. Enunciado nº 274: "Os direitos da personalidade, regulados de maneira não-exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1º, inc. III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação."

complementa a normatização do processamento de dados para formação de histórico de crédito sem, no entanto, prever de forma expressa a proteção da privacidade.

O Marco Civil da Internet (Lei 12.965/2014) prevê a proteção da privacidade e dos dados pessoais como princípios da disciplina do uso da internet no Brasil (art. 3º, II e III, do MCI). A normativa regula a prestação de serviços de aplicação de internet em território nacional – notadamente, os serviços de provedores de internet. Trata-se, também, de uma tutela da privacidade diante do emprego de dados pessoais em um contexto específico.

A Lei Geral de Proteção de Dados, Lei 13.709/2018, atende à exigência de lei para assegurar a proteção de dados pessoais (conforme determina o art. 5º, LXXIX, da CF/1988). A inovação e relevância do documento legal se volta a unificar a regulamentação normativa do tratamento de dados pessoais que, até então, era tutelado de modo implícito (pela Constituição Federal e pelo Código Civil) ou de forma setorizada – como pelo CDC, quanto aos banco de dados; pela Lei de Cadastro Positivo, quando à formação de histórico de crédito; e pelo MCI – quanto aos serviços de provedores de internet.

A rigor, previsões normativas dispersas e casuísticas, não logram uma proteção capaz de tutelar as irradiações da personalidade em todas suas possíveis manifestações (TEPEDINO, 1999). Esse fato, no entanto, não prejudica a tutela aos direitos existenciais da pessoa humana, especialmente quando se considera a cláusula geral de proteção à sua dignidade humana, conforme previsto no art. 1º, III, da Constituição Federal.[30] Esse argumento favorece a compreensão de que a evolução dinâmica dos fatos sociais dispensa uma concomitante e correspondente disciplina legislativa para todas as possíveis situações jurídicas de que a pessoa humana figure como titular. Esse ponto é relevante para a análise de casos que envolvam a utilização de tecnologias disruptivas, como aplicações de software com processamento autônomo.

[30] Gustavo Tepedino conceitua o art. 1º, III, da CF/1988 como cláusula geral de tutela da personalidade. (TEPEDINO, 1999).

4. DIÁLOGO DAS FONTES E TUTELA DOS DADOS PESSOAIS

As implicações decorrentes de uma violação de direitos ou descumprimento de deveres em um tratamento de dados pessoais depende do panorama normativo que recai sobre as relações jurídicas formadas em seu contexto. O tratamento de dados pessoais pode ocorrer em meio a relações de consumo, trabalhistas, empresariais ou públicas, por exemplo. Pode envolver partes em igualdades de condições (a exemplo dos contratos cíveis em geral) ou em situações de assimetrias de poder (como entre o cidadão e o Poder Público). Pode tangenciar temas afetos a legislações específicas, como o Marco Civil da Internet, ou atrair a ponderação de conceitos de legislações "gerais" (como a parametrização da indenização de acordo com a disciplina do Código Civil – arts. 944 e seguintes).

A definição das normativas incidentes nesses casos não é realizada pela lógica da exclusão adotada pelas técnicas de interpretação tradicionais. A própria LGPD, em seu art. 64, chancela a aplicação convergente de diferentes diplomas normativos em diálogo de suas disposições. Quanto à disciplina da responsabilidade civil, o art. 45 (LGPD) é claro ao sujeitar as violações do direito do titular de dados no âmbito de relações de consumo às regras previstas na legislação pertinente. Esses dispositivos revelam a adoção da interpretação sistemática segundo a técnica do diálogo das fontes – ao que Cláudia Lima Marques e Bruno Miragem denominaram como "simbiose protetiva" do titular de dados pessoais (2023, pág. 796 e 799).

Além do respaldo legal e doutrinário, a aplicação do diálogo das fontes no contexto de um tratamento de dados pessoais também é chancelada pela jurisprudência. Em 2023, a Primeira Turma Recursal (Juizado Especial Cível) do Tribunal de Justiça do Distrito Federal (TJDFT) reconheceu a aplicação, em diálogo das fontes, do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados para constatar falha no serviço e descumprimento do dever de segurança por um provedor de rede social. O tema envolveu um caso de estelionato digital/cibernético, no qual uma pessoa teve seu perfil de Instagram hackeado por terceiros – que se utilizaram de sua credibilidade e imagem para perpetrar golpes de vendas falsas por seu perfil. Os trechos da ementa revelam o reconhecimento da relação de consumo e da incidência concomitante da disciplina da LGPD:

> 2. Incontroverso que a Recorrida teve seu perfil do Instagram hackeado por terceiros, que passaram a perpetrar golpes de vendas falsas pelo seu perfil, utilizando-se de sua credibilidade e imagem para auferir renda ilegal; incontroverso, também, que o Recorrente não enviou o e-mail para que a Recorrida possa recuperar a conta.

> 3. Legislação aplicável. **Em harmônico diálogo das fontes, com fulcro no art. 45 da Lei Geral de Proteção de Dados - LGPD, aplica-se ao caso o CDC e a LGPD,** concluindo-se ser, essa, relação consumerista e, o caso, de clara falha na prestação do dever de segurança que recai sobre o provedor de rede social, nos termos do art. 6º, incisos VII e VIII, 42, caput, e 44, incisos I, II e II e parágrafo único, todos da LGPD c/c art. 14, caput, e §§, do CDC.
> 4. Falha no dever de segurança dos dados. **Na condição de agente de tratamento de dados, o Recorrente é responsável por cuidar dos dados por ele** controlados, observando a boa-fé e os princípios da segurança e da prevenção, com a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. O tratamento de dados pessoais será irregular quando não fornecer a segurança que dele se pode esperar, respondendo, o controlador ou operador dos dados, pelos danos decorrentes de sua violação, ao deixar de adotar as medidas de segurança indicadas e necessárias.
> 5. Da responsabilidade pelo dano. O estelionato cibernético é aquele realizado por terceiros que invadem o banco de dados de grandes provedores e utilizam os dados obtidos para realizar obter dinheiro ilegalmente dos contatos e seguidores da pessoa titular do perfil violado. **Uma vez que o Recorrente é quem detém os dados e realiza o seu tratamento sem cuidar da segurança esperada, deve responder objetivamente pelos danos que sobrevierem a partir da violação**. Esse tipo de fraude é evento ligado à organização do negócio explorado - Teoria do Risco da Atividade - razão pela qual deve indenizar os prejuízos causados ao usuário, dado que compreende caso de fortuito interno. [...]
> (TJ-DF 07094063920228070009 1658370, Relator: Rita de Cássia de Cerqueira Lima Rocha, Data de Julgamento: 27/01/2023, Primeira Turma Recursal, Data de Publicação: 14/02/2023) – grifos da autora.

O diálogo das fontes representa a interpretação e análise conjunta de diplomas legais diversos incidentes sobre o mesmo suporte fático, em uma postura hermenêutica que propõe a conciliação e não a revogação de dispositivos. Trata-se de um imperativo no âmbito das relações jurídicas formadas no contexto de um tratamento de dados pessoais. O termo "Geral", portanto, constante da denominação Lei Geral de Proteção de Dados Pessoais (LGPD), se refere à abrangência de sua incidência: situações que envolvam o tratamento de dados pessoais para os mais diversos propósitos. Não se trata de uma adjetivação da lei como antagônica ou contraposta às normas especiais ou gerais.

A aplicação do diálogo das fontes revela a adoção de uma postura hermenêutica que propõe a conciliação de diplomas normativos incidentes sobre o mesmo suporte fático – como o CDC, LCP e MCI. Dessa "simbiose protetiva" é possível estabelecer as seguintes conclusões[31]:

[31] Tais conclusões são extraídas e inspiradas a partir das propostas por Leonardo Bessa (2022, pág. 322) acerca do exame simultâneo do CDC e da Lei do Cadastro Positivo (Lei nº 12.414/2011): "1) a Lei 12.414/2011 não revoga qualquer dispositivo do Código de Defesa do Consumidor; 2) os princípios (boa-fé objetiva, transparência,

1. A Lei 13.7089/2018 não revoga dispositivos do Código de Defesa do Consumidor, da Lei de Cadastro Positivo ou do Marco Civil da Internet;
2. Os princípios da LGPD (finalidade, adequação, necessidade, livre acesso transparência, entre outros), bem como seus conceitos legais (titular, dados pessoais, operador, controlador, tratamento, entre outros) devem ser considerados e aproveitados na interpretação do Código de Defesa do Consumidor, da Lei de Cadastro Positivos e do Marco Civil da Internet;
3. Eventual omissão ou lacuna de uma normativa deve ser suprida pela outra;
4. Eventual conflito de disposições entre os diplomas normativos deve ser resolvido mediante a técnica da proporcionalidade, de acordo com as peculiaridades das circunstâncias fáticas, à luz da Constituição federal, prevalecendo, no caso concreto, a disposição ou interpretação que mais densifica os valores ou princípios constitucionais bem como atende ao equilíbrio de propósitos da LGPD em garantir o livre desenvolvimento da personalidade da pessoa natural e o desenvolvimento econômico e tecnológico e a inovação.

A Lei Geral de Proteção de Dados de fato concentra, em grande medida, a tutela normativa dos dados pessoais. Por outro lado, cabe considerar que a efetivação do direito fundamental à tutela de dados pessoais implica a consideração de disposições que não se limitam às previstas na LGPD. O rol de direitos assegurados ao titular de dados, nesse sentido, ultrapassa as disposições da normativa, tanto pela perspectiva da tutela constitucional ao direito fundamental da dignidade da pessoa humana e de suas projeções, bem como pela análise integrada, em diálogo das fontes, conforme amparado pela doutrina, pela jurisprudência e pela própria LGPD.

Considerando-se a representatividade das disposições do Código de Defesa do Consumidor, da Lei do Cadastro Positivo (LCP – Lei nº 12.414/2011) e do Marco Civil da Internet para a tutela normativa de dados pessoais, a análise da responsabilidade civil por violações aos dados pessoais passa pela consideração dos direitos, deveres e institutos regulados por esses diplomas.

proteção à dignidade do consumidor, entre outros) do CDC, bem como seus conceitos legais e doutrinários (consumidor, fornecedor, banco de dados e cadastro de consumo), devem ser considerados e aproveitados na interpretação da Lei 12.414/2011; 3) eventual omissão (lacuna) de uma norma deve ser suprida pela outra; 4) eventual conflito entre os diplomas deve ser resolvido, com a técnica da proporcionalidade, sob as luzes da Constituição Federal, prevalecendo, no caso concreto, a norma que mais densifica princípio ou valor constitucional.".

4.1 Do tratamento de dados segundo o Código de Defesa do Consumidor e a Lei nº 12.414/2011.

4.1.1 Das entidades de proteção ao crédito e o *credict score*.

A atenção normativa à proteção de dados pessoais nos moldes contemporâneos foi antecedida pela preocupação que motivou disciplina dos bancos de dados e dos cadastros de consumo pelo Código de Defesa do Consumidor. O motivo dessa regulamentação coincide com preocupações atuais, pois também se refere ao reconhecimento do potencial ofensivo da utilização de informações em face aos direitos da personalidade do consumidor, como privacidade, dados pessoais e honra.

De início, cabe notar que não há um rigor normativo que observe uma distinção terminológica entre *banco de dados* e *cadastros de consumo*. Tais categorias são essencialmente diferenciadas a partir de dois critérios estabelecidos por Herman Benjamin. De um lado, considera-se a *origem* da informação (a fonte dos dados) e, de outro, o *destino* de sua aplicação. Tais critérios são assim sintetizados (BESSA, 2022, pág. 318):

> Nos cadastros é o próprio consumidor que, independentemente de parcelamento do produto adquirido, oferece seus dados para o estabelecimento físico ou virtual, os quais serão utilizados para estreitar a relação com o consumidor. A fonte da informação é o próprio consumidor e o destino é um fornecedor específico.
> De outro lado, os bancos de dados de consumo, cuja principal espécies são justamente as entidades de proteção de crédito, a informação advém, em regra, dos estabelecimentos comerciais. O destino final da informação, embora ela permaneça armazenada na entidade, é o mercado, ou seja, os fornecedores.

O cadastro de consumo caracteriza-se como aquele que o consumidor realiza no ato de uma compra em uma loja de roupas, por exemplo, momento no qual o consumidor/cliente dispõe de informações que poderão ser utilizadas pelo fornecedor para informar novidades, reestoque de produtos, divulgação de ofertas ou promoções exclusivas, como descontos em aniversários. As informações do consumidor são comumente utilizadas para o envio desses conteúdos por e-mail ou mensagens instantâneas (como pelo WhatsApp) em um contato comumente direto entre o cliente o fornecedor. O propósito do cadastro de consumo é estreitar a relação entre o consumidor e fornecedor.

Os bancos de dados, por outro lado, são queles que processam informações importantes para a dinamicidade econômica do mercado de consumo. Diferenciam-se do cadastro de consumo pois não se voltam para o atendimento imediato do consumidor ou para o estreitamento destes laços com o fornecedor. Os bancos de dados são aqueles empregados por entidades para atingir os mais diversos propósitos, tais como a obtenção de informações para formar relatórios estatísticos de comportamento de mercado, para formação de históricos de um consumidor como medida para proteção de crédito ou avaliação de seguros por companhias seguradoras. Dentre os diversos bancos de dados que atendem ao mercado, aqueles formados pelas entidades de proteção ao crédito ganham maior visibilidade pois possuem o maior potencial decisivo sobre a condução da vida do consumidor: se este será ou não excluído do mercado de consumo de acordo com o resultado da sua avaliação ao acesso de crédito.

Sobre a importância da função social e econômica do crédito, "*não há dúvidas de que o aumento do volume de crédito responsável é auspicioso para a economia e dinâmica do mercado. Apresenta benefícios ao consumidor, particularmente o de baixa renda que, em regra, não tem condições financeiras de adquirir bens essenciais (geladeira, fogão, eletrodomésticos, móveis)"* sem a obtenção de empréstimo ou financiamento (BESSA, 2022, pág. 324).

Constatada a importância da análise de crédito para a saúde econômica da coletividade, o percurso histórico de formação dos bancos de dados de consumo demonstrou que o tratamento de informações para análise de risco ao crédito é mais dinâmica, racional e barata quando exercida por uma entidade criada para tal objetivo. A partir de 1960, o setor de proteção ao crédito começou a ser explorado economicamente por empresas como o Serasa Experian e o SCPC (Serviço Central de Proteção ao Crédito, pertencente à Boa Vista Serviços). Posteriormente, despontaram outras empresas atuantes no mercado de informação ao crédito, como a Quod e mecanismos de proteção pelo setor público, como o Sistema de Informações de Crédito do Banco Central (SCR).

A operação de sistemas criados para o propósito de análise de risco de concessão ao crédito enquadra a entidade que o funcionaliza como banco de dados de proteção ao crédito – o que, invariavelmente, atrai a incidência dos limites definidos não apenas pelo CDC, mas também pela Lei de Cadastro Positivo e pela Lei Geral de Proteção de Dados.

Isso porque o crédito se baseia na crença de que o mutuário irá cumprir as obrigações assumidas, o que, na sociedade contemporânea, é realizado a partir da avaliação de dados do consumidor. O regime de confiança em uma sociedade de consumo massificado e permeada por relações fugazes e automáticas de compra e venda entre relações de pessoas marcadas pelo

anonimato conduz ao reconhecimento da legitimidade da coleta de informações do consumidor para análise de risco de concessão de crédito, ou seja, para cumprir o papel de estabelecer a confiança entre o consumidor e o fornecedor concessionário do crédito.

A entidade de proteção ao crédito surge como intermediária para estabelecer a confiança nessa relação, ou seja, para estabelecer o grau de segurança ou de risco de inadimplemento do consumidor para que o próprio fornecedor avalie as condições do empréstimo (com maiores juros para fazer frente a maiores riscos, por exemplo) ou mesmo negar a concessão de crédito (em vista da ausência de confiança de que receberá, no futuro, os valores emprestados). Nesse sentido, pode-se afirmar que as entidades de proteção de crédito têm por principal objeto a "*coleta, o armazenamento e a transferência a terceiros (credores potenciais) de informações pessoais dos pretendentes à obtenção do crédito*." (BESSA, 2022, pág. 322).

Diante da crescente importância das atividades exercidas pelos bancos de dados de proteção ao crédito foi promulgada a Lei nº 12.414, em 2011, conhecida como Lei do Cadastro Positivo (LCP). Seu propósito é disciplinar o tratamento de informações utilizadas para a formação do histórico de crédito do consumidor, ao que se faz referência como o tratamento de informações positivas. Trata-se de uma nomenclatura empregada como contraposição à noção de avaliação de crédito pautada apenas pela "negativação" do nome do consumidor, ou seja, da informação restrita ao conhecimento da existência de dívidas vencidas e não pagas.

Objetivamente, acrescentou-se à matéria a possibilidade de processar informações não apenas sobre o inadimplemento do consumidor (informação negativa), mas sobre seu comportamento financeiro, como percentual do comprometimento de sua renda por empréstimos em andamento, da sua pontualidade em pagamentos e outras informações úteis à formação de seu histórico de crédito e à atribuição de uma pontuação – ao que ficou conhecido como formação de um *credit score*.

Tradicionalmente, quem realiza o juízo de valor (a avaliação para concessão ou não do crédito) é o fornecedor (credor/ consulente) que acessa as informações. No entanto, é possível que o gestor (entidade de proteção de crédito) realize a composição da nota ou pontuação de crédito para análise de risco e a disponibilize ao consulente (art. 7º-A, da LCP). Invariavelmente, essa atividade envolve a criação de perfis de consumidores "bons pagadores" – o que reforça a incidência concomitante da LGPD a essa temática.

O tratamento de dados pessoais para fins de proteção ao crédito por meio da formação do histórico de crédito do consumidor encontra amparo na autorização legal para a atividade no âmbito da LGPD (art. 7º, II e X). O artigo 4º, da Lei do Cadastro Positivo, autoriza ao gestor (pessoa jurídica responsável pela administração do banco de dados) a criação de perfis de

consumo ou do histórico de crédito independentemente do consentimento prévio do consumidor.

No funcionamento do cadastro positivo, adota-se o modelo *opt out*, pelo qual o consumidor pode ter seus dados processados independentemente de sua autorização, mas é possível que este opte por obstar a atividade mediante sua expressa oposição e solicitação de retirada de seu perfil da composição do cadastro gerenciado pelo gestor. A licitude do tratamento de dados para esses fins é reforçada pelo inciso X, do art. 7º, da LGPD, o qual dispõe sobre a legitimidade do tratamento de dados pessoais para fins de proteção ao crédito, inclusive quanto ao disposto na legislação pertinente (justamente a Lei do Cadastro Positivo).

Pelo modelo *opt out*, a vontade do pessoa não é irrelevante. Da abertura do cadastro positivo pelo gestor (entidade de proteção ao crédito), deve o gestor ou o credor comunicar o fato ao consumidor no prazo de trinta dias (art. 4º, §4º, da LCP). Mesmo diante da importância das informações para o mercado tomado em sua coletividade e dos potenciais benefícios ao consumidor – como a promessa de redução de juros na contratação de empréstimos – este pode optar por integrar ou não o banco de dados que forma seu cadastro positivo. A Súmula nº 550, do STJ, reforça a prescindibilidade do consentimento do consumidor para a utilização do escore de crédito (*credit score*) e a licitude da prática foi declarada pelo STJ ao formar o Tema Repetitivo nº 710:

> Súmula 550-STJ: A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.
> [***Em realidade, a Súmula 510-STJ originou-se do Tema 710, cuja tese foi assim firmada***:]
> 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.

A despeito da normativa própria e da dispensa de consentimento como base legal para o tratamento de dados, a prestação de serviços de proteção ao crédito deve observar as disposições da LGPD, ainda que de modo compatível com as disposições legais disciplinadas na legislação específica. O art. 43 do CDC trata das informações relativas ao inadimplemento dos consumidores – ou seja, sua "negativação". A LCP abrange o serviço de atribuição de notas aos bons pagadores. Para ambos os propósitos, os direitos do titular devem ser assegurados, nos moldes da disciplina da LGPD, tais como o direito de acesso aos dados e correção de dados incompletos inexatos ou desatualizados (art. 18, II e III, da LGPD). Trata-se da aplicação em diálogo das fontes das normativas incidentes sobre um mesmo suporte fático.

4.1.2 Exigências específicas para a legítima atuação das entidades de proteção ao crédito.

Há pressupostos legais específicos que devem ser rigorosamente observados para legitimar a atuação das entidades de proteção de crédito, os quais são disciplinados mediante a aplicação integrada do CDC e da LCP. Esse diálogo de fontes é chancelado pelo art. 1º, *caput*, deste diploma normativo, o qual estatui que "*Esta Lei* [12.414/2011] *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, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor*."

Como desdobramentos objetivos e práticos da aplicação concomitante e sinérgica de ambas as normas (CDC e LCP), podem ser elencadas as seguintes conclusões:

1)	A Lei 12.414/2011 não revoga qualquer dispositivo do Código de Defesa do Consumidor;
2)	Os princípios (boa-fé objetiva, transparência, proteção à dignidade do consumidor, entre outros) do CDC, bem como seus conceitos legais e doutrinários (consumidor, fornecedor, banco de dados e cadastro de consumo), devem ser considerados e aproveitados na interpretação da Lei 12.414/2011;
3)	Eventual omissão (lacuna) de uma norma deve ser suprida pela outra;
4)	Eventual conflito entre os diplomas deve ser resolvido, com a técnica da proporcionalidade, sob as luzes da Constituição Federal, prevalecendo, no caso concreto, a norma que mais densifica princípio ou valor constitucional.

Tabela 5 - Estruturação das conclusões extraídas pelo diálogo das fontes entre o CDC e a LCP, conforme elencados por Leonardo Bessa (2022, pág. 322)

O aproveitamento de conceitos de uma norma para outra é representativo quanto à análise dos pressupostos legais que devem ser observados pelas entidades de proteção ao crédito. A respeito das exigências quanto ao conteúdo das informações arquivadas, exige o §1º, do art. 43, do CDC, que os dados sejam objetivos, claros, verdadeiros e em linguagem de fácil compreensão. A complementação desses termos é extraída do §2º, do art. 3º, da Lei de Cadastro Positivo, o qual define o significado dessas exigências:

> § 2º Para os fins do disposto no § 1º , consideram-se informações:
> I - objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor;
> II - claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica;
> III - verdadeiras: aquelas exatas, completas e sujeitas à comprovação nos termos desta Lei; e
> IV - de fácil compreensão: aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados.

A respeito do requisito da objetividade dos dados, cabe notar que o juízo de valor, em regra, é exercido pelo fornecedor (aquele que irá consultar o conteúdo dos dados da entidade gestora). No entanto, há exceção, diante da possibilidade, prevista no art. 7º-A, da LCP, de que as próprias gestoras (entidades de proteção ao crédito) exerçam a avaliação do risco do consumidor mediante a disponibilização, ao consulente, de uma nota de riscos ou de pontuação para avaliação do crédito.

O propósito de exigir a clareza das informações constantes dos bancos de dados é possibilitar a sua compreensão pelo consumidor, em especial, para que este possa exercer o direito de acesso e de retificação aos dados pessoais. Assim, pela exigência da clareza das informações, ainda que os registros dos bancos de dados sejam dirigidos aos fornecedores, seu conteúdo deve ser facilmente compreendido pelos consumidores (BESSA, 2022, pág. 331).

Quanto à pertinência da exigência da veracidade das informações, tal requisito complementa a proteção aos direitos da personalidade do consumidor. Informações que não correspondam a uma situação real induzem uma avaliação incorreta pelo consulente e uma consequente violação à honra do consumidor.

Não há, por outro lado, uma obrigatoriedade de que as informações que interessam à avaliação do crédito sejam previamente comprovadas antes de serem inseridas no banco de

dados. No entanto, o consumidor pode questionar a exatidão da informação a qualquer tempo. O fato de não cumprir com o dever de comprovar a veracidade de uma informação pode gerar sanções tanto ao gestor quanto ao consulente.

A facilidade de compreensão se refere à possibilidade de o consumidor compreender por que motivo eventual crédito foi negado ou por qual razão uma taxa de juros foi fixada em determinado patamar. O requisito complementa a necessidade de transparência de parâmetros e a possibilidade de o interessado exigir retificação de seus dados. Ademais, os elementos e critérios considerados na composição das notas (art. 7º-A, LCP) devem ser pertinentes para a composição da pontuação. Esse atributo é complementado por outro requisito, previsto no §3º, do art. 3º, da LCP, o qual proíbe expressamente a utilização de dados excessivos (não vinculados à análise do crédito) ou sensíveis do consumidor (pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas).

Há, ainda, três limites temporais a respeito das informações que podem ser arquivadas nos bancos de dados de proteção ao crédito. Por um lado, o art. 43, §1º, do CDC, estabelece que as entidades de proteção ao crédito não podem manter "*informações negativas por período superior a 5 anos*"; de outro, o §5º do mesmo dispositivo, determina que os bancos de dados de proteção ao crédito não podem conter informações relativas a dívidas prescritas que possam impedir ou dificultar o acesso ao crédito junto aos fornecedores. Por fim, o art. 14, da LCP, estabelece que as informações sobre o adimplemento (informações positivas) não poderão constar de bancos de dados que visem a formação de histórico de crédito do consumidor por período superior a 15 anos.

O prazo de 5 anos (art. 43, §1º, do CDC) independe do prazo prescricional da dívida. Seu termo inicial começa no dia seguinte ao do vencimento da dívida, qualquer que seja a data da efetiva inscrição no cadastro de inadimplentes (BESSA, 2022). Esse aspecto revela outra exigência ao conteúdo dos bancos de dados de proteção ao crédito: a indicação do vencimento da obrigação.

Caso ocorra a prescrição da *cobrança* da dívida (Súmula 323, STJ)[32] antes do decurso do prazo de cinco anos do vencimento da obrigação, a informação também deverá ser excluída do banco de dados. Esse é o teor da exigência constante do art. 43, §5º, da LGPD. Quanto às informações de adimplemento do consumidor (informações positivas), a Lei do Cadastro

[32] Note-se que a prescrição se refere à ação de cobrança, nos termos da súmula 323 do STJ: "A inscrição do nome do devedor pode ser mantida nos serviços de proteção ao crédito até o prazo máximo de cinco anos, independentemente da prescrição da execução."

Positivo admite que poderão constar de bancos de dados por período não superior a 15 (quinze) anos. Ultrapassado esse prazo, tal informação deverá ser excluída da base de dados utilizadas para a formação do histórico de crédito do consumidor (art. 14, da LCP).

Os requisitos quanto ao conteúdo e os limites cronológicos (temporais) da informação arquivada definem a *qualidade dos dados* utilizados pelos bancos de proteção ao crédito. Todos os requisitos elencados consolidam uma grande obrigação para a legítima utilização de bancos de dados de proteção ao crédito: a manutenção da *qualidade* dos dados neles constantes.

Em síntese, o dever de manter a *qualidade* dos dados tratados para fins de proteção ao crédito é atendido se respeitados os critérios estruturados no quadro a seguir:

Qualidade dos dados para formação dos bancos de dados de proteção ao crédito.		
Quanto ao conteúdo do dado arquivado.	LCP, art. 3º, I	Objetividade
	LCP, art. 3º, I	Clareza
	LCP, art. 3º, I	Veracidade
	LCP, art. 3º, I	Facilidade de compreensão
	LCP, art. 3º, §3º.	Não excessivo ou de conteúdo sensível.
	CDC, art. 43, §6º	Formato acessível, inclusive a pessoa com deficiência.
Quanto aos limites cronológicos da informação	CDC, art. 43, §1º	Período de manutenção da informação negativa (dívida vencida e não paga) por tempo não superior a 5 anos. (deve indicar a data de vencimento da obrigação)
	CDC, art. 43, §5º	Vedação de tratamento de informações sobre dívidas prescritas.
	LCP, art. 14.	Período de manutenção de informação positiva (adimplemento) por período não superior a 15 anos.

Tabela 6 - Requisitos para aferir a qualidade dos dados de um banco de dados de proteção ao crédito. Elaborado pela autora.

O dever de manter a qualidade dos dados não esgota as obrigações do fornecedor e do gestor. De início, cabe citar que o registro de cada nova informação negativa (relativa a inadimplemento) deve ser previamente comunicado ao consumidor pela entidade de proteção ao crédito (art. 43, §2º, do CDC e Súmula 359, do STJ[33]). Leonardo Bessa (2022) defende que o dever de comunicação abrange qualquer novo registro negativo no banco de dados e

[33] Súmula 359, do STJ: "*Cabe ao órgão mantenedor do Cadastro de Proteção ao Crédito a notificação do devedor antes de proceder à inscrição*."

independe se a fonte da informação for a todos acessível. Exalta-se, nesses casos, a importância do contexto no qual as informações são inseridas – reconhece-se que os efeitos de um protesto de título ou de ações de cobrança, por exemplo, são diversos ou agravados pela *negativação* do nome de um consumidor em entidade que preste serviços de proteção ao crédito. O aviso deve ser por escrito, dispensável o AR (Súmula 404, do STJ)[34], e é exigido a cada nova inscrição negativa.

Quanto às informações positivas, impõe-se uma única comunicação (art. 4º, §4º, da LCP) a ser realizada no início do tratamento de dados para formação do histórico de crédito, autorizada a utilização de dados pessoais (como endereço residencial, comercial ou eletrônico) para estabelecer o meio para sua efetivação. A Lei Complementar nº 166, de 2019, detalha que obrigação de comunicar ao cadastrado deve ser prévia e conter informações sobre a identidade do gestor, sobre o armazenamento e o objetivo do tratamento dos dados pessoais (art. 5º, V).

O art. 43, §3º, do CDC, chancela o direito à retificação dos dados arquivados pelas entidades de proteção ao crédito. A correção dos dados ou a baixa da indicação do nome do consumidor no cadastro de inadimplentes deve ser realizada pelo credor (Súmula 548, do STJ)[35] no prazo máximo de 5 dias úteis ou em até 10 dias úteis para correção ou cancelamento de informações positivas anotadas em bancos de dados (art. 5º, III, da LCP). No último caso, o consumidor pode optar cancelar ou reabrir seu cadastro, o qual deve ser atendido no prazo de até 2 dias úteis (art. 5º, §6º, da LCP). A Lei de Cadastro Positivo determina a gratuidade desses pedidos (art. 4º, §4º), o que é reforçado pela disciplina do *habeas data*, expressa quanto à gratuidade de procedimento para acesso e retificação de dados, bem como para sua impetração (art. 21, da Lei 9.507/1997[36]).

O direito de acesso aos dados sobre inadimplemento pelo próprio consumidor é assegurado pelo *caput* do art. 43, do CDC. A LCP reforça essa obrigação por dispor que ao cadastrado é assegurado o direito de acesso gratuito e independentemente de justificativa a respeito das informação sobre ele existentes no baco de dados, inclusive sobre seu histórico e sua nota ou pontuação de crédito, que deve ser atendido no prazo de até 10 dias (art. 5º, II, e §3º, LCP).

---

[34] Súmula 404, do STJ: "*É dispensável o aviso de recebimento (AR) na carta de comunicação ao consumidor sobre a negativação de seu nome em bancos de dados e cadastros*."
[35] Súmula 548, do STJ: "*Incumbe ao credor a exclusão do registro da dívida em nome do devedor no cadastro de inadimplentes no prazo de cinco dias úteis, a partir do integral e efetivo pagamento do débito*."
[36] Lei do *Habeas Data*, art. 21: "*São gratuitos o procedimento administrativo para acesso a informações e retificação de dados e para anotação de justificação, bem como a ação de habeas data*."

A LCP aprofunda diversos modos pelos quais o direito de acesso deve ser atendido, com destaque para o que dispõe o art. 6º. O dispositivo obriga aos gestores de bancos de dados, quando solicitados, a fornecer ao cadastrado:

> I - todas as informações sobre ele constantes de seus arquivos, no momento da solicitação;
> II - indicação das fontes relativas às informações de que trata o inciso I, incluindo endereço e telefone para contato;
> III - indicação dos gestores de bancos de dados com os quais as informações foram compartilhadas;
> IV - indicação de todos os consulentes que tiveram acesso a qualquer informação sobre ele nos 6 (seis) meses anteriores à solicitação;
> V - cópia de texto com o sumário dos seus direitos, definidos em lei ou em normas infralegais pertinentes à sua relação com gestores, bem como a lista dos órgãos governamentais aos quais poderá ele recorrer, caso considere que esses direitos foram infringidos; e
> VI - confirmação de cancelamento do cadastro.

Todas essas exigências têm por propósito assegurar os direitos da personalidade do consumidor/cadastrado, em especial quanto à sua privacidade e honra, bem como realizar o princípio da efetiva prevenção a danos materiais e morais, conforme estabelece o art. 6º, VI, do CDC. Nota-se que se todos os pressupostos normativos que embasam a legitimidade da atuação das entidades de proteção ao crédito não forem rigorosamente atendidos, há imediata caracterização de ofensa aos direitos da personalidade do consumidor/cadastrado (BESSA, 2022).

Para fins de objetiva avaliação acerca da regularidade do tratamento de dados pessoais segundo as específicas normativas sobre o tema (CDC e LCP), os deveres e critérios que devem ser observados pelo agente de tratamento para o objetivo de proteção ao crédito no mercado de consumo são consolidados segundo o quadro organizado da seguinte forma:

Principais exigências para legitimar a atuação das entidades de proteção ao crédito.		
Manter a ***qualidade*** dos dados	Observar exigências quanto ao ***conteúdo*** do dado	- Objetividade - Clareza - Veracidade - Facilidade de compreensão - Dado não excessivo ou de conteúdo sensível; - Formato acessível, inclusive a pessoa com deficiência.
	Observar ***limites cronológicos*** da informação	- informação negativa não superior a 5 anos; - relativa à dívida não prescrita

		- informação positiva não superior a 15 anos.
Dever de **comunicação**	(CDC, art. 43, §2º)	Dever de comunicação prévia e por escrito a cada nova inscrição negativa.
	(LCP, art. 4º, §4º e art. 5º, V)	Dever de comunicação única prévia ao início do tratamento de dados, efetivada junto ao endereço residencial, comercial ou eletrônico do cadastrado.
Dever de **retificação** ou de **cancelamento** da informação	(CDC, art. 43, §3º)	Em até 5 dias úteis (relativo às informações negativas)
	(LCP, art. 5º, III)	Em até 10 dias úteis (relativo às informações positivas)
Dever de **cancelamento ou reabertura** do cadastro positivo	(LCP, art. 5º, §6º)	Dever de atender à solicitação de cancelamento ou reabertura do cadastro positivo, no prazo de até 2 dias úteis

Na atividade de processamento de dados para atender à finalidade de proteção do mercado por meio de serviços de proteção ao crédito, em uma aplicação em diálogo do CDC, da LCP e da LGPD, tais requisitos devem ser observados para qualificar um tratamento de dados como regular.

4.2 Do Marco Civil da Internet.

A Lei nº 12.495/2014, conhecida como Marco Civil da Internet (MCI), é o resultado da primeira experiência de regulação em larga escala acerca da utilização da Internet no Brasil. Além de estabelecer direitos e deveres para o uso da Internet, o MCI foi elaborado com o intuito de resolver determinadas questões conflituosas, como as relativas à proteção dos registros, aos dados pessoais e às comunicações privadas; à neutralidade de rede; à responsabilidade civil dos provedores de conexão e aplicações da internet; ao dever de guarda de registros e a sua eventual requisição judicial. O propósito da normativa é basicamente sopesar, de um lado, seu papel como instrumento para proteção de direitos do cidadão na rede e, de outro, a manutenção de uma Internet livre, aberta e democrática.

O MCI elege como alguns de seus princípios a proteção do direito à privacidade e aos dados sociais (art. 3º, I e II), o que orienta seu perfil regulatório na interpretação de regras sobre o fluxo de informações pessoais no meio eletrônico. No entanto, a despeito da coincidência literal de propósitos entre a LGPD e o MCI, o valor social que o Marco Civil da Internet atribui à proteção à privacidade se refere à confidencialidade e ao sigilo das comunicações (BIONI, 2021). Em outras palavras, o MCI define uma centralidade de sua regulação no propósito de

resguardar o sigilo e a inviolabilidade das comunicações privadas as quais somente poderão sofrer interferências de modo excepcional e mediante ordem judicial (art. 7º, II e III[37]).

Nesses termos, Bruno Bioni (2021, pág. 214) enfatiza que o MCI impõe um núcleo duro voltado à preservação da integridade do fluxo informacional em detrimento do poder de disposição dos titulares dos dados pessoais. A normativa define a liberdade de expressão, a inviolabilidade e o sigilo das comunicações como direitos que gozam de posição privilegiada, de modo a afastar da esfera de autonomia de seus titulares a formação da legitimidade do tratamento de dados pessoais que integrem tal processo comunicacional.

A previsão da neutralidade de rede como princípio da normativa (art. 3º, IV) reforça que os pilares do MCI são pautados no direito de externar ideias, juízos de valores e as mais diversas manifestações do pensamento, bem como impedir a intromissão de terceiros ou do Estado, para permitir o livre desenvolvimento da personalidade humana por meio da garantia ao livre fluxo de informações, sem distinção por conteúdo, origem, destino, terminal ou aplicação (art. 9º, do MCI).

O dever de guarda de registros de conexão e de acesso a aplicações de internet é restrito. Na provisão de conexão, o MCI proíbe guardar os registros de acesso a aplicações de internet (art. 14), mas impõe o dever de manter, sob sigilo, os registros de conexão pelo prazo de um ano (art. 13, *caput*). Na provisão de aplicações de internet por pessoa jurídica que exerça essa atividade de forma organizada, o MCI impõe o dever de manter, sob sigilo, os respectivos registros de acessos a aplicações de internet pelo período de seis meses (art. 15, *caput*). O dever de guarda dos dados de conexão (neles incluídos o IP do usuário) impõe aos provedores de acesso a guarda de *dados pessoais* dos usuários, diante da possibilidade e de efetiva identificação do usuário. Nesse sentido, evidencia-se a intensa correlação da disciplina do MCI e da LGPD em matéria de tratamento de dados pessoais.

O MCI afasta do provedor de conexão à internet o dever de responder (art. 18, *caput*) pelo conteúdo ofensivo ou ilícito divulgado no meio digital. Pode-se dizer que essa lei consagra o princípio da inimputabilidade da rede e defende que o combate a ilícitos na Internet deve atingir os responsáveis finais (ou seja, os terceiros responsáveis por elaborar e divulgar o conteúdo ofensivo) e não os meios de acesso e transporte de dados (TEFFÉ; SOUZA, 2019). O foco de proteção da normativa é a liberdade de expressão e a privacidade – compreendida em

[37] MCI. Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

sua esfera de proteção ao sigilo – e também se volta ao propósito de afastar a vigilância dos cidadãos, a censura prévia, a remoção arbitrária de conteúdos e manipulações tendenciosas das informações.

O princípio da inimputabilidade de redes – também invocado nos casos em que se questiona a responsabilidade civil das redes sociais, aplicativos de mensagens instantâneas e demais ferramentas de comunicação no meio digital por conteúdos inseridos por terceiros – é mitigado de modo excepcional, mediante o preenchimento de determinados critérios legais, como o descumprimento de ordem judicial específica que impõe a remoção de um determinado conteúdo bem como a viabilidade técnica para cumprir tal decisão.

Por essa orientação, diante da condição privilegiada que a liberdade de expressão ocupa para a promoção de direitos na rede de Internet, o art. 19, do MCI[38], estabelece que o provedor de aplicações de internet somente poderá ser civilmente responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, no âmbito e nos limites técnicos de seu serviço, não tomar providências para atender ordem judicial específica no prazo assinalado para tornar indisponível o conteúdo elencado como infringente do direito de alguém. Aos provedores de aplicação, portanto, aplica-se a tese da responsabilidade subjetiva. É a regra geral estabelecida pelo MCI.

O Marco Civil da Internet colocou o Poder Judiciário como a instância legítima para definir a licitude ou ilicitude de um conteúdo divulgado na Internet bem como sobre o que deve ser removido ou não do ambiente de comunicações em meio digital. Em princípio, portanto, não é o descumprimento de uma notificação extrajudicial privada que gera a responsabilidade do referido provedor e não há um dever de monitoramento prévio dos conteúdos gerados por terceiros. Aliás, a normativa define que a remoção de conteúdo por iniciativa dos provedores

---

[38] MCI. Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.
§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.
§ 4º O juiz, inclusive no procedimento previsto no § 3º , poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

não pode ser arbitrária, sob ofensa dos preceitos do MCI, em especial, da neutralidade de rede. Por outro lado, é legítima a retirada direta de conteúdo pelos provedores de aplicações quando contrário aos termos e políticas de uso da plataforma.

O Superior Tribunal de Justiça consolidou o posicionamento de que a fiscalização prévia de conteúdos postados por terceiros em plataformas de redes sociais (como Facebook, WhatsApp e Instagram) não constitui atividade intrínseca da rede social. Os riscos de uma imposição nesse sentido poderia constituir um barreira para inovações de caráter tecnológico bem como possibilitar um indesejado efeito de censura prévia, incompatível com as liberdades garantidas pela Constituição Federal, como a liberdade de expressão e de pensamento. Como representativo desse posicionamento, colaciona-se os entendimentos elencados e sintetizados pelo próprio Tribunal Superior:

> REDE SOCIAL. RESPONSABILIDADE CIVIL DO PROVEDOR DE APLICAÇÃO. REDE SOCIAL. FACEBOOK. OBRIGAÇÃO DE FAZER. REMOÇÃO DE CONTEÚDO. FORNECIMENTO DE LOCALIZADOR URL DA PÁGINA OU RECURSO DA INTERNET. COMANDO JUDICIAL ESPECÍFICO. NECESSIDADE. OBRIGAÇÃO DO REQUERENTE. MULTA DIÁRIA. OBRIGAÇÃO IMPOSSÍVEL. DESCABIMENTO.
> 1. Esta Corte fixou entendimento de que
> "(i) **não respondem objetivamente** pela inserção no site, por terceiros, de informações ilegais;
> (ii) **não podem ser obrigados a exercer um controle prévio** do conteúdo das informações postadas no site por seus usuários;
> (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos;
> (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso". Precedentes.
> 2. **Aos provedores de aplicação, aplica-se a tese da responsabilidade subjetiva**, segundo a qual o provedor de aplicação torna-se responsável solidariamente com aquele que gerou o conteúdo ofensivo se, ao tomar conhecimento da lesão que determinada informação causa, não tomar as providência necessárias para a sua remoção. Precedentes. [...]
> 4. A necessidade de indicação do localizador URL não é apenas uma garantia aos provedores de aplicação, como forma de reduzir eventuais questões relacionadas à liberdade de expressão, mas também é um critério seguro para verificar o cumprimento das decisões judiciais que determinar a remoção de conteúdo na internet.
> 5. Em hipóteses com ordens vagas e imprecisas, as discussões sobre o cumprimento de decisão judicial e quanto à aplicação de multa diária serão arrastadas sem necessidade até os Tribunais superiores.
> (STJ - REsp: 1642560 SP 2016/0242777-4, Relator: Ministro Marco Aurélio Bellizze, Data de Julgamento: 12/09/2017, T3 - Terceira Turma, Data de Publicação: DJe 29/11/2017) – **grifos da autora**.

Constata-se, nesses termos, que o dano moral decorrente de mensagens com conteúdo ofensivo inseridas nas plataformas de provedores de aplicações da internet não constitui risco inerente à atividade desenvolvida por este, o que afasta responsabilidade objetiva nos moldes previstos no art. 927, parágrafo único, do CC/2002. A responsabilidade pelo ato de terceiro, nos moldes do art. 19, do MCI, é subjetiva por omissão do provedor e se verifica (apenas) quando este não retira o conteúdo ofensivo após ordem judicial.

Há duas exceções pontuais a essa regra. Em primeiro lugar, figuram os conteúdos protegidos por direitos autorais (art. 19, §2º, do MCI), para os quais não é aplicada a regra da notificação judicial (TEFFÉ; SOUZA, 2019). A responsabilidade do provedor pelos conteúdos gerados por terceiros segue a específica disciplina da legislação autoral vigente e aplicável na data de entrada em vigor do MCI (art. 31, do MCI[39]). A segunda exceção se refere ao dever de o provedor, uma vez notificado extrajudicialmente, retirar imagens, vídeos ou materiais contendo cenas de nudez ou de atos sexuais de caráter privado sem autorização de seus participantes (art. 21, do MCI[40]).

Chiara Teffé e Carlos Souza (2019) compreendem que a vítima da inserção de conteúdo lesivo nas plataformas de aplicação tem a possiblidade de auferir duas compensações distintas: uma pelo provedor e outra pelo terceiro responsável pela inserção do conteúdo ofensivo. De fato, o MCI não afasta o dever de indenizar daquele que diretamente promoveu a divulgação do conteúdo lesivo na plataforma. O usuário que propaga informações e comentários é o responsável principal pelas consequências de suas manifestações e responde pelos eventuais abusos que pratique em relação aos direitos de terceiros.

A esse respeito, cabe colacionar entendimento do Juizado Especial Cível do Tribunal de Justiça do Distrito Federal (TJDFT). No caso, o autor de postagem ofensiva utilizou foto postada pelas próprias vítimas, mas com o acréscimo de conteúdos (legendas) difamatórias, depreciativas e de cunho homofóbico que ultrapassaram o legítimo exercício de sua liberdade

[39] MCI. Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

[40] MCI. Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

de expressão. O reconhecimento do ilícito, nessas circunstâncias não é embasado no Marco Civil da Internet, mas pela disciplina da responsabilidade civil extracontratual, pautada pelos termos do Código Civil:

> DIREITO CIVIL. RESPONSABILIDADE CIVIL. PUBLICAÇÃO DE FOTO E COMENTÁRIOS OFENSIVOS EM REDE SOCIAL (FACEBOOK). INTENÇÃO DE RIDICULARIZAR E PROPAGAR AVERSÃO À ORIENTAÇÃO SEXUAL. OFENSA AO DIREITO À IMAGEM E À HONRA. DANOS MORAIS CARACTERIZADOS. RECURSO CONHECIDO E PROVIDO.
> 1. Trata-se de recurso inominado interposto pelos autores contra a sentença que julgou improcedente o pedido inicial, sob o fundamento de que, analisando o contexto no qual a foto e a mensagem foram postadas pelo réu em sua rede social, não haveria danos morais, na medida em que somente não teria tido abuso da liberdade de manifestação de pensamento.
> 2. Em suas razões recursais, os autores defendem que a publicação da foto com os comentários realizados na rede social Facebook ultrapassaram o limite da livre expressão, uma vez que o objetivo era difundir preconceito em relação aos homossexuais, atribuindo adjetivo negativo em nítido intuito difamatório e injuriador, devendo, por consectário, responder, o réu, pelo abuso que cometeu.
> 3. No caso em análise, os autores, que são noivos, fizeram uma foto em que ambos se vestiam de noivas e a publicaram em seu Instagram. Narram que o réu teve acesso ao registro e fez a **republicação da fotografia em sua própria rede social Facebook, utilizando-se de uma legenda ofensiva e discriminatória**, a que somou um comentário igualmente ofensivo de sua parte. Salientam que o requerido ainda se utilizou de *emojis* em seus comentários que expressam nojo, ódio e estranheza e que vários comentários foram incluídos por outras pessoas na postagem do réu, também homofóbicos e violadores da honra dos autores.
> 4. **O fato de os próprios autores terem postado a foto em suas redes sociais não significa permissão para que outras pessoas a republiquem e, ao argumento de liberdade de expressão, ridicularizem no Facebook a orientação sexual deles**.
> 5. O acervo probatório dos autos demonstra que a republicação da foto feita pelo réu em sua rede social gerou diversos comentários preconceituosos e ofensivos aos autores. Citem-se alguns desses comentários: ?Reflexão profunda: um cara que não gosta de mulher tem mais é que tomar no c.. mesmo!...kkk?. ?É inaceitável essas coisas de homem se vestir de noivinha! Ecaaaa! Ser gay não é desmunhecar?. ?O jeito é rir para não chorar meu amigo, o mundo está perdido?.
> 6. Merece destaque o fato de que o réu, ao ser confrontado em um comentário realizado na postagem da foto, sobre vir a responder na justiça pelos seus atos, ter respondido: ?resolvo fácil?. E ainda diz que: ?eu gosto da resenha, bjao? (ID 5244873). Tais comentários reforçam a ideia de que o réu realmente abusa de seu direito de expressar, fazendo menoscabo, até mesmo, da Justiça.
> 7. Por óbvio que foi a atitude do réu de ter postado em sua rede social a foto dos autores com a utilização da mencionada legenda, ela por si já bastante depreciativa, o fator que desencadeou os comentários igualmente depreciativos e homofóbicos das outras pessoas, devendo ser responsabilizado pelos prejuízos gerados pela sua conduta.

> 8. **A situação vivenciada pelos autores, independentemente da preexistência de postagem da mesma foto em sua própria rede social, certamente que superou os limites do mero aborrecimento**. Inegavelmente, foram eles submetidos à situação vexatória, humilhante, com potencial de causar forte dor íntima e transtornos de ordem emocional.
> 9. A liberdade de manifestação e de expressão é constitucionalmente assegurada a todos, mas o limite claro dela é não atingir os atributos da personalidade alheia injustamente. Nesse sentido, comentários em redes sociais que extrapolam o *animus narrandi*, ou seja, aquele de apenas relatar e informar a coletividade, com o fito apenas de promover a divulgação de ofensas morais devem ser indenizados. [...]
> (TJ-DF 07100353120188070016 DF 0710035-31.2018.8.07.0016, Relator: Gabriela Jardon Guimaraes de Faria, Data de Julgamento: 07/11/2018, 2ª Turma Recursal dos Juizados Especiais Cíveis e Criminais do DF, Data de Publicação: Publicado no DJE : 12/11/2018) – **grifos da autora**.

Quanto ao dever jurídico de prestar informações sobre a identidade do usuário de serviço de internet que seja o autor de inserção de conteúdo na internet que ofenda direito alheio, o MCI reconhece a possibilidade de decisão judicial determinar a obrigação do provedor de conexão/acesso à internet de fornecer, com base no endereço de IP (*Internet Protocol*), os dados cadastrais do autor de ato ilícito (art. 22, do MCI[41]). Nesse sentido, extrai-se do dever legal de guarda imposto pelo MCI a obrigatoriedade de identificação dos usuários pelas empresas de conexão da internet, ainda que não sejam os responsáveis pela postagem. Não se trata, importante ressaltar, de uma imposição de responsabilidade pelos atos de terceiro, mas sim de um desdobramento processual pautado no seu dever jurídico de guarda de determinadas informações.

Uma vez presentes indícios de ilicitude de conteúdo postado, a privacidade do usuário (compreendida no sentido de sigilo de dados pessoais) é mitigada diante da possibilidade de que uma determinação judicial imponha aos provedores de conexão/acesso o fornecimento de dados cadastrais (como nome, endereço, RG e CPF) extraídos a partir dos IPs apresentados pelo provedor de aplicação.

Distintos, portanto, os deveres de provedores – nos moldes regulados pelo MCI – dos deveres dos usuários em não realizar manifestações que ofendam direito da personalidade de outrem, em nítido abuso da liberdade de manifestação do pensamento.

---

[41] MCI. Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

Em síntese, os deveres impostos pelo Marco Civil da Internet são direcionados aos provedores. O provedor de aplicações de internet não se responsabiliza por conteúdo gerado por terceiro (art. 18, do MCI), salvo, de maneira subsidiária, após ordem judicial (art. 19, do MCI) ou a pedido do ofendido (art, 21, do MCI – casos de nudez) para exclusão do conteúdo se omitir no cumprimento. Exige-se, portanto, a omissão ilícita nesses casos.

Cabe notar que a matéria não se encontra plenamente consolidada. Na presente data – 21 de abril de 2023 –, encontram-se afetados os Temas de Repercussão Geral nº 533, 987 e 1141 do Supremo Tribunal Federal acerca dos seguintes temas:

STF. Tema 533	Sobre o dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, *sem intervenção do Judiciário*.
STF. Tema 987	Discussão acerca da constitucionalidade do art. 19 da Lei n. 12.965/2014 (MCI) que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos perpetrados por terceiros
STF. Tema 1141	Responsabilidade civil por disponibilização na internet de informações processuais publicadas nos órgãos oficiais do Poder Judiciário, sem restrição de segredo de justiça ou obrigação jurídica de remoção.

Tabela 7 - Estruturação dos Temas de Rercussão Geral pendentes de julgamento pelo STF relativos à aplicação do MCI. Elaborado pela autora.

A resolução de controvérsias envolvendo a utilização de dados pessoais dos usuários certamente será afetada pelo deslinde dos referidos Temas. No momento, prevalece a compreensão da responsabilidade limitada dos provedores, os quais, a despeito de possibilitarem a divulgação de informações, não são, pelo MCI, responsáveis pelo tratamento irregular de dados pessoais por seus usuários. Diferenciam-se os deveres e correspondentes consequências entre o terceiro que insere o conteúdo e a plataforma que o veiculou.

Quanto aos dados pessoais, no âmbito de análise do MCI, é possível visualizar duas situações distintas que pautam a análise e identificação dos deveres atribuídos aos provedores: a primeira relaciona-se aos deveres de guarda de informações e a segunda diz respeito ao conteúdo gerado por terceiros. Quando se trata do dever de guarda de dados, há uma responsabilidade direta do provedor. Por outro lado, quanto ao conteúdo gerado por terceiros, a responsabilidade será subsidiária e subjetiva, somente se verificando diante de uma omissão ilícita. Reitera-se que esse cenário pode mudar diante dos desdobramentos do Temas de

Repercussão Geral nº 533, 987 e 1141 afetados pelo Supremo Tribunal Federal, o que poderá impactar diretamente no relacionamento interpretativo do MCI e da LGPD.

4.3 Da Lei Geral de Proteção de Dados brasileira.

4.3.1 Dos objetivos e fundamentos da LGPD.

O art. 1º da LGPD determina que o objetivo de sua disciplina é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Os propósitos da própria LGPD coincidem com a evolução conceitual do direito à privacidade e com a valorização dos direitos fundamentais para efetivar a proteção do ser humano – tomado como valor central do ordenamento jurídico. A despeito de não ser elencado de forma expressa nessa lei nacional o direito à proteção das informações do titular, a tutela ao direito da proteção de dados pessoais, enquanto categoria autônoma de direito fundamental, é um dos propósitos que orienta a própria aplicação da LGPD.

A noção contemporânea da privacidade relaciona sua tutela à liberdade de escolhas do indivíduo e chancela o livre desenvolvimento de sua personalidade. Nota-se, no art. 1º (LGPD), uma nítida inspiração de seu texto na decisão paradigmática tomada pelo Tribunal Constitucional Alemão, em 1983 – *Volkszählungsurteil* – BVerfGE 65, 1. Essa decisão recontextualizou a noção de privacidade para além do direito ao sigilo, de modo a contribuir com o desenvolvimento jurídico do conceito relativo à autodeterminação informacional. A Corte alemã também reconheceu a proteção de dados pessoais como projeção de um direito geral de personalidade e como preceito que abrange um direito de poder decidir sobre (1) a divulgação e uso de seus dados pessoais; (2) sobre os limites que sua vida pessoal possa ser revelado e (3) sobre o direito de tomar conhecimento sobre quem sabe e o quanto sabe sobre as informações que lhes digam respeito (SCHWANE, 2005).

O caso paradigmático alemão reconhece os riscos que o processamento de dados por sistemas automatizados podem gerar. Especialmente diante da possibilidade de formar um perfil completo da personalidade dos cidadãos. Essa noção ultrapassa a abordagem dicotômica entre o que é considerado público e a exclusão do conhecimento externo do que for classificado como privado. Trata-se de um caso paradigmático justamente por reconhecer que o *contexto* do uso nos quais os dados podem ser processados é relevante para avaliar os riscos à autonomia e liberdade do indivíduo.

A paradigmática decisão da Corte alemã, em 1983, consolida a relação entre liberdade e proteção de dados pessoais, de modo a revelar a necessidade de tutela de um direito da personalidade que visa proteger o direito da pessoa natural de livremente escolher o modo de ser, de viver e de se relacionar. Trata-se de uma manifestação da autodeterminação informativa, que orienta a análise jurídica de um tratamento de dados a partir do *contexto* das condições atuais e de circunstâncias futuras que possam gerar riscos ao livre desenvolvimento de sua personalidade. É nesse contexto que o conceito de tutela à liberdade deve orientar a aplicação da LGPD.

Quanto ao objetivo de tutelar o direito da privacidade (art. 1º, LGPD), sua invocação para os mais diversos propósitos revela uma difusão de caminhos que torna difícil apontar um conceito único ou descrever sua evolução de forma linear. O que se pode afirmar é que a essência das modificações da tutela jurídica às informações que digam respeito às pessoas não abandona o conceito de privacidade interpretado a partir do artigo de Warren e Brandeis, publicado em 1890 (*the right to be let alone*). O direito de ser deixado só, em uma visão de proteção do indivíduo contra ingerências externas, não se tornou obsoleto com a passagem do tempo.

Houve uma expansão do conceito da privacidade a partir da constatação de que restringir sua concepção apenas como um direito individual negativo, por pressupor uma divisão entre o público e o privado ou entre o íntimo e o divulgado, não é o suficiente para alcançar uma proteção aos fatos e informações considerados de conhecimento público (MENDES e FONSECA, 2022). Esse fato impulsionou o desenvolvimento de um conceito positivo de privacidade, traduzida como uma possibilidade de o indivíduo ter conhecimento e tomar decisões a respeito do tratamento de seus dados.

Esse retrato se amolda à concepção do direito civil-constitucional, pela qual sustenta-se que a tutela da pessoa humana supera a divisão dicotômica direito público *versus* direito privado e não se satisfaz com a tutela ressarcitória e repressiva guiada pelo binômio lesão-sanção. Exige-se, de modo diverso, instrumentos de promoção do homem, considerado em qualquer situação jurídica de que participe, seja contratual ou extracontratual, de direito público ou de direito privado. (TEPEDINO, 1999).

Quanto à tutela da LGPD ao livre desenvolvimento da personalidade da pessoa natural (art. 1º), nota-se que o desenvolvimento da privacidade e da proteção de dados pessoais como aspectos da dignidade da pessoa humana revela que a extensão de sua proteção deve garantir aspectos existenciais de uma pessoa no desenvolvimento de sua personalidade. Ao lado do aspecto negativo e positivo do desenvolvimento jurídico da privacidade e tutela de dados,

portanto, acrescenta-se outro, voltado a garantir a tutela ao seu aspecto existencial, ou seja, o poder de decidir como sobre o *ser*, sobre o *comportar*, sobre o mudar (aspectos individuais) e sobre como quer ser representado perante a sociedade (aspecto coletivo).

A correlação entre os principais preceitos que orientam a LGPD, elencados em seu art. 1º (liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural), compõem os objetivos e os aspectos tutelados pela normativa. Os objetivos, direitos implícitos, e aspectos negativo, positivo e existencial tutelados podem ser assim estruturados:

<table>
<tr><th>Tutela de Dados Pessoais pela LGPD</th><th>Garantir:</th><th>Aspectos protegidos:</th></tr>
<tr><td rowspan="3">Art. 1º.
Objetivos.</td><td>Direito Fundamental da privacidade</td><td rowspan="2">Negativo: direito ao sigilo</td></tr>
<tr><td>Direito Fundamental da Liberdade;</td></tr>
<tr><td>Livre desenvolvimento da personalidade da pessoa natural</td><td rowspan="2">Positivo: direito de exercer controle pelo consentimento e pelo direito ao conhecimento de quem realiza o tratamento e quais informações foram coletadas</td></tr>
<tr><td rowspan="2">Direitos implícitos tutelados:</td><td>Autodeterminação informativa</td></tr>
<tr><td>Direito fundamental à Proteção aos dados pessoais.</td><td>Existencial: direito efetivo de escolher e determinar como sua personalidade será em si formada (aspecto individual) e como será representada perante a sociedade (aspecto coletivo)</td></tr>
</table>

Tabela 8. Estruturação visual dos objetivos da LGPD e aspectos tutelados. Elaborado pela autora.

Há uma intensa correlação entre os objetivos elencados pela LGPD. A privacidade, no contexto atual, abrange a expressão de tutela ao livre desenvolvimento da personalidade da pessoa humana, a qual se relaciona com sua liberdade de escolha. É equivocado compreender que o legislador buscou, na enumeração dos objetivos, uma conceituação estanque e necessariamente diversa entre os termos. Os conceitos se sobrepõem e convergem para a ampla proteção do ser humano. O legislador buscou, em realidade, se esquivar da definição do âmbito de tutela da LGPD de forma limitada à conceituação de seus termos. Ainda que se defenda a diferença terminológica entre privacidade e proteção de dados pessoais – pela qual aquela seja interpretada pelo conceito tradicional de sigilo e esta seja compreendida como um direito de controle –, a abrangência da tutela à pessoa é ampla: compreende todos os aspectos que digam respeito ao desenvolvimento de sua personalidade.

Em outras palavras, garante-se não apenas o direito de ser deixado só (intimidade, sigilo ou privacidade), ou o poder de controle sobre as informações pessoais (em referência à proteção de dados pessoais), mas também a forma como a representação de sua personalidade é formada e retratada perante a sociedade digital (ao que se pode referir como proteção à autodeterminação

informativa, ao livre desenvolvimento da personalidade da pessoa natural ou tutela aos aspectos individuais e coletivos da privacidade).

No cenário tecnológico atual, ao tratar a tutela à privacidade e à proteção de dados pessoais como um dever de ocultação (perspectiva negativa), o foco das medidas frente às novas tecnologias volta-se a evitar cibercrimes, como ataques hackers ou vazamento de dados (*data breaches*), e sobre como responsabilizar aquele que perpetrou tais condutas.

Pelo aspecto positivo, o foco volta-se ao controle da coleta ou a adoção de medidas que garantam o direito de escolha (em especial, pelo consentimento informado), a transparência e o conhecimento do titular sobre dados coletados e as finalidades de seu tratamento, especialmente em relações com desequilíbrios de poder, como a do indivíduo perante o Estado ou perante forças econômicas (*Apple* ou Amazon, por exemplo). A análise do *contexto* nos quais os dados são inseridos ganha relevância. De fato, por vezes não é a publicidade, mas a situação na qual uma informação está inserida é o ponto determinante para aferir um dano. O nome, uma informação notadamente pública, inserido em uma lista de aprovados em um concurso gera um impacto completamente diverso em comparação à sua inserção em um cadastro de inadimplentes ou até mesmo em uma lista de procurados pela INTERPOL.

Quanto à tutela aos aspectos existenciais do tratamento de dados, a inovação e impactos de tecnologias que promovem processamento autônomo de informações (como a Inteligência Artificial) reforçam a necessidade de tutela à autonomia do indivíduo. Não se trata de uma reflexão sobre a exposição exacerbada (aspecto negativo), construção de perfis digitais involuntários com impactos na aquisição de bens ou serviços (sistema de *credit score*) ou mesmo no poder de decisão do indivíduo sobre as finalidades de tratamento de seus dados (aspecto positivo). Cuida-se do reconhecimento de que a própria existência e escolhas de um indivíduo não são necessariamente livres, pois potencialmente manipuladas. Casos de *fake news* no âmbito político e sanitário induziram a reflexão sobre o papel da desinformação pulverizada e direcionada de acordo com o perfil dos indivíduos desenhado a partir de tratamento de dados pessoais.

A autonomia da pessoa é colocada em xeque, tanto pela perspectiva de assegurar a possibilidade de tomar decisões a respeito de sua personalidade como pela forma de garantir que as suas escolhas não sejam determinadas por fatores externos ilegítimos. Esses aspectos assumiram especial relevância diante da profusão de desinformações a respeito da vacinas contra a COVID-19 e da efetividade de cuidados paliativos no tratamento de doenças, os quais assumiram impactos de proporções desarrazoadas no combate à pandemia.

Ademais, o direcionamento de informações de acordo com as tendências políticas de cada pessoa é elemento que reforça divisões sociais maniqueístas, impedem o diálogo e até fomentam movimentos violentos. A preocupação com o tratamento de dados, nesses casos, não diz respeito ao direito de sigilo ou de controle dos dados pelos titulares. Aliás, estes são muitas vezes fornecidos voluntariamente pelos próprios titulares. O tema diz respeito, em realidade, sobre a tomada de medidas aptas a limitar a influência do tratamento de dados na indução de escolhas do titular, como no combate à *fake news*. Ocorre que o mero debate sobre tomar alguma medida nesses casos já carrega polêmicas, especialmente quando se considera o direito fundamental à liberdade de expressão e de manifestação do pensamento (art. 5º, IV e IX, da CF/1988).

A efetivação da tutela dos aspectos existenciais do indivíduo não é completamente elucidada pela LGPD. Há direcionamentos principiológicos, mas a aplicação concreta dependerá, em essência, de políticas públicas e da jurisprudência que será consolidada a partir das decisões dos tribunais.

Além dos objetivos, o art. 1º da LGPD estabelece o seu objeto de incidência: o tratamento de dados pessoais. Nesse ponto, cabe verificar se há alguma atividade que envolva o tratamento (conforme os exemplos elencados no art. 5º, X, da LGPD) e se tal atividade é exercida com o emprego de dados relacionados a pessoas identificadas ou identificáveis (art. 5º, I). O passo seguinte se volta a verificar se o tratamento de dados pessoais está ou não listado nos propósitos que, se verificados, afastam o âmbito de tutela da LGPD (art. 4º, da LGPD) e, em caso negativo, cabe considerar se os aspectos territoriais da atividade se enquadram nas hipóteses previstas no art. 3º, da LGPD.

Antes de adentrar nas questões relativas à aplicação da LGPD, cabe considerar que não apenas seus objetivos (art. 1º) orientam sua incidência. O art. 2º, do mesmo diploma, elenca os fundamentos que orientam a interpretação da normativa. Os sete incisos do dispositivo enumeram propósitos que, em uma leitura rápida, parecem até ser contrapostos:

Fundamentos que orientam a interpretação da LGPD – art. 2º.	
O respeito à privacidade A autodeterminação informativa A inviolabilidade da intimidade, da honra e da imagem;	A liberdade de expressão, de informação, de comunicação e de opinião; O desenvolvimento econômico e tecnológico e a inovação;

Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.	A livre iniciativa, a livre concorrência e a defesa do consumidor

Tabela 9 - Divisão e ordenação dos fundamentos "contrapostos" do art. 2º, da LGPD. Elaborado pela autora.

Conforme afirma Tarcísio Teixeira e Ruth Maria Guerreiro, "*não há que se falar em progresso sem a utilização de dados, pois estes são a base de grandes conquistas tecnológicas, e a tendência é que cada vez mais o tratamento de dados seja a grande força motriz da economia*." (2022, p. 14). O tratamento de dados pessoais para propósitos organizacional, político ou financeiro não é condenado pela LGPD. A disciplina da proteção de dados tem como fundamento, além da proteção do indivíduo, o desenvolvimento econômico, tecnológico e a inovação (art. 2º, V, da LGPD), bem como a livre iniciativa e a livre concorrência (art, 2º, VI, da LGPD). A extensão da tutela ao titular de dados pessoais exige a convergência desses fundamentos. O intérprete, portanto, não pode se pautar pela contraposição de propósitos, mas pela necessária convergência destes na análise da regularidade de um tratamento de dados pessoais.

De acordo com a LGPD, a utilização de dados pessoais para propósitos mercadológicos ou institucionais (art. 2º, V e VI, da LGPD) e para o exercício da liberdade de expressão, de informação, de comunicação e de opinião (art. 2º, III, da LGPD) deve obedecer os limites determinados pela privacidade (art. 2º, I, da LGPD); autodeterminação informativa (art. 2º, II, da LGPD); inviolabilidade da intimidade, da honra e da imagem (art. 2, IV da LGPD) para que, em suma, sejam respeitados os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, VII, da LGPD). Tais limites, no entanto, nem sempre são claros. Variam de acordo com o caso concreto que pauta a análise.

A LGPD, além de centralizar a tutela de dados pessoais em um documento legal, também assume o papel de ponderar interesses em (aparente e constante) conflito. Os debates acerca da utilização de dados pessoais indicam que posicionamentos dicotômicos serão a regra no enfrentamento de casos concretos (como o debate sobre a liberdade de expressão frente à privacidade de um indivíduo). A feição eminentemente principiológica da normativa tem o benefício de garantir perenidade da normativa, mas reforça a centralidade do intérprete no exercício da parametrização de direitos em aparente conflito. O que se pode afirmar, com segurança, é que qualquer posição maniqueísta no uso de dados pessoais deve ser afastada.

Cabe reiterar que manipulação de informações para os mais diversos propósitos diversos – como financeiros ou mesmo políticos – não é condenada. Na sociedade contemporânea, nem poderia ser. A LGPD assume propósito eminentemente regulador do exercício de um tratamento de dados – e não repressor dessa atividade. A sociedade demanda a utilização de dados na relações sociais e para o desenvolvimento dos setores tanto públicos como privados. As análises sobre proteção do indivíduo não podem culminar em obstáculo ao desenvolvimento tecnológico, o qual, em última análise, beneficia toda a coletividade.

4.3.2 Suportes fáticos para incidência da LGPD.

Os dados de pessoas jurídicas não são considerados pessoais para fins de incidência da LGPD. O diploma apenas abrange dados que identifiquem ou tornem identificáveis pessoas *naturais* (art. 1º, art. 5º, I, LGPD). Já o meio pelo qual o dado pessoal é tratado é amplo o suficiente para abranger qualquer sistema que o empregue, seja físico ou digital, seja de modo *online* ou *offline* (TEIXEIRA, GUERREIRO 2022).

A *finalidade* pelo qual o dado é empregado é relevante para determinar a incidência da LGPD (art. 4º). Não se enquadram no escopo da Lei Geral de Proteção de Dados os tratamentos de dados pessoais realizados exclusivamente por pessoa natural para fins eminentemente particulares e não econômicos, por exemplo. É o caso de anotações em agendas telefônicas nos *smartphones* de uso pessoal. A LGPD também exclui de seu escopo os dados pessoais utilizados para fins artísticos, jornalísticos e acadêmicos (art. 4º, II, da LGPD) ou, ainda, para atender a exclusivos fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais (art. 4º, III, da LGPD).

Sobre a finalidade jornalística como motivo legítimo a mitigar a privacidade e a proteção e dados pessoais, cabe considerar que o Supremo Tribunal Federal considerou incompatível com a Constituição a noção de um direito ao esquecimento. Nesses termos, não se admite qualquer tentativa de obstar, seja em meio analógico ou digital, a comunicação de dados pessoais relacionados com a divulgação de fatos ou dados verídicos (desde que licitamente obtidos). Tampouco seria possível utilizar de algum dos fundamentos da LGPD para pleitear a exclusão de uma publicação jornalística relativa a fatos verdadeiros. Nesse sentido, são os entendimentos do Supremo Tribunal Federal e do Superior Tribunal de Justiça:

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a

> divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais – especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral – e as expressas e específicas previsões legais nos âmbitos penal e cível.
> STF. Plenário. RE 1010606/RJ, Rel. Min. Dias Toffoli, julgado em 11/2/2021 (Repercussão Geral – Tema 786) (Info 1005).
>
> O direito ao esquecimento é considerado incompatível com o ordenamento jurídico brasileiro. Logo, não é capaz de justificar a atribuição da obrigação de excluir a publicação relativa a fatos verídicos.
> STJ. 3ª Turma. REsp 1961581-MS, Rel. Min. Nancy Andrighi, julgado em 07/12/2021 (Info 723).

A LGPD também exclui de sua incidência os dados que tenham origem fora do território nacional – desde que não haja nenhuma comunicação ou uso compartilhado destes com agentes de tratamento brasileiros – ou, ainda, que sejam objeto de transferência internacional com outro país que não o de proveniência – desde que, nesse caso, o país de proveniência proporcione grau de proteção de dados adequados ao previsto na LGPD (art. 4º, IV, da LGPD).

Nos termos de seu art. 3º, a LGPD incide sobre qualquer operação realizada no território nacional (inciso I). Por outro lado, ainda que o tratamento de dados ocorra fora do Brasil, a LGPD incidirá nos casos em que a atividade realizada compreender a oferta ou fornecimento de bens ou serviços a pessoas que estejam no Brasil (inciso II) ou que envolvam dados pessoais coletados no território nacional (inciso III). A abrangência territorial quanto à aplicação da LGPD, portanto, não se restringe aos limites geográficos do Brasil. A normativa inclui sob seu regime operações realizadas no território nacional e também alcança circunstâncias que envolvam o oferecimento de bens ou serviços ao mercado consumidor brasileiro ou que envolvam o tratamento no exterior de dados pessoais coletados no território nacional. Como afirma Teixeira e Guerreiro (2022, pág. 15), para avaliar se a atividade de tratamento de dados pessoais se submete ao regime de proteção da LGPD, "*não são levados em consideração: o país sede da empresa, o meio de operação e tratamento de dados, a localização dos dados e nem mesmo a nacionalidade do titular dos dados, bastando que se encontre em território nacional no momento da coleta*."

Sobre o tema, mas no âmbito de investigação criminal, cabe indicar que o STJ decidiu que a empresa Facebook Inc., mesmo com a sede situada nos EUA, deve cumprir ordens judiciais para fornecimento de dados independentemente de pedido de cooperação jurídica

internacional ou da circunstância de possuírem filiais no Brasil e/ou realizarem armazenamento em nuvem:

> CRIME PRATICADO EM TERRITÓRIO NACIONAL, ATRAVÉS DE SERVIÇO OFERECIDO AOS USUÁRIOS BRASILEIROS. IRRELEVÂNCIA DE A PROVEDORA OPTAR PELO ARMAZENAMENTO DOS DADOS EM NUVEM.
> 1. Empresas que prestam serviços de aplicação na internet em território brasileiro devem necessariamente se submeter ao ordenamento jurídico pátrio, independentemente da circunstância de possuírem filiais no Brasil.
> 2. O armazenamento em nuvem é estratégia empresarial que não interfere na obrigação de observância da legislação brasileira quando o serviço é prestado em território nacional.
> 3. A recalcitância injustificada no cumprimento de decisão judicial atrai a imposição de multa como penalização da prática de ato atentatório à dignidade da Justiça.
> (STJ. 5ª Turma. RMS 66392-RS, Rel. Min. João Otávio de Noronha, julgado em 16/08/2022 – Info 750).

Sobreleva a importância da análise interpretativa integrada de normas diversas incidentes sobre o mesmo suporte fático quando se considera o posicionamento do Superior Tribunal de Justiça a respeito da incidência da lei brasileira sempre que a operação de coleta, armazenamento ou tratamento de registros, dados pessoais ou comunicações por provedores de conexão e de aplicação de internet ocorrer no território nacional, ainda que as atividades sejam realizadas por empresa com sede no estrangeiro:

> INTERNET. JURISDIÇÃO. SOBERANIA DIGITAL. PREQUESTIONAMENTO. AUSÊNCIA. MARCO CIVIL DA INTERNET. ALCANCE. APLICAÇÃO DA LEGISLAÇÃO BRASILEIRA. PERTINÊNCIA DA JURISDIÇÃO NACIONAL.
> [...]
> 2. O propósito recursal consiste em determinar a competência da Poder Judiciário Brasileiro para a determinação do fornecimento de registros de acesso de endereço de e-mail, localizado em nome de domínio genérico ".com".
> 3. Em conflitos transfronteiriços na internet, a autoridade responsável deve atuar de forma prudente, cautelosa e autorrestritiva, reconhecendo que a territorialidade da jurisdição permanece sendo a regra, cuja exceção somente pode ser admitida quando atendidos, cumulativamente, os seguintes critérios: (i) fortes razões jurídicas de mérito, baseadas no direito local e internacional; (ii) proporcionalidade entre a medida e o fim almejado; e (iii) observância dos procedimentos previstos nas leis locais e internacionais.
> 4. Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil. Precedente.

> 5. É um equívoco imaginar que qualquer aplicação hospedada fora do Brasil não possa ser alcançada pela jurisdição nacional ou que as leis brasileiras não sejam aplicáveis às suas atividades.
> 6. Tem-se a aplicação da lei brasileira sempre que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet ocorra em território nacional, mesmo que apenas um dos dispositivos da comunicação esteja no Brasil e mesmo que as atividades sejam feitas por empresa com sede no estrangeiro.
> (STJ. 3ª Turma. REsp 1745657-SP, Rel. Min. Nancy Andrighi, julgado em 03/11/2020 – Info 683). – grifos da autora.

No percurso interpretativo da LGPD, os dispositivos enunciados têm como propósito principal elencar as etapas de análise necessárias para avaliar sua incidência. Nesse ponto, sobre os aspectos que atraem a disciplina da LGPD, analisam-se a atividade de tratamento de dados (arts. 1º e 5º, incisos I e X); os propósitos ou finalidades do tratamento (art. 4º); e o âmbito de incidência da LGPD (art. 3º). A partir desse ponto, o percurso interpretativo da LGPD se volta a identificar as partes que compõem a relação jurídica formada bem como identificar os direitos e deveres atribuídos pela normativa.

4.3.3 Das partes que compõem a relação jurídica regulamentada pela LGPD

No percurso interpretativo da LGPD proposto, os três primeiros passos se propõem a caracterizar a incidência da LGPD de acordo com as atividades que se pretende executar: 1) se a atividade configura tratamento de dados pessoas (arts. 1º, 5º, incisos I e X); 2) que atividade não se enquadra em algum dos propósitos ou finalidades que dispensam a aplicação da LGPD (art. 4º, LGPD); 3) que o tratamento de dados se insere no âmbito de incidência da norma brasileira (art. 3º, LGPD).

O quarto passo envolve a identificação dos deveres impostos aos agentes de tratamento. Para tanto, o agente deve identificar seu papel na atividade: se de controlador (tomador de decisões), de operador (executa as decisões) ou de encarregado (intermediador entre o controlador, o titular de dados e a ANPD).

Na relação estabelecida no tratamento de dados pessoais, figura, de um lado, o titular e, de outro, o agente de tratamento. O titular é a pessoa natural a quem se referem os dados pessoais que são objeto do tratamento enquanto aquele que realiza a atividade de processamento desses dados é denominado “agente de tratamento”.

Agente de tratamento é expressão que abrange tanto a figura do controlador como a do operador (art. 5º, IX, da LGPD). Quanto às semelhanças, ambos podem ser pessoas naturais ou

jurídicas, de direito público ou privado. A diferença se situa nas atribuições. O controlador é o responsável por tomar *decisões* referentes ao tratamento de dados pessoais. O operador, por sua vez, é quem *executa* o tratamento de dados pessoais nos moldes decididos pelo controlador.

Figura 9. Representação das figuras de controlador e encarregado, com destaque para a diferença de suas atribuições. Elaborado pela autora

Para facilitar a compreensão quanto à distinção de atribuições, toma-se como exemplo uma pessoa jurídica que comercializa calçados em uma loja física e que pretenda ingressar no comércio eletrônico para vender seus produtos. Para tanto, elenca como medidas necessárias a elaboração, em uma plataforma virtual, de um site que propicie interface favorável com clientes e que possibilite a realização de pagamentos online; o gerenciamento e inventário do depósito dos produtos; a organização da logística de envios e prazos atendidos; e a promoção de ações de publicidade e de prospecção para aumentar o alcance do conteúdo do site e dos produtos a novos clientes bem como para a manutenção do engajamento com aqueles que já são consumidores. No exemplo, todas essas atividades, para melhor funcionamento e tratamento personalizado, fazem uso de dados pessoais coletados tanto pela navegação do titular de dados no site da pessoa jurídica quanto pelas informações fornecidas pelo próprio consumidor para realização da compra de produtos.

A empresa poderia assumir todas essas atribuições e, assim, concentrar tanto a figura do controlador, pelas decisões tomadas, quanto a do operador, pela execução dessas medidas. Por outro lado, a fornecedora, no exercício de sua função de controladora, pode tomar as decisões acerca dos propósitos que pretende alcançar e delegar as atividades operacionais a terceiros – que assumirão a figura do operador dos dados.

Podem ser contratados operadores diferentes para executar, no exemplo: [A] a criação e manutenção da plataforma virtual no qual os produtos são comercializados; [B] a gestão do

pagamento seguro de forma online; [C] a organização logística de inventário de calçados e de entrega dos produtos transacionados; e [D] a utilização de histórico de compras e outros dados coletados para promoção de ações de publicidade e marketing para prospecção dos produtos a novos clientes e manutenção do interesse daqueles que já são consumidores.

Nesse cenário, o controlador aparece como a figura central que toma decisões acerca do tratamento de dados por quatro diferentes empresas:

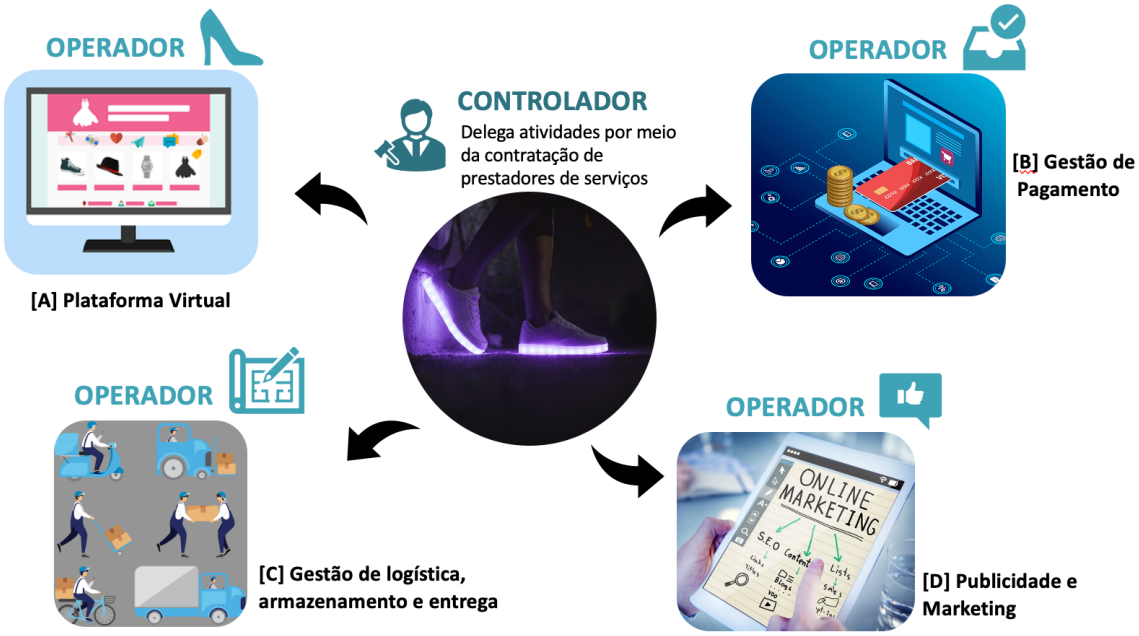

Figura 10 - Exemplificação da Fornecedora de sapatos como controladora dos dados e a respectiva delegação da execução de suas decisões a operadores de tratamento.

Tanto ao controlador como ao operador é atribuído o dever de garantir o regular tratamento de dados perante a Autoridade Nacional de Proteção de Dados (ANPD) – conforme os termos do artigo 52, *caput*[42] (LGPD) – e perante o titular de dados – conforme art. 42, *caput*

[42] LGPD. Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); IX - (VETADO). X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

(LGPD)[43]. Não se confundem com a figura do encarregado, ou seja, com aquela pessoa indicada pelos agentes de tratamento para atuar como canal de comunicação (intermediador) entre o controlador, os titulares de dados e a ANPD (art. 5º, VIII, LGPD).

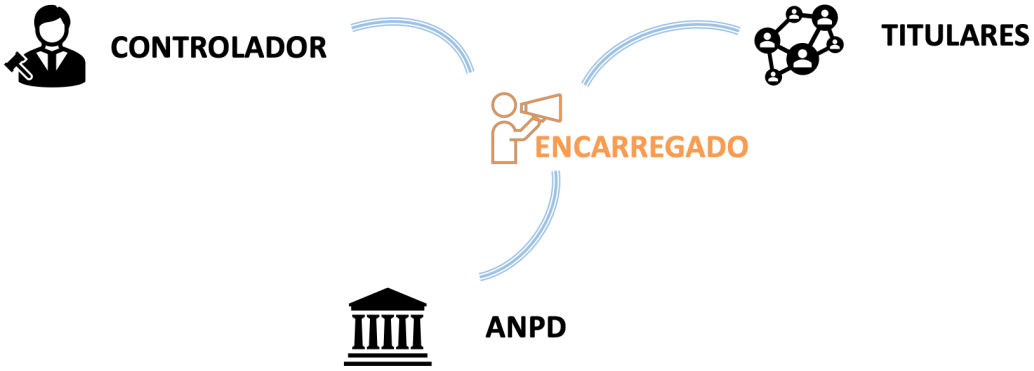

Figura 11. Representação da função de intermediador do encarregado.

O encarregado deve ser identificado de forma pública e, preferencialmente, de forma clara e objetiva no sítio eletrônico do controlador (art. 41, §1º, LGPD). Nos termos do §2º do art. 41 (LGPD), suas atividades consistem em:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Além da diferença de atribuições, especialmente quanto à incumbência do dever de garantir a regularidade do tratamento de dados pessoais, outra grande diferença entre a figura dos agentes de tratamento e a do encarregado é que a indicação deste pode ser dispensada pela Autoridade Nacional (art. 41, §3º, LGPD) considerando-se o porte da empresa ou volume das operações de tratamento de dados.

No percurso interpretativo da LGPD, verificada a incidência da normativa e a identificação do papel assumido na relação jurídica estabelecida no âmbito de um tratamento

[43] LGPD. 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.

de dados, cabe aos agentes de tratamento, em especial ao controlador, enquadrar a atividade pretendida em algumas das bases legitimadoras de tratamento de dados. Sobre o tema, é relevante notar que a LGPD diferencia dados pessoais "comuns" (art. 5º, I) dos dados sensíveis (art. 5º, II), conforme hipóteses elencadas, respectivamente, pelo arts. 7º e 11 de seu texto legal.

4.3.4 Das bases legitimadoras do tratamento de dados e dos direitos dos titulares.

Antes de iniciar qualquer operação, o agente de tratamento deve enquadrar sua atividade dentro das hipóteses legitimadoras do tratamento de dados previstas no artigo 7º (para o caso de tratamento de dados pessoais que se enquadrem na categoria definida pelo art. 5º, I) ou no artigo 11 (na circunstância de tratamento de dados pessoais sensíveis[44]). Enquanto o artigo 7º elenca dez incisos que elencam as hipóteses legais para o tratamento de dados pessoais "comuns", o artigo 11 dispõe sobre nove bases legais para o tratamento de dados sensíveis.

Na análise de todas essas bases legitimadoras, o ponto diferencial mais representativo entre o art. 7º e o 11 se refere à impossibilidade de se utilizar o legítimo interesse como hipótese legal para o tratamento de dados sensíveis. Por outro lado, há uma coincidência no conteúdo quanto às demais hipóteses, as quais podem ser enquadradas em dois grupos: o tratamento regular com base no consentimento expresso do indivíduo e o tratamento regular com base em um respaldo legal (independentemente de autorização do titular).

4.3.4.1 Do consentimento do titular

O consentimento revela uma preocupação do legislador em efetivar a participação do indivíduo no fluxo de informações que lhes digam respeito. Traduz-se em uma possibilidade para que uma pessoa natural exerça sua autodeterminação em relação aos dados pessoais que lhes digam respeito (DONEDA, 2006).

O respaldo à efetivação da autonomia de uma pessoa, como forma de exercer seu direito da personalidade, é anterior à LGPD, conforme se verifica pelo enunciado nº 404, da Jornada de Direito Civil (JDC), a respeito do art. 21, do Código Civil, pela qual é previsto que "*a tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal*

[44] Art. 5º, 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;

dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas."

O enunciado nº 405 da JDC reforça a noção de que não há informações inúteis diante da relevância do cenário tecnológico atual: "*as informações genéticas são parte da vida privada e não podem ser utilizadas para fins diversos daqueles que motivaram seu armazenamento, registro ou uso, salvo com autorização do titular*". Desse modo, a manifestação de concordância com uma finalidade do tratamento de dados não pode ser estendida a outra sem o respectivo consentimento do seu titular. Em outras palavras, o ordenamento exige a aquiescência específica da pessoa natural para cada novo propósito da atividade de tratamento de dados pessoais.

Nos termos da LGPD, o consentimento deve configurar uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII); deve ser fornecido por escrito – em cláusula destacada (art. 8.º, 1º) – ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º, *caput*), vedada as autorizações genéricas (art. 8º, §4º).

A mudança de finalidade dos dados coletados mediante consentimento não é proibida, mas deve ser comunicada ao titular – o qual pode revogar sua aquiescência caso discorde da alteração (art. 8º, §6º). Aliás, a revogação do consentimento é direito do titular, que deve ser realizado em procedimento gratuito e facilitado (art. 8º, §5º).

As exigências previstas na LGPD corroboram com a constatação de que o ônus da prova do consentimento não cabe ao titular de dados. A própria normativa atribui ao controlador a responsabilidade de demonstrar que o consentimento foi obtido em conformidade com a lei (art. 8º, §2º). Trata-se de uma inversão *ope legis* do ônus da prova, ou seja, determinada pela própria legislação.

Ocorre que a inversão *ope legis* que atribui a comprovação do consentimento ao agente tratamento ainda não é reconhecida pelos tribunais (ao menos não de forma ampla ou consolidada). Há entendimentos que afirmam ser do titular de dados a incumbência de demonstrar que os dados tenham sido obtidos de forma ilícita – ao invés de determinar ao agente de tratamento o ônus de demonstrar a licitude da coleta de dados que armazena.

Representativo dessa situação é o caso em que um consumidor pleiteou a condenação de empresas de telefonia para cessar ligações de telemarketing e reparar danos morais experimentados. O Tribunal de Justiça do Distrito Federal não acolheu tal pretensão sob a justificativa de que o consumidor não teria demonstrado que os números de telefone foram

obtidos de forma ilícita e que a atividade de telemarketing, mesmo sem a indicação da legalidade da origem ou da forma como coletada os dados pessoais, não configura uma atividade ilegal:

> SERVIÇOS DE TELEMARKETING. LGPD. ABUSO DE DIREITO. NÃO DEMONSTRADO. AUSÊNCIA DE DANO EXTRAPATRIMONIAL INDENIZÁVEL.
> [...]
> 2. **A oferta de produtos e serviços por telemarketing, por si só, não constitui ilegalidade** ou violação às normas de proteção ao consumidor, posto não se constituir em prática vedada pelo ordenamento jurídico pátrio. [...]
> 3. Inexistindo qualquer indício de prova de que o número telefônico do autor tenha sido obtido por meio de vazamentos de dados ou utilizado de forma ilícita, não se constata potencial violação à Lei Geral de Proteção de Dados Pessoais - LGDP, atribuível às empresas apelantes. [...]
> 4.1. **Empresas que se desoneraram do *onus probandi* de que os telefonemas supostamente originários de seus serviços de telemarketing não lhes pertencem**; não representaram frequência abusiva, ou, ainda, que tenham sido realizados após a solicitação autoral de cessação dos contatos publicitários, afastando as respectivas responsabilidades de indenizar os alegados danos extrapatrimoniais experimentados pelo autor.
> Acórdão 1422420, 07057689620218070020, Relator: CARMEN BITTENCOURT, 1ª Turma Cível, data de julgamento: 18/5/2022, publicado no DJE: 26/5/2022. – grifos da autora.

Acrescente-se que o consentimento não é exigido para os dados tornados manifestamente públicos pelo titular (art. 7º, §4º, LGPD). Essa autorização, por outro lado, não se confunde com a possibilidade do uso indiscriminado de tais dados. Os direitos do titular e os princípio previstos na Lei devem ser observados assim como o *contexto* no qual a informação foi tornada pública. Ademais, o tratamento de dados pessoais cujo acesso é público deve ser pautado pela finalidade, boa-fé e o interesse que justificaram a sua disponibilização (art. 7º, §3º, LGPD). "*Vale recordar aqui, dados cuja divulgação pública é obrigatória: o fato de alguém ser proprietário de um imóvel, sócio de uma empresa ou casado. Outro exemplo é a consulta de CPFs no site da Receita Federal com o propósito de mera confirmação da titularidade para operações financeiras*." (VIOLA e TEFFÉ, 2023, pág. 124).

Dados de acesso público são aqueles gerados ou acumulados pelo Poder Público que não estejam sob sigilo ou sob restrição de acesso nos termos da Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação, ou simplesmente LAI. Tal conceito é extraído a partir da redação do art. 2º, II, do Decreto nº 8.777/2016 – normativa que institui a Política de Dados Abertos do Poder Executivo Federal. Assim, o dado será público devido a políticas adotadas pelo Poder Público. Diferenciam-se dos dados manifestamente públicos, que são

aqueles tornados públicos pelo próprio titular. Sobre a diferença entre dados públicos e dados manifestamente públicos, vale transcrever a elucidativa diferenciação (BIONI, 2019 pág. 267):

> Em termos conceituais, dados de acesso público são distintos dos manifestamente públicos. Neste último, a disponibilização da informação se daria por iniciativa do próprio titular e não por terceiros e, por fim, o seu acesso não teria qualquer tipo de restrição. Por exemplo, a informação do item "b" não é manifestamente pública nem divulgada por quem a ela está vinculada. Para acessá-la, é necessário fazer uma consulta à base de dados do Poder Judiciário – uma espécie de "filtro" –, que é quem disponibiliza tal informação sobre o possível devedor (réu de uma ação), enquanto os dados de um perfil público de uma rede social são divulgados pelo seu próprio titular, sendo plenamente acessível por quem quer que seja.

Bruno Bioni (2019) ressalta que os §§ 3º e 4º do art. 7º, ainda que tratem das categorias de "acesso público" e "manifestamente públicos", não sugerem a adoção da classificação dicotômica entre dado público e privado para fins de incidência da LGPD – como se adotasse essa opção em detrimento da consideração contemporânea da privacidade contextual. A consideração dos aspectos tutelados pela LGPD em seu art. 1º – privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural – afastam a adoção de uma lógica meramente binominal (público *vs.* privado) na proteção da personalidade do indivíduo.

A racionalidade dicotômica, no entanto, ainda é aplicada pelos tribunais brasileiros para pautar a extensão da proteção de dados pela LGPD. É o exemplo do caso enfrentado pelo Tribunal de Justiça de São Paulo em que diversos consumidores pleitearam indenizações, a título de dano moral, pelo "vazamento" de seus dados mantidos juntos à empresa Eletropaulo, pessoa jurídica vítima de incidente de cibersegurança. Os dados vazados corresponderam aos necessários para instalação elétrica, tais como nome, CPF, data de nascimento, idade, telefone fixo, telefone celular e e-mail.

A 27ª Câmara de Direito Privado do TJ-SP, mesmo reconhecendo a falha na segurança de sistema da empresa como a causa que permitiu que terceiros (por ação de hackers) tivessem acesso a esses dados, negou qualquer ofensa aos direitos da personalidade dos consumidores afetados. Foi utilizado o argumento de que dados "comuns", amplamente ou comumente divulgados no cotidiano, não são aptos a ensejar, "*nem de longe*", ofensa aos direitos da personalidade de seus titulares. É representativo desse entendimento o trecho do voto destacado:

> No caso, analisando os dados que foram violados, **a maioria envolve qualificação do consumidor (nome, RG, CPF), que não é acobertado por**

> **mínimo sigilo** e o conhecimento por terceiro em nada macularia qualquer direito da personalidade da parte autora. Os demais dados não são considerados sensíveis ou violadores de qualquer privacidade ou intimidade. Referidos dados são costumeiramente fornecidos por todos, seja em estabelecimento comercial (físico ou virtual), portarias de acesso a imóveis, aplicativos e sites de compras, muitas vezes até com autorização para sua cessão posterior a terceiros. Informações sobre o consumo de eletricidade da unidade consumidora ou o número de instalação pode até ser acessado em residências em que o relógio medidor se situa na área externa e, também quanto a estes **dados, de pouca relevância** se mostra para terceiros que o acessarem, **não ofendendo, nem de longe, direito da personalidade**.
> Portanto, a violação de tais dados, por si só, não incorre em ofensa a direito da personalidade capaz de ensejar reparação moral.
> (TJ-SP - AC: 10083083520208260704 SP 1008308-35.2020.8.26.0704, Relator: Alfredo Attié, Data de Julgamento: 16/11/2021, 27ª Câmara de Direito Privado, Data de Publicação: 16/11/2021) – **grifos da autora**.

Nota-se, pela fundamentação do excerto do voto colacionado, que o Tribunal sustenta que o fato de o nome, CPF e RG de consumidores não estarem acobertados pelo mínimo sigilo, não seriam dados suscetíveis de causar qualquer dano ao direito da personalidade. Trata-se de uma avaliação dicotômica que alça o sigilo como o valor acobertado pela proteção aos dados pessoais. Nesse sentido, por se tratarem de dados de fácil acesso, não teriam relevância suficiente para ensejar responsabilidade pelo seu vazamento.

Cabe destacar que o tema ainda deve ser avaliado por Tribunal Superior – o que pode modificar as conclusões apontadas. Ressalte-se que o mesmo caso ainda tem avaliações e deslindes distintos no âmbito do próprio tribunal de São Paulo. A 4ª Turma Recursal Cível do TJ-SP reconheceu, para o mesmo caso (vazamento de dados sob a guarda da empresa Eletropaulo), que a ação de eventual hacker constitui fortuito interno que geram danos morais *in re ipsa*, decorrentes do próprio vazamento de dados:

> Recurso inominado – Vazamento de dados pessoais de cliente por empresa fornecedora de energia elétrica – Relação de consumo – Tratamento de dados pessoais de pessoa localizada no território nacional e após 17/09/2020 – LGPD aplicável ao caso – **Vazamento denota que não foram adotadas medidas de segurança eficazes pela controladora/fornecedora (art. 46 da LGPD), o que caracteriza defeito na prestação do serviço** – Responsabilidade objetiva da controladora/fornecedora (art. 14 do CDC) – Ação de eventual hacker que constitui fortuito interno – Danos morais in re ipsa, conforme precedente do STJ – Indenização arbitrada em R$ 5.000,00 – Sentença reformada – Recurso provido.
> (TJ-SP - RI: 10030862120218260003 SP 1003086-21.2021.8.26.0003, Relator: Carlos Eduardo Santos Pontes de Miranda, Data de Julgamento: 25/10/2021, 4ª Turma Recursal Cível - Santo Amaro, Data de Publicação: 25/10/2021) – **grifos da autora**.

A noção de que dados comumente oferecidos pelo titular não estão albergados sob a proteção dos direitos da personalidade recaem na lógica dicotômica pela qual dados públicos não merecem proteção. Não foi a opção adotada pela LGPD, cuja tutela avança para a reflexão das *finalidades* para as quais os dados foram publicizados ou colocados em circulação e os *contextos* nos quais os dados são publicamente acessíveis em atenção à proteção da autodeterminação do indivíduo para o livre desenvolvimento de sua personalidade (art. 1º, *caput*, LGPD).

Sobre a avaliação da regularidade de um tratamento de *dados públicos* para finalidades diversas das que motivaram a sua divulgação pelo Poder Público, Bruno Bioni (2019, pág. 267) elenca duas situações didáticas que exemplificam a importância de análise pautada pela compatibilidade entre as *finalidades* desses tratamentos levando-se em conta o *contexto* que motivou a publicização desses dados:

> a) se, **para fins de transparência**, o Poder Público divulga os nomes, os cargos e a renda dos servidores, tal base de dados dificilmente poderia ser reutilizada para fins de marketing. Por outro lado, seria **possível o seu uso para diagnosticar eventual nepotismo** na Administração Pública;
>
> b) se o Poder Judiciário **disponibiliza certidões sobre processos judiciais para, dentre outras coisas, aferir a capacidade de (in)solvência** dos cidadãos, muito provavelmente, essa informação **poderia ser utilizada para a análise de crédito**. Por outro lado, **seria questionável o seu uso para desclassificar o devedor-candidato em um processo de contratação**. – grifos da autora.

No mesmo sentido, o fato de um dado tornado público pelo próprio titular ser plenamente acessível não fornece carta branca para sua utilização. É preciso considerar o contexto e a finalidade em que o dado foi publicizado por seu titular. O fato de uma pessoa publicar uma foto em uma rede social não autoriza uma empresa a utilizá-la para promover um produto, por exemplo. Por outro lado, é possível, em princípio, utilizar dados disponibilizados pelo titular em sites como Academia.com para promover convites de grupos de pesquisa ou atividades similares nas áreas de interesse selecionadas. Para reforçar essa compreensão, cabe citar outros exemplos (BIONI, 2019, pág. 268):

> Por exemplo, a princípio, terceiros não poderiam usar dados de uma rede social, mesmo que de perfis públicos, para fins de marketing. As circunstâncias pelas quais tais dados foram tornados públicos pelo seu próprio titular deram-se para uma outra finalidade, que é a de se relacionar com quem integra o seu círculo social.

> Por outro lado, a princípio, seria compatível o uso de dados de perfis públicos de uma rede profissional (e.g., LinkedIn) por terceiros, como headhunters, para aproximar seus usuários às vagas profissionais de seu eventual interesse. Esse uso é compatível com a finalidade não só da plataforma em si, como, principalmente, a razão pela qual tais dados são públicos.

Cabe citar outro exemplo, no qual uma pessoa *postou* uma foto em sua rede social (Facebook), na qual se apresentava em um relacionamento com alguém do mesmos sexo, e terceiro republicou tal imagem em seu próprio perfil, na mesma rede social, ridicularizando e manifestando comentários homofóbicos que ridicularizaram sua orientação sexual. O fato de o dado ter se tornado manifestamente público pelo ato do próprio titular não autoriza seu tratamento para finalidade diversa (e ainda agressiva) da que motivou sua divulgação. Nesse sentido:

> 3. No caso em análise, os autores, que são noivos, fizeram uma foto em que ambos se vestiam de noivas e a publicaram em seu Instagram. Narram que o réu teve acesso ao registro e fez a **republicação da fotografia em sua própria rede social Facebook, utilizando-se de uma legenda ofensiva e discriminatória**, a que somou um comentário igualmente ofensivo de sua parte. Salientam que o requerido ainda se utilizou de *emojis* em seus comentários que expressam nojo, ódio e estranheza e que vários comentários foram incluídos por outras pessoas na postagem do réu, também homofóbicos e violadores da honra dos autores.
> 4. O fato de os próprios autores terem postado a foto em suas redes sociais **não significa permissão para que outras pessoas a republiquem** e, ao argumento de liberdade de expressão, ridicularizem no Facebook a orientação sexual deles.
> [...]
> (TJ-DF 07100353120188070016 DF 0710035-31.2018.8.07.0016, Relator: Gabriela Jardon Guimaraes de Faria, Data de Julgamento: 07/11/2018, 2ª Turma Recursal dos Juizados Especiais Cíveis e Criminais do DF, Data de Publicação: Publicado no DJE : 12/11/2018) – **grifos da autora**.

A dispensa do consentimento, portanto, não isenta o tratamento de dados de acesso público e manifestamente público da conformação com a LGPD, em especial diante da proteção contextual nos quais são inseridos. Importante esclarecer que tais dados não deixam de ser pessoais. Ademais, a proteção e o cuidado com as informações pessoais não dizem respeito apenas às esferas do sigilo da privacidade. No modelo de tutela de dados contemporâneo, também se considera que os dados pessoais são componentes essenciais para determinar o grau de liberdade e de autodeterminação individual de cada pessoa. Assim, ainda que se dispense o consentimento como base legitimadora de uma atividade, o tratamento de dados não pode ser

indiscriminado pois aspectos existenciais da tutela de dados pessoais, e não apenas o sigilo, são tutelados.

4.3.4.2 Autorização legal.

Verificam-se similaridades entre as diversas bases legitimadoras do tratamento de dados pessoais previstas no art. 7º, da LGPD. Vislumbra-se, de forma didática, que o dispositivo elenca dez incisos que podem ser enquadrados em três grupos: 1) consentimento informado; 2) autorização legal; e 3) legítimo interesse.

Sobre o consentimento informado (inciso I, art.7º, LGPD), detalhado no tópico anterior, defende-se que o inciso V se aproxima da compreensão de uma autorização normativa com base no consentimento do titular. O dispositivo prevê que tratamento de dados poderá ser realizado "*quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados*". Se o consentimento informado deve ser inequívoco e provado pelo controlador, reforça-se o argumento de que o tratamento de dados é realizado por solicitação do próprio titular. Nota-se, portanto, a aproximação de conteúdo e propósito das hipóteses previstas no inciso I e V do art. 7º, da LGPD.

Não se trata de uma sinonímia. A opção do legislador ao fornecer hipóteses de forma mais detalhada pode ser motivada pelo objetivo de garantir maior segurança jurídica aos contratos firmados, o que é bem vindo na relações contratuais em massa formadas na Sociedade da Informação.

A rigor, toda hipótese de tratamento regular será aquela autorizada em lei (inclusive o consentimento e o legítimo interesse). Afinal, se está previsto na LGPD, tratar-se-á de uma hipótese legal. Por outro lado, vislumbra-se que a LGPD deixou claro que o consentimento ou o detalhamento de um legítimo interesse é dispensável para os casos em que a própria norma autoriza ou determina o processamento de dados pessoais. É o caso da finalidade do tratamento de dados para fins de proteção ao crédito (art. 7º, X, LGPD[45]). A despeito de atender a um interesse social e econômico reconhecido inclusive jurisprudencialmente (STJ, REsp 1.419.697/RS, julgado em 12/11/2014), a própria LGPD autoriza a atividade de acordo com a legislação pertinente (CDC e LCP).

[45] LGPD. 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.

Da mesma forma, o cumprimento de obrigação legal ou regulatória pelo controlador implica no atendimento de exigências previstas em legislação própria (art. 7º, II, LGPD). A realização de estudos por órgão de pesquisa pode se enquadrar tanto no legítimo interesse ou, se prevista em lei, por imposição normativa, como no caso de pesquisas realizadas pelo IBGE (art. 7º, IV, da LGPD).

A LGPD é uma lei que concentra a disciplina do tratamento de dados pessoais em um único documento. Esse fato não implica no reconhecimento desse diploma como a única normativa a disciplinar o tratamento de dados pessoais. A exemplo da Lei de Acesso à Informação, suas disposições não foram revogadas e convivem, em interpretação harmônica, com as disposições da LGPD. Em relação a dados de interesse público, para cumprimento de deveres de transparência e publicidade impostas ao Poder Público, não há conflito entre a LGPD e a LAI. Há autorização legal para o tratamento e divulgação de dados com base na LAI.

Nesse sentido, cabe citar o exemplo de que os entes públicos são compelidos a incluírem nos respectivos Portais de Transparência não apenas o vencimento bruto de cada cargo, mas o nome de todos os agentes e servidores públicos, o cargo exercido, bem como os vencimentos, remunerações, diárias, auxílios, ajudas de custo, vantagens pecuniárias, indenizações, pensões e proventos de aposentadoria auferidas a qualquer título. É pacífico que a divulgação pormenorizada de tais informações não viola a intimidade e a vida privada de seus agentes, sujeitando-os à exposição oficial desses dados de interesse público (ARE 652.777/SP - RG, Rel. Min. Teori Zavascki, DJe 01/07/2015).

A hipótese legal que legitima o tratamento e exposição de dados de servidores públicos não se encontra na autorização de cada titular, mas no dever legal imposto por norma diversa da LGPD. A conformidade com a LGPD, no caso, se baseia no enquadramento do tratamento de dados em uma imposição/autorização normativa.

4.3.4.3 Legítimo interesse.

O legítimo interesse é uma das cláusulas mais amplas previstas na LGPD. O detalhamento da expressão no art. 10 (LGPD) determina que, para se enquadrar nessa hipótese, o controlador deverá utilizar apenas os dados pessoais estritamente necessários para a finalidade pretendida (art. 10, §1º). Indicam-se dois parâmetros para fundamentar a finalidade legítima, mas a própria lei afirma que não se trata de um rol fechado:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

A flexibilidade da cláusula do legítimo interesse como "*carta coringa regulatória*" (BIONI, 2019, pág. 238) abrange situações nas quais uma relação preestabelecida dispensaria um novo consentimento para usos implícitos (pressupostos) de uma atividade já autorizada; quando não houvessem meios para obter tal tipo de autorização ou quando a exigência de consentimento ou autorização legal inviabilizaria o próprio tratamento de dados.

O legítimo interesse não é hipótese que autoriza o tratamento de dados sensíveis. Empresas e o Poder Público podem tratá-los se tiverem o consentimento explícito da pessoa para uma finalidade definida, ou, sem a concordância do titular, para as hipóteses vinculadas ao atendimento de obrigações legais ou situações ligadas a políticas públicas; a estudos via órgãos de pesquisa; a um direito, em contrato ou processo; à preservação da vida e da integridade física de uma pessoa; à tutela de procedimentos realizados por profissionais da área de saúde ou sanitária; ou, ainda, à prevenção de fraudes contra o titular (art. 11, LGPD). Não há como deixar de notar que tais hipóteses tangenciam a noção de um legítimo interesse na utilização de dados pessoais sensíveis. Ainda assim, o legislador optou por não elencar tal hipótese no rol definido pelo art. 11, da LGPD.

4.3.4.3.1 – Medidas para aferir o legítimo interesse.

Tamanha dificuldade de se estabelecer limites para a configuração do legítimo interesse conduziu à formulação de quesitos, formulários ou testes para sua validação. É o exemplo do LIA (*legitimate interest assessment*) ou teste da ponderação – proposto para ser aplicado no contexto da GDPR – ou a avaliação em quatro etapas para o modelo brasileiro – conforme defendido por Bruno Bioni (2019), referenciado por este como teste de proporcionalidade.

O autor (BIONI, 2019) extrai uma prática e didática estruturação de questões a serem enfrentadas para aferir a legitimidade do interesse do agente para o tratamento de dados que pretende executar. Para tanto, realiza a estruturação dos dispositivos da LGPD em quatro etapas. A primeira examina a licitude do interesse e a delimitação da situação em concreto na qual se pretende exercer o tratamento. Trata-se da verificação da legitimidade do interesse do agente

de tratamento. Como segundo passo, o autor propõe avaliar se a necessidade do tratamento é pautada pela minimização dos dados a serem utilizados para alcançar o interesse (legítimo) pretendido e se há outras formas (bases legais) de legitimar o tratamento almejado.

Em terceiro lugar, o autor parte da interpretação sistemática da LGPD – de modo a conformar a boa-fé (art. 6º, I, da LGPD) à análise dos incisos do seu art. 10 – para concluir que o legítimo interesse do agente de tratamento deve ocorrer dentro das legítimas expectativas do titular, ou seja, o uso pretendido dos dados deve ser parametrizado tanto pela compatibilidade do interesse do agente quanto pelo contexto do uso pretendido dos dados frente à expectativa do titular. Nesse terceiro ponto, cabe questionar se há benefícios do tratamento ao titular ou em que extensão suas liberdades e direitos fundamentais são atingidos.

Em quarto lugar, a atenção volta-se para o fato de que o legítimo interesse não prescinde de medidas que salvaguardem os interesses do titular. Nesses termos, averiguado se ao titular foi conferida a opção de se opor à atividade (*opt out*), se foram adotadas as medidas para garantir a devida transparência do processamento de dados, se foi realizado o devido relatório de impacto à proteção de dados e se foram empregados meios aptos a mitigar os riscos do titular dos dados (como anonimização após o alcance da finalidade pretendida ou exclusão dos dados).

A avaliação em quatro etapas que formam o "teste de proporcionalidade" elaborado por Bruno Bioni pode se desdobrar em perguntas a serem realizadas tanto pelo agente de tratamento quanto pela Autoridade Nacional de Proteção de Dados ou pelo Poder Judiciário para aferir o legítimo interesse no qual um tratamento de dados. Com as devidas adaptações propõe-se a estruturação visual das quatro etapas em perguntas no seguinte formato:

1º. Verificação da legitimidade do interesse.	
Amparo legal: LGPD. Art. 10, *caput* e I.	
O interesse do controlador é amparado por uma finalidade legítima?	O interesse contraria outros comandos legais?
	Há benefícios ou vantagens que apoiem ou promovam as atividades do controlador?
A finalidade está bem articulada a uma situação concreta?	O enquadramento não pode configurar uma autorização para uso indiscriminado ou genérico dos dados.
2º. Avaliação da necessidade.	
Amparo legal: LGPD. Art. 10, §1º.	
Minimização: somente podem ser tratados os dados estritamente necessários para a finalidade pretendida.	Os dados são o único meio para atingir a finalidade pretendida?
	Há alternativas menos intrusivas ou outros meios para que o titular seja menos impactado?
3º. Balanceamento. Verificação do legítimo interesse perante as legítimas expectativas do titular	
Amparo legal: LGPD. Art. 10, II.	
Perspectiva do titular de dados.	A coleta de dados é esperada **ou** o tratamento é compatível com o uso que originou a coleta inicial dos dados?
	Há impactos positivos aos titulares?
	Quais são as repercussões negativas em termos de discriminação e cerceamento de sua autonomia?
4º. Adoção de Salvaguardas.	
Amparo legal: LGPD. Art. 10, §§2º e 3º.	
Transparência.	Quais medidas foram adotadas para garantir a transparência do tratamento de dados franqueado pelo legítimo interesse?
	É possível garantir ao titular o exercício de oposição a tal atividade (*opt out*)?
	Há relatório de impacto à proteção de dados elaborados previamente ao tratamento?
Minimização de riscos	É possível anonimizar os dados tratados?
	Quais medidas foram tomadas para mitigar os riscos ao titular de dados?

Tabela 10. Verificação do legítimo interesse em quatro etapas. Estruturação adaptada a partir da avaliação proposta por Bruno Bioni (2019, pág. 246 e 247). Elaborado pela autora.

Não se trata de uma fórmula estanque, mas de uma avaliação adaptável cujo detalhamento depende da vulnerabilidade e riscos de perfilização do titular frente ao tratamento de dados almejado.

4.3.4.3.2 – Casos exemplificativos de aplicação do legítimo interesse.

O site oficial do órgão independente criado para defender os direitos de informação do Reino Unido (ICO) elenca exemplos que facilitam a compreensão da aplicação do legítimo interesse. O ICO (*Information Comissioner's Office*)[46] equipara-se à Autoridade Nacional de Proteção de Dados do Brasil e tem por propósito assegurar direitos e o interesse público que digam respeito à tutela da informação. Em tradução livre e com comentários adicionais, cite-se três situações-exemplo.[47]

Na primeira, os interesses entre as partes (controlador e titular dos dados) são convergentes; na segunda, a necessidade do tratamento de dados relativiza o direito de um titular, mas é compatibilizada com a proteção de outros titulares por meio de ações de mitigação; por fim, na terceira, o interesse do controlador é legítimo, ainda que contraposto aos interesses do titular de dados:

1) Exemplo no qual o interesse das partes convergem.
Pretensão de uma empresa de seguros em monitorar pretensões fraudulentas por meio do processamento de dados pessoais. O propósito comercial é legítimo: visa garantir que seus clientes não sejam indenizados mediante alegações fraudulentas. O interesse dos demais clientes e do público em geral é compatível com a pretensão da controladora: garantir que fraudes sejam detectadas e prevenidas. Em última análise, evitar indenizações fraudulentas repercute no barateamento do custos com o seguro cobrado dos demais clientes.

[46] Disponível para acesso em: https://ico.org.uk/ Acesso em 24/04/2023.
[47] Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#what_counts Acesso em 24 de abril de 2023.

Legítimo interesse do controlador: evitar indenizações com base em alegações fraudulentas.

Expectativa legítima do titular: redução dos custos com seguro.

2) Exemplo no qual se revela a necessidade do tratamento de dados.

Uma figura política publica um vídeo em que denuncia a superlotação de ônibus e metrôs operados por determinada empresa particular, concessionária de serviço público. O vídeo ganha grande repercussão em diversos meios de comunicação.

A empresa particular responsável pelo transporte público pretende divulgar gravações de seu circuito fechado (câmeras de segurança) na qual figura a pessoa política autora da denúncia diante de vagões ou lugares vazios para contraditar os seus relatos de superlotação. Ocorre que a filmagem também inclui a imagem de outros passageiros.

Há o interesse legítimo da concessionária em divulgar as imagens como um direito de resposta a uma notícia que considera enganosa e potencialmente prejudicial à sua reputação e interesses comerciais, inclusive, mas não exclusivamente, diante do caráter a lesivo frente ao potencial ao interesse público do ente político responsável em renovar de seu contrato de concessão.

Para cumprir com essa pretensão, não se vislumbra outro meio senão a divulgação da gravação de passageiros para contraditar o que foi noticiado. No entanto, para dar sua versão dos fatos, bastaria a exposição da figura pública, mas não da identificação dos demais passageiros, que poderiam ser borrados ou desfocados e ainda assim cumprir com o propósito pretendido.

Legítimo interesse do controlador: exercer o direito de resposta.

Expectativa legítima do titular: dos demais passageiros, ter suas imagens desfocadas.

3) Exemplo no qual o interesse é legítimo, mas contraposto ao do titular.

Uma instituição financeira (como um banco) se vê diante de uma situação de inadimplência no pagamento de parcelas por um cliente que contratou seus serviços de financiamento. O consumidor não responde às tentativas de comunicação e tampouco é localizado na residência indicada no contrato. Não houve notificação à instituição financeira sobre um novo endereço ou contato telefônico. Na pretensão de cobrar as prestações vencidas e não pagas, o banco contrata e compartilha dados do titular com

agência de cobrança especializada. O interesse para cobrar a dívida é legítimo e o compartilhamento dos dados pessoais do cliente é necessário para atingir sua pretensão. É provável que os interesses da instituição financeira sejam contrários ao do cliente se este pretende, de fato, não ser localizado e se esquivar do pagamento do crédito adquirido. No entanto, o interesse da instituição financeira é legítimo e apto a admitir o compartilhamento dos dados com a agência de cobrança.

Legítimo interesse do controlador: realizar a cobrança do débito.
Expectativa do titular: contraposto ao da instituição financeira, mas não prevalente.

É relevante notar que as bases legais para o tratamento de dados representam, em grande medida, os deveres dos agentes de tratamento e os direitos dos titulares. A identificação dessas obrigações são essenciais para compor o quadro de tutela normativa dos dados pessoais. De toda forma, a LGPD dedica capítulo específico para disciplinar os direitos do titular de dados que devem ser observados para garantir a regular atividade de tratamento de dados pessoais (arts. 17 a 22) .

4.3.5 Direitos do titular de dados e deveres dos agentes de tratamento

Durante o tratamento de dados pessoais, tanto o operador como o controlador devem manter o respeito aos direitos do titular (arts. 17 a 22) e observar os princípios norteadores do tratamento de dados pessoais (art. 6º). Esses dispositivos reforçam a necessidade de cumprir com seus deveres não apenas no início do tratamento de dados (que em geral, inicia-se com a coleta de dados pessoais), como também durante o processamento e até mesmo com o término do tratamento de dados pessoais (art. 15 e 16).

Pela LGPD, o controlador de dados deve providenciar a confirmação da existência de tratamento ao titular de dados (art. 18, I, LGPD) e garantir o direito ao acesso facilitado a seus dados (art. 18, II e art. 9º, LGPD) mediante requisição em formato simplificado (art. 19, I, LGPD) ou por meio de declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até quinze dias, contado da data do requerimento do titular (art. 19, II, e art. 14, §2º, LGPD).

Da mesma forma, é dever do controlador, mediante requerimento do titular, informar as entidades com as quais compartilhou os seus dados (art. 18, VII, LGPD) e sobre a possibilidade

ou não de fornecer seu consentimento para o tratamento pretendido – bem como sobre as consequências de sua negativa (art. 18, VIII e art. 9º, §3º, LGPD). De forma correlata, é garantido ao titular de dados o direito de revogar, a qualquer tempo e de forma gratuita, o consentimento manifestado (art.18, IX e art. 8º, §5º) e o direito de oposição ao tratamento de dados não baseado no consentimento nas situações em que ocorra o descumprimento da norma ou seja possível o exercício de sua autonomia frente à pretensão do controlador (art. 18, §2º, LGPD).

Ao titular de dados também é garantido o direito à portabilidade de dados a outro fornecedor de serviço ou produto (art. 18, V), mediante sua expressa requisição e de acordo com a regulamentação da Autoridade Nacional. O direito à portabilidade de dados pessoais não inclui aqueles relativos aos segredos comercial e industrial ou aos dados que já tenham sido anonimizados pelo controlador (art. 18, §7º) uma vez que a própria LGPD não qualifica os dados anônimos como dados pessoais para efeitos de sua disciplina (art. 12, *caput*, LGPD).

O controlador deve promover a correção de dados incompletos, inexatos ou desatualizados do titular (art. 18, III) e providenciar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei (art. 18, IV). Ademais, é obrigação dos agentes de tratamento garantir a segurança da informação em relação aos dados pessoais (art. 47, LGPD) e adotar medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito (art. 46, *caput*) em atendimento aos padrões técnicos mínimos dispostos pela Autoridade Nacional (art. 46, §1º, LGPD) desde a fase de concepção até a execução (art. 46, §2º, LGPD) e término da relação nas quais os dados pessoais foram tratados (art. 47, LGPD).

Para garantir seus direitos, a LGPD chancela o direito de petição do titular dos dados pessoais perante o próprio operador ou controlador (art. 18, *caput*, LGPD), perante a Autoridade Nacional (art. 18, §1º, LGPD) e perante os organismos de defesa do consumidor (art. 18, §8º, LGPD). As disposições não excluem a legitimidade de atos institucionais como os do Ministério Público e de outras entidades vocacionadas à tutela de direitos transindividuais (direitos coletivos *lato sensu*), conforme reforça, para a esfera judicial, o art. 22, da LGPD, que garante que a defesa dos interesses e dos titulares de dados pode ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente à disciplina dos instrumentos de tutela individual e coletiva.

Note-se que os direitos do titular de dados não se esgotam com os previstos na LGPD. O quadro normativo que tutela os dados pessoais é pautado pelo diálogo das fontes e guiado

pelo princípio da tutela à dignidade da pessoa humana (art. 1º, III, da CF/1988). O diálogo das fontes acrescenta ao titular, a depender do contexto e circunstâncias fáticas, direitos e institutos protetivos previstos em normas distintas, como as elencadas no Código de Defesa do Consumidor (CDC), na Lei de Cadastro Positivo (LCP), no Marco Civil da Internet (MCI) e no Código Civil (CC). A tutela à dignidade da pessoa humana, por sua vez, direciona a ampla tutela da pessoa natural para além de disposições expressa na norma, de modo a garantir a efetiva existência digna de alguém tanto por uma perspectiva individual quanto coletiva,

O regime de responsabilidade civil aplica-se quando há uma suposta violação aos direitos do titular de dados. A comprovação do dano depende de diversos fatores, necessariamente aferíveis pela análise das circunstâncias do caso concreto. Isso porque o próprio ordenamento jurídico admite conformações e mitigações legítimas aos direitos albergados sob a tutela da dignidade da pessoa humana. Ademais, as consequências da atribuição de responsabilidade por violação aos direitos do titular não seguem a mesma lógica patrimonial clássica da mensurada pela diferença da situação de uma coisa antes e após o dano.

O reconhecimento da compensação de um dano aos direitos do titular não pode ser pautado por aspectos patrimoniais tendo em vista as características de inalienabilidade, indisponibilidade e irrenunciabilidade dos direitos da personalidade. No contexto de violação dos direitos ao titular de dados responsabilidade civil sobreleva a importância da análise da responsabilidade civil pautada por aspectos extrapatrimoniais cuja consequência envolve o reconhecimento ou não de um dano moral indenizável.

5. MITIGAÇÃO OU VIOLAÇÃO DOS DADOS PESSOAIS: DO DANO MORAL.

O dano moral é categoria constitucional de construção fundamentalmente jurisprudencial. Não há, na atual ordem jurídica brasileira, um conceito legal que destrinche seu conteúdo. Aliás, uma previsão legal que definisse seus contornos e incidência engessaria uma única perspectiva no tempo, em prejuízo à sua natural (e necessária) evolução (FARIAS, ROSENVALD, NETTO; 2023). Isso porque o início do reconhecimento da ressarcibilidade de um dano extrapatrimonial veio permeado de referências ao preço da dor e do sofrimento – *pretium doloris* – em uma lógica patrimonial incompatível com a ordem de proteção existencial de uma pessoa humana (SCHREIBER, 2015).

Herança de uma lógica patrimonial, essa compreensão afere a extensão do dano e do correspondente dever de indenizar pela teoria da diferença, ou seja, pela verificação de qual foi o valor deduzido do patrimônio inicial da vítima pela lesão provocada pelo agressor. Pela lógica da dor, segundo a teoria da diferença, a configuração do dano moral se confunde com a mensuração da assimetria entre os sentimentos manifestados anteriormente à lesão e os que se revelaram depois do dano injusto.

Ocorre que fatos prosaicos do cotidiano podem revelar dor, mágoa, sofrimento ou angústia para alguém, mas não representar grandes abalos para outra pessoa. Se o dano fosse aferido pela manifestação dor, uma pessoa extremamente sensível a fatos cotidianos teria mais legitimidade para requerer uma indenização do que aquela pessoa que não manifesta consternação pela experiência danosa vivenciada.

Ademais, a aproximação do dano moral ao sentimento de desprazer deslegitima o reconhecimento de lesões indenizáveis por indivíduos que transitória ou permanentemente não têm a aptidão de compreender uma situação lesiva ou manifestar seu pesar pela sua ocorrência – como o caso do nascituro, infantes, pessoas acometidas por deficiência intelectual ou por situações de inconsciência.

O pesar e a consternação não passam de sensações subjetivas, eminentemente pessoais e intransferíveis. O reconhecimento desse fato ampara a compreensão de que o dano moral indenizável "*não pressupõe necessariamente a verificação de sentimentos humanos desagradáveis como dor ou sofrimento*." (Enunciado nº 444, CNJ, V JDC).

O equívoco de vincular o reconhecimento do dano moral à comprovação da dor, decepção ou outros sentimentos desagradáveis recai na confusão entre causa e consequências de um dano. Os sentimentos negativos não passam de eventuais consequências de um dano moral – e não uma causa necessária para sua configuração.

A lógica de afetação extrapatrimonial é outra. A aproximação do dano moral a um modelo pautado pelo princípio da dignidade da pessoa humana demonstra que o dano moral surge objetiva e concretamente quando um bem jurídico existencial é afetado.

Por outro lado, compreender o dano moral como lesão à dignidade da pessoa humana é lógica que também se submete ao risco carregar tanto subjetivismo quanto à avaliação da dor. Em uma perspectiva, a tentativa de concretizar a avaliação do dano moral conduz à compreensão de que o bem jurídico existencial afetado se confunde com a ofensa a um direito da personalidade (como intimidade, honra ou privacidade). Isso porque os direitos da personalidade se manifestam como projeções da dignidade da pessoa humana. Não esgotam, mas materializam sua proteção. Por esse lógica, pautada pela verificação de uma transgressão a um direito da personalidade, seria mais viável, em tese, a aferição de um dano extrapatrimonial.

A lógica de verificação de um dano a partir da afetação de um valor abrangido pela dignidade da pessoa humana é válida. Ocorre que a materialidade de um dano se torna (mais) evidente a depender do caso analisado. A afetação física e psíquica de uma pessoa atropelada por um ilícito culposo, por exemplo, revela uma manifesta (e evidente) afetação ao direito da personalidade de uma vítima. No caso, ocorreu um dano à dignidade da pessoa humana, verificada pela lesão à sua integridade psicofísica, por uma causa que não se apresenta como justificativa para uma mitigação legítima. Por outro lado, a verificação de um dano ao direito à privacidade é mais nebulosa. Os limites para pautar um fato como uma transgressão ou uma mitigação válida pelo exercício de outro direito (como liberdade de expressão ou de imprensa) são tênues.

Para solucionar essa questão, deve ser feito o exame objetivo do fato, na ponderação da conduta supostamente lesiva e o interesse supostamente lesado. Para Cristiano Chaves, Nelson Rosenvald e Felipe Braga Netto (2023, pág. 354), é por meio desse exercício que restará evidenciado se há interesse existencial concretamente merecedor de tutela bem como será possível identificar se o caso revela um dano injusto (e reparável) ou um dano justificado a depender do resultado de proporcionalidade da colisão de direitos e bens jurídicos no caso concreto.

Ilustrativamente, com amparo no Enunciado 279, do CJF, a ofensa à dignidade e o dano à intimidade de alguém pela publicação de uma matéria jornalística exige o exame de uma série de variáveis tais como: 1) o interesse público da divulgação do fato; 2) da notoriedade do

ofendido; 3) da veracidade do fato e 4) da finalidade da publicação (informativa, comercial ou biográfica).[48]

De fato, não há como avaliar um dano moral indenizável sem considerar as circunstâncias peculiares. Não se trata, cabe ressaltar, de avaliar a extensão do sofrimento de alguém caso a caso. O exame objetivo de um fato exige a ponderação de aspectos contrapostos: de um lado, um interesse existencial supostamente lesado (a exemplo da privacidade) e, de outro, o exercício legítimo ou não um interesse contraposto (a exemplo da liberdade de imprensa). Somente a partir da análise das circunstâncias concretas (objetivas, ressalte-se) é possível aferir se houve um dano a um bem jurídico existencial ou se o caso caracteriza uma mitigação legítima desse direito.

Dano moral, portanto, é a violação a um direito existencial inerente à dignidade da pessoa humana aferido a partir da valoração em concreto das circunstâncias de um evento. Se da ponderação resultar a conclusão de que o alegado prejuízo configura, *in concreto*, em uma mitigação legítima do direito suscitado, não haverá dano a ser ressarcido.

5.1 Limitações constitucionais à privacidade e proteção de dados pessoais.

A cláusula geral de proteção da pessoa humana (art. 1º, III, da CF/1988) é um valor máximo do ordenamento jurídico capaz de moldar o exercício da autonomia privada e submeter a atividade econômica a novos critérios de validade. No entanto, em respeito ao texto constitucional, a cláusula de proteção da dignidade da pessoa humana e seus desdobramentos ou projeções (como os direitos da personalidade) não formam um reduto de poder do indivíduo – sob pena de se extrair uma perspectiva patrimonial desse paradigma de proteção humana. (TEPEDINO, 1999).

A proteção de dados pessoais, como projeção da dignidade da pessoa humana e direito fundamental e da personalidade, admite conformações e mitigações legítimas ao seu conteúdo – que não se traduzem em dano ao aspecto que visa proteger. Os dados pessoais, assim como a privacidade (BESSA, 2022), revelam-se como um direito e não um dever de seu titular. Em

[48] Enunciado 279, da IV Jornada de Direito Civil, do Conselho Nacional de Justiça: "*a proteção à imagem deve ser ponderada com outros interesses constitucionalmente tutelados, especialmente em face do direito de amplo acesso à informação e da liberdade de imprensa. Em caso de colisão, levar-se-á em conta a notoriedade do retratado e dos fatos abordados, bem como a veracidade destes e, ainda, as características de sua utilização (comercial, informativa, biográfica), privilegiando-se medidas que não restrinjam a divulgação de informações*."

outras palavras, conforme amparado pelo Superior Tribunal de Justiça[49], podem sofrer limitações voluntárias, desde que não permanentes ou gerais.

A tutela dos dados pessoais, portanto, pode sofrer mitigações legítimas de seu conteúdo de modo a afastar a conformação de um dano moral indenizável. Em primeiro lugar, tal direito pode ser limitado voluntariamente. Não há irregularidades em *postar* fotos em plataformas de redes sociais ou participar de programas de *reality show* que envolvam a vigilância de participantes. A disposição do direito é voluntária e, nesses casos, lícita.

Em segundo lugar, o conflito entre a tutela aos dados pessoais com exercício de outros direitos fundamentais admite sua solução com técnicas de ponderação e limitações recíprocas. A preponderância de um em detrimento de outro em determinado caso concreto não configura dano indenizável se pautado pelas regras hermenêuticas apontadas. (MENDES, 2018)

Em terceiro lugar, a própria lei pode prever hipóteses que admitem a mitigação do direito à proteção dos dados pessoais – a exemplo do dever de divulgação compulsória de dados pessoais de servidores, como nome e remuneração, amparado no art. 7º, §3º, VI, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (LAI).

Cabe acrescentar que o enunciado 139 da Jornada de Direito Civil sustenta que os direitos da personalidade também podem sofrer limitações ainda que não especificamente previstas em lei, desde que não exercidas com abuso de direito do titular, contrariamente à boa-fé objetiva e aos bons costumes – trata-se de hipótese pautada pelo disposto no art. 187 do Código Civil, o qual prevê que o exercício abusivo de um direito configura ato ilícito.

Para reforçar a legitimidade dessas limitações, são detalhadas limitações constitucionais dos direitos à privacidade e à proteção dos dados pessoais reconhecidas pela jurisprudência, em especial: o não reconhecimento de um direito ao esquecimento, a liberdade de imprensa, a exploração econômica e a diferença entre as atribuições do dever de fornecer dados pessoais por provedores de internet.

5.1.1 Direito ao esquecimento

O direito ao esquecimento é entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em veículos de comunicação social (seja em meio analógico ou digital). Ainda que defendido por

[49] É o que afirma a tese 1, da Jurisprudência em Teses, edição nº 137 - Direitos da Personalidade – I. Disponibilizada em 14/11/2019. . Disponível em: https://processo.stj.jus.br/SCON/jt/doc.jsp?livre=%27137%27.tit. Acesso em 16/03/2023.

alguns setores – como no caso do superado Enunciado nº 531, da Jornada de Direito Civil, que dispõe que "*A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento*" –, o Supremo Tribunal Federal declarou a incompatibilidade do direito ao esquecimento com o ordenamento jurídico constitucional. Trata-se de tema reconhecido em recurso afetado de repercussão geral, cuja tese, de nº 786, afirma que:

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais - especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral - e as expressas e específicas previsões legais nos âmbitos penal e cível.
> (STF. RE 1010606. Rel. Min. Dias Toffoli. Julgado em 11/02/2021, DJe 20/05/2021. Tema de Repercussão Geral nº 786).

Exemplo elucidativo para representar situações aos quais se buscou a invocação de um direito ao esquecimento se refere ao caso de programas de televisão que tratam de crimes notáveis. Ainda que a pedido de familiares da vítima ou do autor do crime – ou seja, mesmo de pessoas que não estejam diretamente envolvidas no fato criminoso, mas por ela afetados emocional ou socialmente –, não há a possibilidade de proibir, de forma prévia, a veiculação de informações de fatos do gênero, ainda que revele dados pessoais dos envolvidos (ou seja, que exponham ou identifiquem indivíduos vinculados a uma situação socialmente repreensível). Eventual abuso na exposição de alguém deverá ser tratado na forma de demandas ressarcitórias ou com a imposição de retratação (mas não, reitera-se, com uma prévia proibição de veiculação).

A liberdade de informação não é desmedida. Tal como qualquer direito fundamental, não é absoluta. A título de exemplo, o STJ define que é possível a determinação de que provedores de busca na internet procedam a desvinculação do nome de determinada pessoa, com fato desabonador a seu respeito dos resultados de pesquisa, desde que não haja o emprego de qualquer outro termo que especifique tal busca. Tal cenário não se confunde com o reconhecimento de um direito ao esquecimento (Informativo 743. STJ. Terceira Turma. Processo em segredo judicial, julgado em 21/06/2022, DJe 30/06/2022).

Nota-se que o caso não se trata de uma obrigação de excluir conteúdo informativo[50], pois a busca de um nome associado a evento ou tema específico ainda torna possível a apresentação de resultados com informações do sujeito, ainda que desabonadoras.

5.1.2 Liberdade de imprensa.

O STJ reconhece que a ampla liberdade de informação, opinião e crítica jornalística não compõem um direito absoluto. Há limitações, tais como a preservação dos direitos da personalidade, nestes incluídos os diretos à honra, imagem, privacidade e intimidade.[51] A jurisprudência recomenda que, sopesados valores em conflito, é recomendável, em regra, a prevalência à liberdade de expressão e de crítica (especialmente quanto às pessoas investidas de autoridade pública). Tal prevalência não configura uma exclusão de direitos da personalidade, mas sim uma limitação legítima desde que protegido seu núcleo essencial, sob pena de configurar abuso de direito (STJ. AgInt no AREsp 862410/SP. Rel. Min. Raul Araújo, julgado em 12/12/2022, DJe 14/12/2022). No mesmo sentido, decidiu o STJ que:

> não constitui ato ilícito apto à produção de danos morais a matéria jornalística sobre pessoa notória a qual, além de encontrar apoio em matérias anteriormente publicadas por outros meios de comunicação, tenha cunho meramente investigativo, revestindo-se, ainda, de interesse público, sem nenhum sensacionalismo ou intromissão na privacidade do autor**.**
> O embate em exame revela, em verdade, colisão entre dois direitos fundamentais, consagrados tanto na CF quanto na legislação infraconstitucional: o direito de livre manifestação do pensamento de um lado e, de outro lado, a proteção dos direitos da personalidade, como a imagem e a honra. [...] é inconteste também que as notícias cujo objeto sejam pessoas notórias não podem refletir críticas indiscriminadas e levianas, pois existe uma esfera íntima do indivíduo, como pessoa humana, que não pode ser ultrapassada.
> De fato, as pessoas públicas e notórias não deixam, só por isso, de ter o resguardo de direitos da personalidade. Apesar disso, em casos tais, a apuração da responsabilidade civil depende da aferição de culpa sob pena de ofensa à

[50] Nesse sentido, afirma o STJ que "o direito ao esquecimento não justifica a exclusão de matéria jornalística. O Supremo Tribunal Federal definiu que o direito ao esquecimento é incompatível com a Constituição Federal (Temma 786). Assim, o direito ao esquecimento, porque incompatível com o ordenamento jurídico brasileiro, não é capaz de justificar a atribuição da obrigação de excluir a publicação relativa a fatos verídicos." STJ. 3ª Turma. REsp 1.961.581-MS, julgado em 07/12/2021, DJe 13/12/2021 (Info 723).

[51] STJ. Jurisprudência em Teses, edição nº 137 - Direitos da Personalidade – I. Tese nº 3. Disponibilizada em 14/11/2019. Disponível em: https://processo.stj.jus.br/SCON/jt/doc.jsp?livre=%27137%27.tit. Acesso em 16/03/2023. No mesmo sentido e mesma edição, dispõe a Tese nº 4 que "*no tocante às pessoas públicas, apesar de o grau de resguardo e de tutela da imagem não ter a mesma extensão daquela conferida aos particulares, já que comprometidos com a publicidade, restará configurado o abuso do direito de uso da imagem quando se constatar a vulneração da intimidade ou da vida privada*."

> liberdade de imprensa. REsp 1.330.028-DF, Rel. Min. Ricardo Villas Bôas Cueva, julgado em 6/11/2012.

O STJ sustenta que, desde que não se refira ao núcleo essencial de intimidade e de vida privada da pessoa, a divulgação de notícia ou crítica acerca de atos ou decisões do Poder Público ou de comportamento de seus agentes – como a de um magistrado[52] –, não configuram, a princípio, abuso no exercício da liberdade de imprensa. É o abuso no exercício da liberdade de expressão jornalística que é passível de ensejar a reparação civil por dano moral e, inclusive, de configurar crime contra honra se verificada a intenção de difamar, injuriar ou caluniar.[53]

Cabe notar que o intuito de difamar, injuriar ou caluniar é determinante, inclusive, na análise de ocorrência de abuso no exercício da liberdade de expressão. Não se proíbe a utilização de dados pessoais para expressão jornalística ainda que de forma crítica ou irônica. Sobreleva, portanto, a importância do exame do caso concreto, para o qual a finalidade se mostra determinante para verificar a ocorrência de abuso no exercício de direitos.

A diferença de consequências jurídicas a partir da identificação da finalidade na análise do caso concreto é evidenciada no caso de emprego de imagens. A utilização de imagem de uma pessoa para fins jornalísticos não exige autorização, diferentemente da finalidade para uso econômico ou comercial, situação na qual a indenização por publicação não autorizada independe da prova do prejuízo, ao que se refere como *dano in re ipsa*, nos termos previstos na súmula 403, do STJ: *independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais*." Reforça essa distinção a Tese nº 6 e nº 7, do Jurisprudência em Teses, do STJ, que dispõem, respectivamente, que:

> Tese 6: às pessoas públicas, apesar de o grau de resguardo e de tutela da imagem não ter a mesma extensão daquela conferida aos particulares, já que comprometidos com a publicidade, restará configurado o abuso do direito de uso da imagem quando se constatar a vulneração da intimidade ou da vida privada.
> Tese 7: a publicidade que divulgar, sem autorização, qualidades inerentes a determinada pessoa, ainda que sem mencionar seu nome, mas sendo capaz de identificá-la, constitui violação a direito da personalidade. (Enunciado n. 278 da IV Jornada de Direito Civil do CJF)".
> (STJ. Jurisprudência em Teses, edição nº 137 - Direitos da Personalidade – I. Tese nº 6 e 7, respectivamente.

[52] STJ. Quarta Turma. REsp 1.325.938-SE, julgado em 23/08/2022, (Info 749)
[53] STJ. Jurisprudência em Teses, edição nº 130 – Dos Crimes Contra a Honra. Tese nº 8. Disponibilizada em 09/08/2019. Disponível em: https://processo.stj.jus.br/SCON/jt/toc.jsp?livre=@docn=000006530#TEMA8. Acesso em 16/03/2023.

Disponibilizada em 14/11/2019. Disponível em: https://processo.stj.jus.br/SCON/jt/doc.jsp?livre=%27137%27.tit. Acesso em 16/03/2023.)

Nesses termos, ainda que haja limites jurisprudenciais à liberdade de imprensa, seu exercício, em tese e em abstrato, prepondera quando em confronto com direitos relacionados ao sigilo ou resguardo do indivíduo. Trata-se de outro exemplo de mitigação de um aspecto tutelado pelo direito de proteção aos dados pessoais.

5.1.3 Divulgação voluntária para exploração econômica de dados pessoais.

O STJ compreende que a voz entra proteção nos direitos da personalidade, seja como direito autônomo ou como parte integrante do direito à imagem ou do direito à identidade pessoal.[54] No entanto, essa característica, por si só, não afasta a possibilidade de sua exploração comercial. O Tribunal Superior reconhece a possibilidade e validade do negócio jurídico que tenha por objeto a gravação de voz, desde que autorizada (ainda que de forma tácita) pelo titular e utilizada dentro dos limites contratuais (STJ. REsp 1.630.851-SP, Rel. Min. Paulo de Tarso Sanseverino, julgado em 27/4/2017, DJe 22/6/2017).

No mesmo sentido da Súmula 403, do STJ, que reconhece o dever de indenizar pelo uso não autorizado de imagem de pessoa empregada para fins comerciais, o STJ também afirma que a publicidade que divulgar, sem autorização do titular, qualidades inerentes a determinada pessoa que permitam a sua identificação, ainda que sem mencionar seu nome, constitui violação a direito da personalidade (STJ. Jurisprudência em Teses, edição nº 137 - Direitos da Personalidade – I. Tese nº . 8. Disponibilizada em 14/11/2019).

Os fins comerciais ou econômicos para exploração de aspectos da personalidade (como a voz e os dados pessoais) são, portanto, permitidos. Esse aspecto reforça que a privacidade e a proteção dos dados pessoais são um direito, mas não um dever de seu titular. Não há caráter absoluto dos direitos fundamentais e da personalidade. Os parâmetros para seu emprego, no entanto, são mais exigentes e as consequências mais rigorosas – em especial no contexto de uso de informações pessoais sensíveis ou de menores. Nesse sentido, por exemplo, o STJ define que o uso não autorizado da imagem de menores de idade gera dano moral *in re* ipsa (STJ.

[54] STJ. Jurisprudência em Teses, edição nº 138 - Direitos da Personalidade – II. Tese nº . 3. Disponibilizada em 29/11/2019. Disponível em: https://processo.stj.jus.br/SCON/jt/doc.jsp?livre=%27137%27.tit. Acesso em 16/03/2023.

Jurisprudência em Teses, edição nº 137 - Direitos da Personalidade – I. Tese nº . 9. Disponibilizada em 14/11/2019).

Cabe citar, conforme elucidativa lição de Leonardo Bessa (2011, pág. 49), que a "*autonomia, a possibilidade de escolhas do indivíduo em busca da felicidade integra o conteúdo da dignidade da pessoa humana. A privacidade, nessa linha, deve ser concebida com a possibilidade de limitar algumas informações pessoais e não o dever de manter esses dados sob restrição*." Não há, portanto, uma proibição geral de utilização de dados pessoais. O direito de não exercer um direito também é garantido ao seu titular.

Há, no entanto, parâmetros que devem ser observados. Não se admite a limitação voluntária de um direito a ponto de gerar a sua supressão total ou a abstenção geral e irreversível desse direito. No limite, eventual consentimento ou divulgação voluntária não abre espaço para uma utilização desmedida, eterna ou fora dos propósitos inicialmente autorizados.

5.1.4 Fornecimento de dados pessoais por provedores de internet.

A Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, contempla cláusulas gerais e princípios de conformação de direitos individuais no âmbito do ciberespaço que servem como bases hermenêuticas para o Poder Judiciário. Dentre a ampla gama de possibilidades ampliadas pela internet tanto para a realização de garantias constitucionais como para a concretização de direitos fundamentais, o panorama jurídico geral e hermenêutico do MCI volta-se ao amparo dos provedores de internet, sob o argumento de tutela constitucional da liberdade de pensamento e de expressão. Desse modo, grande parte da tutela à privacidade e aos dados pessoais garantidos por esse diploma normativo se voltam ao aspecto negativo de sua compreensão, ou seja, ao resguardo do sigilo, ao anonimato, à restrição de acesso aos dados de seus usuários.

Mesmo nesse contexto, o Superior Tribunal de Justiça reconhece a legitimidade da mitigação desses direitos. Para o Tribunal Superior, os provedores da internet, sejam os de conexão ou os de aplicação, são obrigados a guardar os dados pessoais de seus usuários por um tempo determinado. Aos provedores de *conexão* à internet, cumpre a guarda de dados pessoais do usuário como nome, endereço, RG e CPF. Quanto aos provedores de *aplicações* de internet, é exigida a guarda dos dados de conexão (nestes incluídos o respectivo endereço de IP).

Os provedores de conexão à internet (também conhecidos como provedores de acesso) são aqueles que oferecem "*a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP*" (art. 5º, V,

MCI). No Brasil, a grande maioria dos provedores de conexão acabam se confundindo com os prestadores de serviços de telecomunicações que, em conjunto, detêm a maior parte da participação desse mercado, tais como a Claro, GVT, Vivo, Oi e TIM. Há um dever jurídico dos provedores de conexão em armazenar os dados cadastrais de seus usuários durante o prazo de prescrição de eventual ação de reparação civil (STJ. 3ª Turma. REsp 1622483/SP, Rel. Min. Paulo de Tarso Sanseverino, julgado em 15/05/2018). Os dados pessoais, nesse caso, referem-se à identificação do usuário, como nome, endereço, RG e CPF.

Os provedores de aplicações de internet, por outro lado, compreendem as empresas que oferecem um "*conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet* " (art. 5º, VII, MCI). São provedores de aplicações aqueles que, com ou sem fim lucrativo, organizam-se para o fornecimento de funcionalidades na internet, tais como serviços de e-mail, redes sociais, compartilhamento de vídeos ou de imagens ou de hospedagem e armazenamento de dados – a exemplo de empresas como Meta (antigo Facebook), Instagram e YouTube.

Para o STJ, os provedores de aplicações de internet não são obrigados a guardar e fornecer os dados pessoais dos usuários, mas devem propiciar meios para que se possa identificar cada um deles, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Para cumprir com essa obrigação, é suficiente que o fornecedor guarde e forneça, quando exigido judicialmente, o número de IP correspondente à publicação ofensiva indicada pela parte. (STJ. 3ª Turma. REsp 1829821-SP, Rel. Min. Nancy Andrighi, julgado em 25/08/2020 – Info 680).

É interessante notar que o STJ afirma que o endereço de IP não é um dado pessoal, a despeito de reconhecer que se trata de um elemento que pode auxiliar na identificação do usuário cadastrado na plataforma do provedor de conteúdo (o que, em tese, coincide com a classificação do art. 5º, I, da LGPD):

> 3. **Ainda que não exija os dados pessoais dos seus usuários**, o provedor de conteúdo, que registra o número de protocolo na internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de internet.
> 4. A jurisprudência deste Superior Tribunal de Justiça é consolidada no sentido de - **para adimplir sua obrigação de identificar usuários** que eventualmente publiquem conteúdos considerados ofensivos por terceiros - **é suficiente o fornecimento do número IP** correspondente à publicação ofensiva indicada pela parte.

> (STJ - REsp: 1829821 SP 2019/0149375-4, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 25/08/2020, T3 - TERCEIRA TURMA, Data de Publicação: DJe 31/08/2020) – grifos da autora.

Pelas disposições da LGPD, o endereço de IP é considerado um dado pessoal pois pode tornar uma pessoa identificável (art. 5º, I, LGPD). No mesmo sentido, a Comissão Europeia de Proteção de Dados (Parecer 4/2007 – 01248/07/PT, WP 136) considera os endereços de IP como dados pessoais justamente pelo fato de que o tratamento de dados desses endereços são realizados com o objetivo de identificar aqueles que utilizaram um computador para inserir conteúdos considerados ofensivos ou que violem direitos de propriedade intelectual.

Por outro lado, cabe considerar que o endereço de IP nem sempre é o suficiente para permitir a identificação do usuário. Há , como exemplo, situações em que o suposto agressor utiliza um computador de uma *lan-house* ou de um cibercafé nos quais a identificação do cliente não é uma exigência. Nesses casos, se não há meios razoáveis para identificação do usuário, tais dados não seriam qualificados como pessoais. Parece ser a opção adotada pelo Tribunal Superior.

De toda forma, o STJ considera que, uma vez presentes indícios de ilicitude na conduta de usuário que, por exemplo, insere vídeos no YouTube com ofensas à memória de uma pessoa falecida, a privacidade do usuário, no caso concreto, não prevalece. Nesse caso, o Tribunal reconheceu que é possível a mitigação desse direito fundamental para possibilitar, mediante ordem judicial, a obtenção de dados para futura (e eventual) responsabilização pessoal de usuários responsáveis pela divulgação de fatos ofensivos e inverídicos:

> 5. Nesse contexto, **havendo indícios de ilicitude** e em se tratando de pedido específico voltado à obtenção dos dados cadastrais (como nome, endereço, RG e CPF) dos usuários cuja remoção já tenha sido determinada - a partir dos IPs já apresentados pelo provedor de aplicação -, **a privacidade do usuário não prevalece**.
> (STJ - REsp: 1914596 RJ 2021/0002643-4, Relator: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 23/11/2021, T4 - QUARTA TURMA, Data de Publicação: DJe 08/02/2022) – grifos da autora.

Em síntese, no âmbito do dever de guarda de dados pessoais de acordo com as categorias de provedores (de acesso e de aplicação), é consolidado o entendimento de que a proteção de dados pessoais, em sua perspectiva de sigilo, pode ser mitigada mediante ordem judicial em caso de ofensa a direitos de outrem. As obrigações de guarda de cada categoria de provedor, no entanto, são diferentes quanto ao tipo de dado que deve ser armazenado, conforme sintetizado pelo quadro a seguir:

Dever de guarda de dados pessoais por Provedores de Internet. Segundo o STJ.	
Provedor de Conexão (ou de Acesso)	**Provedor de Aplicações**
SIM. Devem guardar dados pessoais.	NÃO. Dispensados do dever de guarda de dados pessoais, basta armazenarem o IP (*cabe a ressalva de que tais dados podem ser considerados pessoais a depender da perspectiva de análise*).
Dever de guarda de dados pessoais do usuário (nome, endereço, RG e CPF)	Dever de guarda de dados de conexão (incluído o respectivo endereço de IP).
Devem armazenar dados cadastrais pelo prazo de prescrição de eventual ação de reparação civil e devem fornecer dados cadastrais de usuários que cometam atos ilícitos.	Devem coibir o anonimato e atribuir a cada manifestação uma autoria certa e determinada. (STJ. 3ª Turma. REsp 1829821-SP. Info 680).
Art. 5º, V (MCI): oferecem a habilitação de um terminal para o envio e recebimento de pacotes de dados pela internet, mediante atribuição ou autenticação de um endereço de IP.	Art. 5º, VII (MCI): empresas que oferecem um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.
No Brasil, confundem-se com os prestadores de serviços de telecomunicações.	São exemplos de funcionalidades oferecidas: serviços de e-mail; redes sociais; compartilhamento de vídeos.
Ex.: VIVO, Claro, TIM, GVT.	Ex.: Meta (antigo Facebook); Instagram; Youtube.

Tabela 11 - Diferença entre os deveres de guarda de dados pessoais das categorias de Provedor de Internet. Elaborado pela autora.

Cabe reiterar que o STJ compreende que provedores de aplicações não são obrigados à guarda de dados pessoais, apenas ao endereço de IP. Por outro lado, é legítimo considerar o próprio endereço de IP como dado pessoal, especialmente diante de sua aptidão para identificar uma pessoa natural, conforme as disposições da própria LGPD (art. 5º, I) e os padrões internacionais publicados, como exemplo, pela Comissão Europeia de Proteção de Dados Pessoais

Importante apontar que o tema de responsabilidade dos provedores deve ser afetado pela difusão de modelos de tecnologia que podem criar novos dados com base em padrões e estruturas de dados já existentes, as denominadas Inteligências Artificiais generativas, como o *Chat GPT*, lançado pela empresa OpenAI em 2022.[55] No caso, diferente de plataformas de relações sociais (como o Facebook ou Instagram) é a própria plataforma que cria o conteúdo – e não os usuários desses aplicativos. Nesse sentido, a qualidade dos dados tratados é

[55] Disponível em: https://www.conjur.com.br/2023-jun-21/campos-badaro-uso-ias-generativas-setor-publico . Acesso em 12/07/2023.

determinante para os resultados apresentados por um programa de IA generativa. Essa forma de produção e difusão de conteúdo deve ser aprofundada, para verificar a possibilidade de seu enquadramento como provedor de conteúdo ou de conexão ou outro posicionamento adequado para eventuais danos causados por essa tecnologia.

5.2 Da afetação do estado anímico e do dano *in re ipsa*.

A inobservância dos deveres associados ao tratamento dos dados do titular faz nascer a pretensão de reparação dos potenciais danos causados e de fazer cessar imediatamente a ofensa perpetrada aos direitos da personalidade. Para aferir a existência do dano extrapatrimonial, tribunais e parte da doutrina declaram que o dano moral é *in re ipsa*, ou seja, que deriva do próprio fato ofensivo de modo que, provada a ofensa, *ipso facto*, restaria presumido o dano moral, dispensando-se a prova de sua existência (Cavalieri, 2021).

Para Cristiano Chaves, Nelson Rosenvald e Felipe Braga Netto (2023), o dano moral só pode ser presumido quanto às consequências variáveis subjetivas da vítima (dor, mágoa), mas não sobre a demonstração da existência do próprio dano extrapatrimonial, o qual deve ser aferido pela ponderação entre a conduta supostamente lesiva e o interesse alegadamente lesado. A dificuldade de comprovação da materialidade do dano (como ofensa à intimidade ou à integridade psicofísica) não dispensa o autor do ônus probatório do próprio dano sofrido.

A fórmula do dano *in re ipsa*, se interpretada como uma comprovação do próprio dano, revela um apego à noção de que o dano moral decorre de uma percepção subjetiva do ofendido, em um nítido desvio de perspectiva entre a causa (lesão a um interesse existencial) e a consequência (dor, mágoa, tristeza). Em outras palavras, se o dano *in re ipsa* é invocado para presumir sentimentos ruins de pessoa causados por um fato supostamente lesivo, haverá uma confusão entre a causa e consequência que deturpa a análise da existência do próprio dano. Nas palavras dos autores (CHAVES, ROSENVALD, BRAGA NETTO; 2023; pág. 352):

> A desnecessidade da demonstração da dor, mágoa ou de qualquer outra forma de lesão à suscetibilidade da vítima não deve ser motivado no fato do dano moral ser presumido por uma lesão à dignidade, porém pelo fato de que aquele sentimento não passa de eventuais consequências de um dano moral, pois este se traduz na própria lesão ao interesse existencial concretamente merecedor de tutela.

Nessa linha de raciocínio, é criticável o entendimento fixado pelo Superior Tribunal de Justiça que compreende que o vazamento de dados pessoais não gera dano *in re ipsa*:

> 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 moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.
> (STJ - AREsp: 2130619 SP 2022/0152262-2, Data de Julgamento: 07/03/2023, T2 - SEGUNDA TURMA, Data de Publicação: DJe 10/03/2023)

De fato, não é o vazamento em si que comprova um dano moral, mas a ponderação concreta e dinâmica dos interesses contrapostos que demonstrem a ocorrência uma efetiva violação a um direito existencial (e não de uma mitigação legítima). Os sentimentos da vítima não passam de eventuais consequências do dano moral. Ocorre que os fundamentos utilizados pelo Tribunal Superior nesse representativo julgado representativo são questionável sob diversos aspectos.

Em primeiro lugar, o STJ afirma que dados de natureza comum (art. 5º, I, LGPD) não são íntimos. Uma vez não acobertados pelo sigilo (como nome, endereço ou CPF), não poderiam violar o direito da personalidade das vítimas. Ocorre que, sob a perspectiva de uma garantia à democracia moderna, a proteção aos dados pessoais incentiva o desenvolvimento de uma tutela voltada ao "devido processo informacional" (BIONI; MARTINS, 2020) o qual abrange a definição de limites da personalização no tratamento de dados (para evitar abusos ou discriminações) e empoderamento do cidadão contra ações arbitrárias e kafkianas do Estado ou outros entes com poderes em dimensões desproporcionais ao do titular dos dados. O dever de mitigar assimetrias de poder, nesse sentido, independe da classificação dos dados pessoais como sigilosos ou não.

Em segundo lugar, a Corte sustenta que apenas os dados sensíveis seriam merecedores de tutela apta a ensejar dano moral presumido. Essa hierarquização entre dados "comuns" e sensíveis, apesar de útil a demonstrar, *a priori,* riscos maiores para determinadas categorias de dados (art. 5º, I e II, LGPD) não pode conduzir a uma banalização de dados pessoais pelos simples fato deles serem considerados "comuns". Essa base argumentativa reforça a noção de que a tutela de dados se restringe ao resguardo do sigilo de informações, baseada na superada proteção baseada na dicotomia pautada pela informação pública *vs*. privada.

Em terceiro lugar, o STJ exigiu prova da utilização indevida dos dados por terceiros. No entanto, o dano aos dados pessoais, na sociedade contemporânea, é muitas vezes despercebido pela própria vítima ou por ela tomado como insignificante. Isso incentiva ações desidiosas e até mesmo criminosas, que seguem impunes frente às suas ações. Não se quer dizer com isso que

qualquer vazamento de dados gera, necessariamente, dano moral aos envolvidos. É possível que um tribunal considere a inexistência de potencial danoso pelo vazamento (caso os dados sejam criptografados, por exemplo) ou mesmo que o fato seja inerente às sujeições da vida em sociedade (ou seja, um mero aborrecimento). Ocorre que essa conclusão deve ser pautada *in concreto* pela análise da potencial violação do dever de segurança pelo agente de tratamento e não pela incumbência à vítima para fazer prova leonina tanto do autor do dano (que pode ser o hacker ou quem adquiriu os dados vazados) como da violação sofrida (como uma perfilização da qual sequer terá conhecimento).

Ademais, a compreensão do dano *in re ipsa* como demonstração de sofrimento pelo próprio fato ampara decisões ainda pautadas pela necessidade de comprovação da dor, nervosismo ou mesmo pelo choro para possibilitar a condenação por dano moral, conforme se verifica da seguinte ementa:

> 1. Considera-se praticado o dano moral quando uma pessoa se revelar afetada em seu ânimo psíquico, moral ou intelectual, seja por ofensa à sua honra, na sua privacidade, intimidade, imagem, nome ou em seu próprio corpo físico.(...).
> 3. A angústia da vítima restou comprovada pelos depoimentos testemunhais, que informaram que a autora ficou abalada, nervosa, abatida e chorou muito, sendo caracterizados os danos morais, pois o tratamento dirigido pela requerida à autora evidencia o abalo aos direitos da personalidade desta, não somente pelas palavras, mas também pelo constrangimento perante terceiros em seu local de trabalho."
> TJDFT. Acórdão 1345366, 07074499520208070001, Relatora: LEILA ARLANCH, 7ª Turma Cível, data de julgamento: 2/6/2021, publicado no DJE: 2/7/2021.

Como sustentado, pautar o dano moral pela comprovação de afetação do estado anímico de alguém evidencia um desvio de perspectiva que considera uma consequência (sofrimento) como a causa do dever de compensar (dano moral).

Nota-se uma resistência pela jurisprudência (ainda que não consolidada) em compreender a violação do que atualmente se compreende por proteção de dados pessoais (proteção à aspectos existenciais do indivíduo), em contraposição à farta tutela aos conceitos tradicionais de privacidade, compreendidos como sigilo, intimidade ou resguardo da vida privada. É o caso enfrentado a respeito da instalação de câmaras direcionadas para o imóvel vizinho, que gravou o interior de sua residência e, por constatar violação ao direito de sigilo ou intimidade (no sentido de resguardo da vida privada), foi dispensada maiores provas de afetação da personalidade da vítima (como vexame ou constrangimento):

> Danos morais – relação de vizinhança – câmeras de segurança – gravação do interior do imóvel vizinho – violação da intimidade e privacidade
> 2. Diante da análise dos elementos probatórios coligidos aos autos é possível observar que o apelante instalou câmeras de vigilância em sua residência, voltadas para a área externa ao imóvel, com o intuito de obter, principalmente, a gravação da rua, assegurando, com isso, mais segurança em sua residência. Ocorre que uma das câmeras foi direcionada não apenas para a rua, mas também para o interior do imóvel vizinho, local de residência do apelado.
> 3. Com efeito, embora a instalação de câmeras de segurança em imóvel seja, em regra, hipótese de exercício regular de direito (art. 188, inc. I, do Código Civil), é certo que no presente caso foi constatada a violação ao direito à intimidade do recorrido.
> 3.1. **No caso, verifica-se que o apelante abusou do exercício de seu direito, uma vez que a aludida gravação atinge a esfera jurídica extrapatrimonial do apelado.** Por isso, deve-se conferir maior peso à preservação dos aspectos inatos à personalidade (art. 12 do Código Civil).
> 4. Convém ressaltar que o art. 5º, inc. X, da Constituição Federal erigiu alguns desses aspectos como direito fundamental, tendo enunciado que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas".
> 4.1. Em situações como a presente o próprio Texto Constitucional possibilita a condenação ao pagamento de indenização pelo "dano material ou moral decorrente de sua violação", como estabelece o aludido art. 5º, inc. X, da Constituição Federal.
> TJDFT. Acórdão 1399242, 07159102220218070001, Relator: Alvaro Ciarlini, 2ª Turma Cível, data de julgamento: 9/2/2022, publicado no DJE: 8/3/2022. – grifos da autora.

Cabe notar que a decisão acima, de relatoria do Exmo. Álvaro Ciarlini, realiza a ponderação de interesses para aferir o dano a interesse existencial, pois contrapõe o exercício regular de um direito (instalação de câmeras de segurança em imóvel) em face do grau de afetação do direito à intimidade da outra parte. Em outras palavras, o dano moral, no caso, não é *in re ipsa*, mas pautado pela análise circunstancial, concreta e dinâmica dos interesses contrapostos. Essa postura tem maior amparo para manter a coerência e segurança jurídica nas decisões a respeito do reconhecimento do dano moral. Ocorre que, atualmente (21 de maio de 2023), ainda não verificam decisões no mesmo sentido ou com a mesma técnica de ponderação para amparar violações aos dados pessoais de um indivíduo.

Nessa linha, a crítica ao reconhecimento do dano *in re ipsa* também recai sobre a simplificação de uma análise que deveria ser dinâmica. Ao invés de conferir coerência nas decisões, acaba por engessar posicionamentos que utilizam desse argumento como subterfúgio tanto para reconhecer o dano moral como para afastar a necessidade de realizar uma ponderação de interesses contrapostos de acordo com as circunstâncias de um caso concreto.

PARTE II – RESPONSABILIDADE CIVIL E PROTEÇÃO DE DADOS PESSOAIS.

6. NATUREZA JURÍDICA DA RESPONSABILIDADE CIVIL NA LGPD.

O propósito da responsabilidade civil é estabelecer requisitos para definir quem deve arcar com os danos inerentes do convívio social. A noção naturalística do *neminem laedere*, suscitada como fundamento para estabelecer a lógica do instituto da responsabilidade civil, traduz a ideia de que aquele que causa um dano tem o dever de repará-lo. No entanto, a regra do cotidiano é que as pessoas arquem com os próprios prejuízos ou cheguem a um acordo sobre uma compensação pelos danos sofridos.

Para imputar a alguém o dever de suportar o prejuízo de outra pessoa, é preciso que a norma jurídica prescreva requisitos ou elementos para que a uma pessoa seja imposto o dever de arcar com prejuízo alheio. Afinal, pelo princípio da legalidade, "*ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*" (art. 5º, II, CF/1988). Conforme leciona Leonardo Bessa (2022, p. 75):

> A definição normativa da responsabilidade civil diz respeito a quem deve arcar com os danos inerentes à vida em sociedade. Para que a vítima do dano não suporte o próprio prejuízo, é necessário estabelecer, por norma jurídica, os requisitos ou pressupostos para que uma terceira pessoa tenha o dever de indenizar o prejuízo alheio. Configurados os pressupostos em determinado caso concreto, surge o dever (obrigação sucessiva) de indenizar dano causado a terceiro.
> Em outras palavras, para melhor compreender a questão, deve se raciocinar que, antes de qualquer disciplina jurídica, a regra é que a própria vítima arque com seus danos. Os pressupostos ou requisitos, para que terceiro assuma o dano, deve ser explícito as normas definidoras de responsabilidade civil.

Esse raciocínio designa que, em regra, a própria vítima acaba por arcar com os danos sofridos. Não há um dever pressuposto apto a obrigar a alguém a suportar prejuízo alheio. A responsabilidade civil exige previsão normativa. Seus pressupostos e requisitos devem ser explícitos na norma e é necessário o cumprimento de cada um deles, no caso concreto, para gerar o dever sucessivo de indenizar dano causado a terceiro. Nessa linha, a culpa – pressuposto que caracteriza a responsabilidade civil subjetiva – deve estar expressa na norma (BESSA, 2022). Não é, nem poderia ser, um elemento implícito extraído fora do texto legal.

Exemplo representativo dessa premissa consta no art. 37, §6º, da CF/1988. O dispositivo define a responsabilidade objetiva das pessoas jurídicas de direito público e de direito privado prestadoras de serviço público quando seus agentes, nessa qualidade, causarem danos a

terceiros. O direito de regresso, por sua vez, exige a comprovação de dolo ou culpa dos agentes, tendo em vista tratar-se de elemento expresso na norma. Cuida-se, respectivamente, de responsabilidade de natureza objetiva do Estado e de natureza subjetiva de seus agentes:

> Art. 37. § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

Sobre a responsabilidade civil no tratamento de dados pessoais pelo Poder Público, sua natureza jurídica é reconhecidamente objetiva, tendo em vista que, independentemente da discussão acerca da natureza objetiva ou subjetiva prevista no art. 42*, caput*, da LGPD, esse dispositivo deve ser lido em harmonia com o art. 37, §6º, da CF/1988, o qual impõe a responsabilidade objetiva do poder público pelos danos causados a terceiros pela conduta seus agentes.

A aplicação prática desse entendimento pode ser verificada em jurisprudência. Em caso enfrentado pelo TRF3, a autora buscou a condenação do INSS (Instituto Nacional do Seguro Social) por ter sofrido assédio por ligações ininterruptas de instituições bancárias e financeiras em geral logo após o deferimento do benefício de pensão por morte em decorrência do óbito de seu marido. O Tribunal reconheceu que o vazamento de informações para empresas de crédito foi o fator que possibilitou o exercício de marketing ativo para ofertas de crédito:

> [...] e as informações relativas ao referido benefício, certamente, **só podem ter sido obtidas pelas instituições financeiras, de forma tão célere, por meio de vazamento/transferência de dados** do sistema do INSS, autarquia responsável pela concessão e implantação do benefício previdenciário concedido à autora, o que **demonstra uma ausência de controle e segurança** em seu banco de dados, afrontando o direito à privacidade dos seus beneficiários.
> (Recurso Inominado Cível RecInoCiv 5000086-03.2021.4.03.6345, Juíza Federal Janaina Rodrigues Valle Gomes, TRF3 - 12ª Turma Recursal da Seção Judiciária de São Paulo, data: 15/06/2022) – grifos da autora.

Na fundamentação do acórdão, foi reconhecida a responsabilidade objetiva da autarquia previdenciária, a qual é definida independentemente da divergência doutrinária a respeito da natureza da responsabilidade civil prevista na LGPD (em especial, no seu art. 42), tendo em vista justamente as disposições do §6º, do art, 37, da CF/1988:

> Embora exista divergência na doutrina no que tange a natureza da responsabilidade prevista no art. 42 da LGPD, se subjetiva ou objetiva, no

> que tange ao poder público, não tenho dúvida que sua natureza é objetiva. Meu posicionamento está embasado na **redação do art. 37. §6º da CF/88 que impõe a responsabilidade objetiva do poder público pelos danos causados a terceiros**. Desta forma, **a leitura do art. 42 da LGPD deve ser feito em harmonia com o texto constitucional**, pelo que rejeito a alegação do INSS nesse ponto.
> Fixadas tais premissas, o prova dos autos é robusta e indica claramente o vazamento de dados relativos aos benefício de pensão por morte concedido à parte autora por parte do INSS, sem o consentimento de seu titular.
> A concessão da pensão por morte previdenciária à autora está comprovada por meio do documento anexado no id. 254982858 (NB 193.109.960-7), tendo sido concedido o benefício em 07/06/2021, com data de início fixada em 20/05/2021.
> (Recurso Inominado Cível RecInoCiv 5000086-03.2021.4.03.6345, Juíza Federal Janaina Rodrigues Valle Gomes, TRF3 - 12ª Turma Recursal da Seção Judiciária de São Paulo, data: 15/06/2022) – grifos da autora.

Cabe notar que, nesse caso, a condenação por dano moral foi sustentada não pelo vazamento de dados pessoais em si, mas pela afetação de tranquilidade da viúva pelo assédio incessante de ofertas de crédito. Há uma postura relutante da jurisprudência em reconhecer o dever de indenizar de modo desvinculado à perturbação dos sentimentos subjetivos de uma pessoa. De fato, não se defende que qualquer descumprimento de normas atinentes à proteção de dados pessoais (como o dever de segurança) seja elemento único para configurar o prejuízos aos direitos existenciais do titular de dados. A aferição do dano, como elemento da responsabilidade civil, exige a ponderação de interesses em conflito *in concreto* para aferir efetivo prejuízo a interesse existencial tutelado pelo ordenamento jurídico.

Decerto, no caso enfrentado pelo TRF3, demonstra-se não um mero vazamento de dados criptografados do INSS, inacessíveis ao público externo, mas, sim, uma desvirtuação da finalidade de um tratamento de dados para atender aos interesses de instituições que não convergem com interesses do titular dos dados. A ausência de legítimo interesse, de consentimento ou de amparo legal nesse caso concreto torna ilícito o uso desses dados para fins econômicos ou financeiros nos moldes nos moldes promovidos pelas instituições financeiras.

Nesses termos, a responsabilidade por danos causados no tratamento de dados pessoais pelo Poder Público é objetiva, tendo em vista a previsão expressa dos requisitos na norma jurídica indicar tal natureza (em especial, com base no art. 37, §6º, CF/1988). Outro exemplo representativo desse raciocínio pode ser verificado pela responsabilidade civil objetiva e subjetiva por ato ilícito prevista no Código Civil (artigos 186, 187 e 927).

O art. 927, *caput*, prevê a obrigação de reparar àquele que comete um dano por ato ilícito – conforme conceitos constantes dos artigos 186 e 187 do Código Civil. O art. 186 exige o elemento volitivo pois conceitua o ato ilícito como o dano decorrente de ação ou omissão

voluntária, negligência ou imprudência que viole direito de outrem. O art. 187, por outro lado, prevê que o ato ilícito por abuso de direito prescinde de dolo ou culpa, restando configurado quando o exercício de um direito excede os limites impostos pelo fim econômico, social, pela boa-fé ou pelos bons costumes. Nessa perspectiva, a responsabilidade civil por ato ilícito pode apresentar duas naturezas: uma objetiva e outra subjetiva.

O ato ilícito, como violação de um dever jurídico[56], admite formular dois juízos de valor: um sobre caráter nocivo do ato ou de seu resultado (aspecto objetivo) e outro sobre a conduta de seu agente (aspecto subjetivo). Essa perspectiva envolve o conceito de que ato ilícito ora é definido pela conduta (culposa), ora é determinado pelo dano (injusto). Nesse sentido, Judith Martins Costa leciona (2018, p. 667):

> O ordenamento acolhe não apenas a ilicitude subjetiva, isto é, a lesão derivada de ato (doloso ou culposo, voluntário, negligente ou imprudente; comissivo ou omissivo) que viola direito e causa dano a outrem (art. 186), mas igualmente a lesão proveniente da chamada «ilicitude objetiva» – porque independente do elemento subjetivo (culpa ou dolo) –, normalmente configurada no momento do exercício de posições jurídico-subjetivas, quando tido, este, como inadmissível ou disfuncional, segundo certas balizas que o enunciado legal pontua.

A responsabilidade civil por ato ilícito no Código Civil não pressupõe, *contrario sensu*[57], uma regra geral de responsabilidade subjetiva, segundo a qual a exigência de culpa seria a regra que atribui um pressuposto implícito na disciplina de responsabilidade civil. O raciocínio deve ser baseado em premissa diversa, pautado pela norma expressa e não por uma premissa implícita.

---

[56] De modo diverso, Anderson Schreiber afirma que *ilicitude* somente pode ser utilizada para indicar o ilícito subjetivo, ao passo que a expressão *antijuridicidade* se refere ao ilícito objetivo. O autor valoriza a distinção semântica para caracterizar se a análise de uma conduta leva em conta a vontade do humano que a pratica: "Então, quem viola um dever jurídico ou o direito de outrem, pratica um ato antijurídico – contrário ao direito – mas nem por isso, comete ato ilícito. A ilicitude depende da configuração desta possibilidade de agir de maneira diversa, sem a qual a responsabilidade subjetiva não se impõe. [...] De qualquer modo, é certo que a antijuridicidade, como componente objetivo da ilicitude, corresponde à violação de um dever de conduta, não se confundindo com a ilicitude em si, que exige, além disso, um componente vinculado visceralmente à conduta do sujeito: o da culpabilidade, essencial à responsabilidade subjetiva" *in Novos paradigmas da responsabilidade civil*, 6ª ed. São Paulo: Atlas, 2015 p. 153-154.

[57] Tepedino, Barboza e Moraes afirmam que a tese da desvinculação da culpa do conceito de ato ilícito vai de encontro à segurança jurídica: "Mostra-se equivocada a tentativa de ampliar a noção de ato ilícito, a despeito de seus elementos essenciais, em detrimento da segurança jurídica. A tese, desprovida de base doutrinária, revela-se falsamente progressista, como se propalasse um desprendimento da noção de culpa. Ao contrário, contudo, acaba por ampliar a noção do ilícito, recrudescendo a visão do direito como instrumento não de promoção, mas de repressão, voltado exclusivamente para o momento patológico das relações sociais. Afinal, o ato ilícito constitui-se em fonte das obrigações e sua ampliação desmesurada nenhum proveito traz às relações privadas." *In* TEPEDINO, Gustavo; MORAES; Maria Celina Bodin de; BARBOSA, Heloísa Helena. *Código Civil interpretado*: conforme a Constituição da República. 3ª. Ed. Rio de Janeiro: Renovar; 2014.

Defende-se, portanto, que a culpa, como requisito da responsabilidade subjetiva, deve estar prevista na norma, como regra de adequação ao art. 5º, II, da CF/1988 (princípio da legalidade). Nessa perspectiva, o Código Civil prevê duas cláusulas gerais de responsabilidade civil: uma objetiva (art. 187 c/c art. 927, parágrafo único) e outra subjetiva (art. 186, c/c art. 927, *caput*). A diferença entre os requisitos exigidos para cada uma, reitera-se, não é analisada de forma pressuposta, mas de acordo com o disposto expressamente pela norma.

A exigência de que os elementos da responsabilidade civil sejam taxativamente previstos pela norma jurídica permite concluir que a natureza objetiva da responsabilidade civil prescinde da sentença "*independentemente da existência de culpa*" (BESSA, 2022). A expressão de fato consta em diversos dispositivos, como na cláusula geral de responsabilidade objetiva do Código Civil, prevista em seu art. 927, parágrafo único: "*haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei,* [...]" bem como na disciplina da responsabilidade civil pelo fato do produto e do serviço no Código de Defesa do Consumidor (artigos 12 e 14).

Ocorre que a locução "*independentemente da existência de culpa*" é dispensável. Ainda que presente no parágrafo único do art. 927, do Código Civil, bem como nos arts. 12 e 14, do CDC, seu emprego é desnecessário para constatar a natureza objetiva da responsabilidade civil. A sua utilização tem justificativa histórica, o que não se confunde com uma exigência normativa. Trata-se de uma expressão utilizada para fazer face à cultura jurídica de responsabilidade subjetiva estabelecida pelo Código Civil de 1916 (BESSA, 2022), mas não de uma exigência do ordenamento jurídico.

Em síntese, tendo em vista que a imputação de um dever de reparar decorre da norma jurídica, a responsabilidade civil não pode ser pressuposta, tampouco poderia ser implícita a indicação de seus requisitos.

Por esse raciocínio, conclui-se que a responsabilidade civil disciplinada em seção própria na Lei Geral de Proteção Dados (arts. 42 a 45) é objetiva, tendo em vista a ausência do elemento *culpa* dentre os requisitos elencados para a configuração de um dever de indenizar. Difere-se, por exemplo, da previsão expressa da responsabilidade civil subjetiva dos profissionais liberais nas relações de consumo, conforme prevê o art. 14, §4º, do CDC: "*A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa*."

A definição da natureza objetiva da responsabilidade civil prevista na LGPD orienta a disposição dos pressupostos para sua configuração. Os elementos fato, nexo causal e dano são definidos a partir desse raciocínio. A despeito da dispensa de culpa para configurar o dever

sucessivo de reparar um dano, os desafios para o intérprete não se tornam menos complexos. É o que se passa a aprofundar.

7. DAS DUAS ESPÉCIES DE TRATAMENTO IRREGULAR NA LGPD.

7.1 Inspiração do quadro da responsabilidade civil da LGPD nos modelos internacionais de leis de proteção de dados pessoais.

O início da elaboração de diplomas normativos voltados à proteção de dados remonta à década de 1970. O foco central inicial desse período foi assegurar o adequado processamento de dados pessoais por órgãos governamentais – que então eram as figuras que detinham o maior poder sobre as informações da sociedade. Nos Estados Unidos, tem-se o *US Privacy Act of 1974*, utilizado para regular a coleta e utilização de dados pessoais de cidadãos americanos pelo governo federal dos Estados Unidos (LINOWES, 1977).

Em uma tradução livre, no *US Privacy Act of 1974* foram enumerados os seguintes princípios: coleta limitada; qualidade dos dados; especificação dos propósitos; uso limitado; segurança; transparência; participação; responsabilidade. A aplicação setorizada e limitada desse documento foi reforçada pela então Comissão de Proteção de Dados de 1977, a qual recomendou fortemente que a aplicação das disposições do diploma se limitassem ao âmbito público (e não ao setor privado) bem como apenas à esfera federal

Posteriormente, o foco da regulação voltou-se ao fortalecimento da responsabilidade no tratamento de dados para setores tanto públicos quanto privados.

Em 1980, a OCDE[58] (Organização para a Cooperação e Desenvolvimento Econômico) publicou recomendações para incentivar a tomada de ações proativas dos agentes de tratamento de acordo com os riscos de sua atividade frente à liberdade das pessoas. Os denominados "*Fair Information Principles"* (FIPS) formaram as seguintes recomendações elaboradas para a proteção da privacidade, da transparência e do fluxo de dados: coleta limitada; qualidade dos dados; especificação dos propósitos; uso limitado; segurança; transparência; participação; e responsabilidade (OECD, 1980)[59].

[58] A Organização para a Cooperação e Desenvolvimento Econômico é um organismo integrado por 37 nações, que se reúnem para trocar experiências e elaborar diretrizes em diferentes áreas que impactam a economia mundial. O Brasil engaja-se à OCDE desde 1994. Disponível em: https://www.oecd.org/latin-america/paises/brasil-portugues/ Acesso em 04/05/2023.

[59] No original: "*collection limitation principle; data quality principle; purpose specification principle; use limitation principle; security safeguards principle; openness principle; individual participation principle; accountability principle*." Organisation for Economic Co-operation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. September 23, 1980. Disponível em: <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>. Acesso: 29/03/2023.

A despeito de não assumirem caráter vinculante, os FIPS influenciaram as mais diversas legislações de proteção de privacidade. O melhor exemplo da implementação desses princípios ocorreu em 1995, pela Diretiva de Proteção de Dados da União Europeia (DPD). Desde 2018, tal diretiva foi sucedida pela General Data Protection Regulation (GDPR). A semelhança dos preceitos da Lei Geral de Proteção de Dados com os princípios elaborados pela OCDE não é uma coincidência. A LGPD em muito se inspirou nas disposições e formas de tutela da GDPR.

Nos Estados Unidos, a proteção de dados integra o direito à privacidade e sujeita-se a legislações setoriais que regulam as respectivas áreas específicas, como bancárias, de seguros-de saúde e de consumo. Não há uma lei geral de proteção de dados. A norma de aplicação mais ampla ainda é a Privacy Act de 1974, a qual se limita a incidir sobre agências de governo federais.

A proteção de dados nos Estados Unidos, portanto, depende do contexto e do setor em que são processados. A título de exemplo, no contexto comercial, a proteção de dados recai sobre a *Federal Trade Commision* (FTC) que avalia as violações à uma quebra de expectativa de privacidade dos consumidores não como uma violação à pessoa em si, mas como método de competição desleal no mercado.[60] Há uma forte cultura de controle de dados pelo titular, o que reforça um aspecto de tomar os dados pessoais como bens patrimoniais, sujeitos à disposição de acordo com a vontade do titular.

A perspectiva americana segue o modelo normativo guiado pela noção de que qualquer atividade que envolva o processamento de dados é permitida e válida, desde que não restrita ou explicitamente proibida. É distinta do modelo europeu e do brasileiro, que impõem ao agente de tratamento o dever de observar diversas obrigações e princípios em qualquer atividade de tratamento de dados bem como garantem direitos àqueles cujos dados pessoais estão sujeitos a processamento.

As diretrizes e disposições de ambos os modelos, americano e europeu, se fazem presentes como inspiração nas disposições da LGPD. Quanto à disciplina sobre a responsabilidade civil do agente de tratamento, a identificação dos modelos seguidos pela LGPD auxiliam na interpretação de seus dispositivos (arts. 42 a 45).

---

[60] Emprega-se, nesses contextos, a disposição da Seção 5 do FTC Act, que assim dispõe: "*(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful. (2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, [except certain specified financial and industrial sectors] from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce*." Disponível em: https://www.ftc.gov/ Acesso em 04/05/2023.

Preliminarmente, é importante ressaltar que que o instituto da responsabilidade civil, nos moldes delineados pela *civil law* europeia e brasileira, não é um conceito presente nas tradições jurídicas do *common law*, como a americana ou inglesa. A inspiração do modelo americano na aplicação da LGPD deve ser analisada com cuidado e atenção à essa premissa.

No direito consuetudinário, somente incorre em responsabilidade civil aquele que comete delitos específicos, os denominados "*torts*" – expressão muitas vezes traduzida como matéria de responsabilidade civil extracontratual (SOARES, 1997). A responsabilidade civil, nesses casos, refere-se a situações nas quais a violação de uma norma jurídica ou de um dever jurídico obriga o causador de uma falta a reparar o dano sofrido pela vítima. Não há, reitera-se, um princípio geral de responsabilidade civil baseado na culpa ou no risco, como existe para as tradições jurídicas do *civil law*. (AVGOUTI, 2015). Em tradução livre, pela autora:

> A descrição das principais características pelo direito consuetudinário sobre o instituto da responsabilidade civil acentua ainda mais as diferenças fundamentais que as distinguem da lei francesa [*Civil Law*]. Ao contrário da lei consuetudinária, o regime de responsabilidade civil no direito civil não se baseia na atribuição de responsabilidades específicas; está, em realidade, enraizada na noção geral de culpa ou do risco. O direito consuetudinário não tem um princípio geral de responsabilidade baseada nesses mesmos moldes.

Para o direito consuetudinário, também não há o que se descreve por responsabilidade objetiva. Em seu lugar, há o favorecimento de um "padrão objetivo de atendimento" que permite aos juízes sua aplicação por uma abordagem casuística (*in concreto*). A abordagem das duas tradições – *civil law* e *common law* – é diferente nesses casos, mas o objetivo de proteger a vítima é o mesmo. No entanto, a norma consuetudinária estabelece um procedimento rigoroso com vários obstáculos jurisprudenciais a serem superados para então estabelecer uma obrigação de reparar àquele eventualmente considerado responsável. (AVGOUTI, 2015)

Nesse sentido, ganha relevância a origem que inspirou a redação dos dispositivos da Lei Geral de Proteção de Dados brasileira. O art. 42 da LGPD em muito se assemelha à redação do art. 82 do RGPD[61], pois compartilham do foco na regulação da conduta do agente de tratamento:

[61] RGPD. Art. 82. **1.** Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. **2.** Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Disponível em: https://gdpr-text.com/pt/read/article-82/ Acesso em 16/01/2023.

Da responsabilidade e do ressarcimento de danos.	
LGPD	**RGPD.**
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.	Art. 82. **1.** Qualquer pessoa que tenha sofrido danos materiais ou imateriais **devido a uma violação do presente regulamento** tem direito a receber uma indenização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. **2.** Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por **um tratamento que viole o presente regulamento.** O subcontratante é responsável pelos danos causados pelo tratamento **apenas se não tiver cumprido as obrigações decorrentes do presente regulamento** dirigidas especificamente aos subcontratantes **ou se não tiver seguido as instruções lícitas do responsável** pelo tratamento.

Figura 12 - Quadro comparativo para evidenciar semelhanças entre o arr. 42, LGPD, e do art. 82, da GDPR.

Nota-se que o dever de indenizar previsto nesses dispositivos (art. 42, LGPD e art. 82, GDPR) convergem para a perspectiva americana de situar a responsabilidade civil como o descumprimento de um dever específico, qual seja, o descumprimento à legislação de proteção de dados pessoais que cause dano ao titular. De acordo com esses dispositivos, não é qualquer dano decorrente de um tratamento de dados que deve ser suportado pelo agente de tratamento. Tal prejuízo deve ser vinculado à inobservância de um dever específico atribuído ao agente de tratamento que deveria observá-lo.

Essa aproximação de regimes de responsabilidade não significa uma simples transposição de perspectivas do *common law* para o *civil law* brasileiro. A vinculação da responsabilidade civil à violação de um dever específico (arts. 42, LGPD e 82, GDPR) não se confunde com uma autorização geral pautada pela lógica "o que não é proibido é permitido". Em outras palavras, afastar a responsabilidade civil diante de danos decorrentes de tratamento de dados que sigam disposições específicas não implica uma "carta em branco" aos agentes de tratamento. Há outra espécie de responsabilidade civil prevista na LGPD que não acompanha a mesma exigência (art. 44, *caput*, segunda parte) bem como não há óbice para a incidência de regimes de responsabilidade civil previstos em outras normativas (como no CDC) ou relativos a outras esferas, como a responsabilidade administrativa ou penal.

O *caput* do art. 44 (segunda parte) – diferente do art. 42, *caput*, e art. 44, parágrafo único – inspira-se nos dispositivos do Código de Defesa do Consumidor, em especial, quanto à

disciplina do fato do produto, que visa tutelar a segurança e não a mera funcionalidade dos produtos e serviços colocados no mercado (art. 12 a 14)[62].

Da responsabilidade e do ressarcimento de danos.	
LGPD	**CDC.**
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 [...]	Art. 14, §1º: O serviço é defeituoso **quando não fornece a segurança que o consumidor dele pode esperar**, levando-se em consideração as circunstâncias relevantes, [...]

Figura 13 - Quadro comparativo para evidenciar semelhanças entre o art. 44, caput, segunda parte, da *LGPD, e do art. 14, §1º, do CDC.*

Essa correlação é ainda evidenciada pelo artigo 45, da LGPD, o qual pontua que as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente, bem como pelo artigo 64, que preceitua que os direitos e princípios expressos na LGPD não excluem outros previstos no ordenamento jurídico ou nos tratados internacionais dos quais o Brasil seja parte e que sejam relacionados à matéria.

A inspiração das normativas que inspiraram a redação e modelos de responsabilidade previstas na LGPD não é fato que possa ser ignorado pelo intérprete, mas essa correlação deve ser pautada com cautela e especial atenção ao fato de que não há um regime de responsabilidade civil para a *common law* equivalente ao previsto pelos regimes de *civil law* brasileiro e europeu.

Ainda que se note uma inspiração de um dos principais dispositivos da responsabilidade civil da LGPD (art. 42, *caput*) na perspectiva do *common law* (pautada por delitos específicos), o ordenamento jurídico brasileiro não abandona cláusulas gerais de responsabilidade civil pautadas pela culpa ou risco por danos causados em um tratamento de dados pessoais. Ademais, o intérprete não pode olvidar do dever de interpretação sistemático imposto pela LGPD (arts. 45 e 64, LGPD) – o que abre espaço para a responsabilidade civil também ser pautada por outros diplomas normativos, como o CDC.

Por fim, o art. 42, *caput*, da LGPD, não esgota a disciplina da responsabilidade civil prevista na normativa. O art. 44, *caput*, segunda parte (LGPD) também integra a disciplina desse instituto e apresenta inspiração de sua redação em diploma normativo diverso (o CDC),

[62] Destaca-se a redação do art. 12, §1°: "o produto é defeituoso quando não oferece a segurança que dele legitimamente se espera [...]".

que sujeita análise do dever de reparar danos causados pelo tratamento de dados pessoais pela violação não a um dever específico, mas pela inobservância a um dever geral de segurança.

Tratamento irregular. LGPD	**Art. 42, LGPD.**	Inspirado no GDPR. ["*inspiração*" no *commom law*.]	Delitos específicos.
	Art. 44 (segunda parte), LGPD.	Inspirado no CDC.	Violação do dever geral de segurança.

Figura 14 - Indicação da semelhança do modelo seguido pelos dispositivos da LGPD sobre a responsabilidade civil.

Essa dupla inspiração de modelos normativos indica que a da responsabilidade civil da LGPD é orientada tanto por delitos específicos (conforme guiado pela GDPR) quanto pela violação de um dever geral de segurança (aos moldes previstos pelo CDC). Essa duplicidade reforça a adoção de um regime dual de responsabilidade civil na LGPD (arts. 42 a 45). É que se passa a demonstrar.

7.2 Regime dual de responsabilidade civil na LGPD.

A responsabilidade civil na LGPD é disciplinada em seção específica, composta pelos artigos 42 a 45. Em um panorama geral de seus preceitos, o art. 42 estabelece a responsabilidade objetiva do controlador ou operador que, em violação à legislação, causa dano a outrem em razão do exercício de atividade de tratamento de dados. O art. 43 prevê as hipóteses que, uma vez comprovadas, excluem o dever de indenizar (ou seja, elenca as denominadas excludentes de responsabilidade). O art. 44 se encarrega de estabelecer o conceito de tratamento irregular. Por fim, o art. 45 reforça a aplicação integrada da legislação de proteção de dados e das regras de responsabilidade previstas nas normas de consumo. Destaca-se, nesse ponto, a importância do papel do CDC na interpretação da responsabilidade civil prevista na LGPD (em *diálogo das fontes*).

A despeito da disposição topográfica dessa seção iniciar sua disciplina pelo art. 42 (LGPD), melhor compreensão do tema parte do seu art. 44, *caput*, que detalha o que qualifica um tratamento de dados como irregular para fins de análise da disciplina de responsabilidade civil nos moldes regulados pela LGPD.

Pelo art. 44, da LGPD, *tratamento irregular* é expressão apresentada como gênero de duas espécies: uma por violação à legislação e outra por inobservância à expectativa de segurança do titular de dados pessoais.

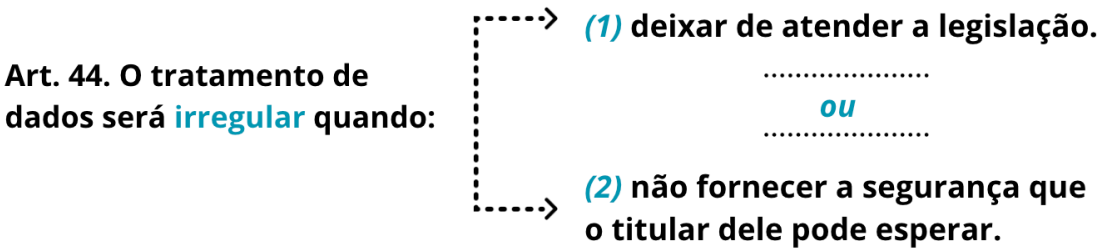

Figura 15 - Representação visual do "tratamento irregular" como gênero de duas espécies.

O dispositivo (art. 44, LGPD) revela duas esferas de proteção (ou objetivos) da lei de proteção de dados brasileira. Uma é voltada a assegurar a adequação da *conduta dos agentes* de tratamento às normas que regulam a atividade de tratamento de dados pessoais. A outra tem como foco a *tutela da pessoa natural*, pelo aspecto de proteção à sua legítima expectativa de segurança no tratamento de informações que as identifiquem ou as tornem identificáveis.

Será regular o tratamento de dados pessoais que atender a ambas as esferas de proteção:

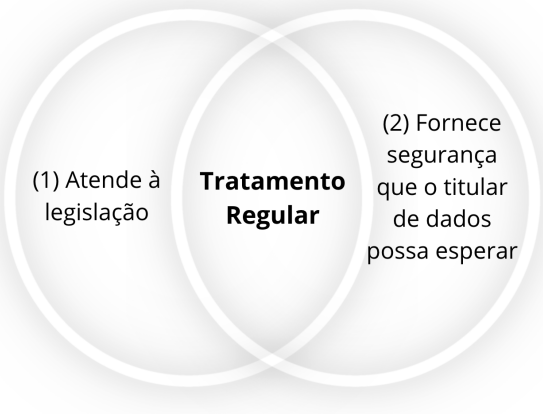

Figura 16 - Representação visual das duas esferas de proteção da LGPD e correspondente designação do que qualifica um tratamento de dados como uma atividade regular.

A despeito de poucos artigos, a disposição topográfica dos dispositivos que regulam a responsabilidade civil na LGPD não torna evidente a classificação defendida – tampouco seus desdobramentos ou suas consequências.

Não há previsão expressa de que o tratamento irregular enseja o direito de indenização à vítima nos mesmos moldes do que prevê o Código Civil a respeito da responsabilidade civil

por ato ilícito – o qual conceitua o ato ilícito nos arts. 186 e 187 e prevê o respectivo dever de reparação em seu art. 927, *caput*: "*aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo*".

No entanto, o dever de reparar o dano pelo tratamento irregular não é afastado. Trata-se de uma consequência lógica da norma reforçada pelo "*dever de reparação*" e "*dever de resposta*" previstos, respectivamente, no art. 42, *caput*[63] e no art. 44, parágrafo único[64], ambos da LGPD:

Dispositivo da LGPD	Conduta	Obrigação
Art. 42, *caput*	[...] 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
Art. 44. Parágrafo único.	[...] **der causa a dano** por violar a segurança dos dados ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei,	Responde pelos danos em razão da violação da segurança dos dados.

Tabela 12 - Do dever de reparar previsto expressamente na LGPD.

Quanto à primeira espécie de tratamento irregular, caracterizada pelo dano causado *por violação à legislação*, importa notar que a LGPD exige, em dois dispositivos distintos, que a conduta danosa apta a ensejar reparação esteja vinculada à inobservância de uma previsão normativa. É o que disciplina tanto o art. 42, *caput*, como o art. 44, parágrafo único:

> **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.
> **Art. 44. 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.

Ressalta-se, nesse ponto, a caracterização da responsabilidade civil como uma obrigação sucessiva, ou seja, decorrente da violação de um dever antecedente específico (previsto pela

[63] LGPD. 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.
[64] LGPD. Art. 44. 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.

norma). Pelos dispositivos indicados, a estruturação do que se compreende por tratamento irregular pode ser assim complementada:

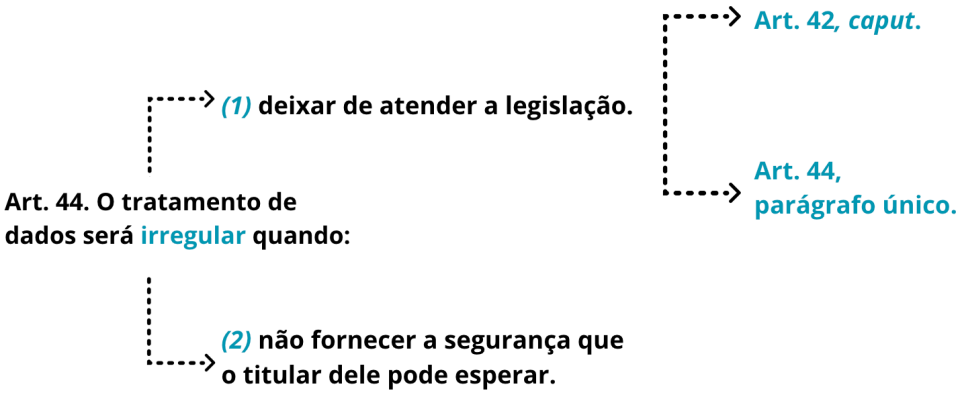

Figura 17 - Representação visual do enquadramento do art. 42, caput e art. 44, parágrafo único, da LGPD, como modalidades da primeira espécie de tratamento irregular de dados pessoais.

A responsabilidade civil prevista no art. 42, *caput*, da LGPD, exige, como requisitos, que o dano decorra de uma atividade exercida pelo controlador ou operador e que o exercício de tal atividade esteja vinculado a uma violação à legislação de proteção de dados (ou seja, às disposições da LGPD). O dispositivo reforça que há consequências não apenas administrativas (como multas aplicadas pela Autoridade Nacional) mas também de ordem cível pelo descumprimento de suas determinações. Como exemplo de atividade que viole o art. 42, *caput*, tem-se o tratamento de dados que não é realizado com base no consentimento informado, no legítimo interesse ou em outra base legal que legitime a atividade (conforme previsto nos arts. 7º e 11, da LGPD).

O art. 44, parágrafo único, da LGPD, disciplina a responsabilidade civil do agente de tratamento que causar danos decorrentes de sua conduta omissiva quanto ao dever de adotar medidas de segurança. O dispositivo remete ao art. 46, da mesma norma, para estabelecer quais são as medidas de segurança que ensejam tal responsabilidade. O art. 46, §1º, da LGPD, estabelece que cabe à Autoridade Nacional dispor sobre padrões técnicos exigíveis para tornar aplicável o dever imposto aos agentes de tratamento de adotar medidas de segurança (art. 46, *caput*, LGPD).

Pela leitura combinada do art. 44, parágrafo único e do art. 46, *caput* e §1º, da LGPD, não é, portanto, qualquer violação de segurança dos dados que se enquadra nessa modalidade de responsabilidade civil. É a omissão às determinações de segurança emitidas pela ANPD que caracteriza a conduta apta a ensejar o dever de reparar nos termos do art. 44, parágrafo único (LGPD):

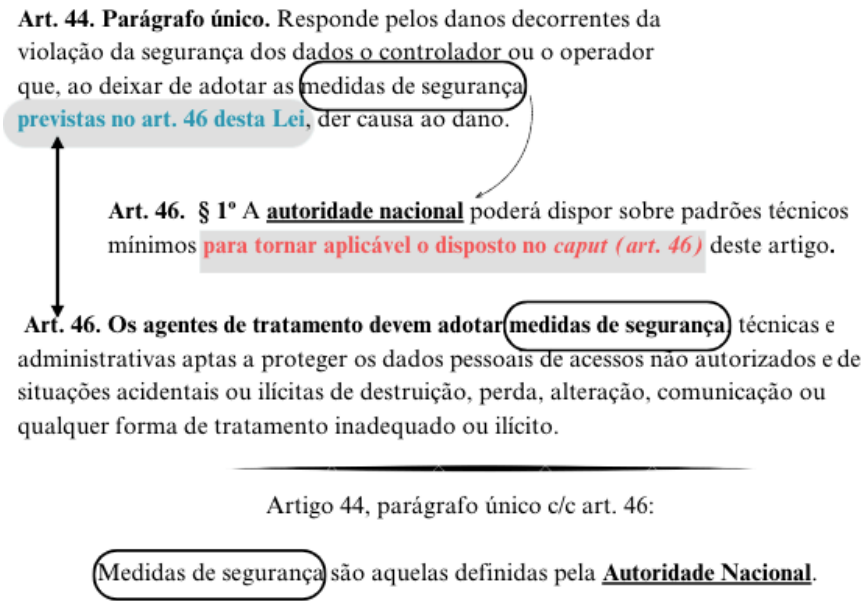

Figura 18 - Vinculação da expressão "medidas de segurança" como aquelas definidas pela ANPD.

Prosseguindo na estruturação da classificação defendida, nota-se que há dois dispositivos que fazem referência ao tratamento irregular (gênero) na espécie deixar de atender à legislação: um que menciona a violação à legislação de proteção de dados (art. 42, *caput*) e outro que trata da responsabilidade do agente de tratamento pelos danos causados por sua omissão em adotar medidas de segurança definidas pela ANPD. Tratam-se de duas modalidades dessa espécie de tratamento irregular de dados pessoais:

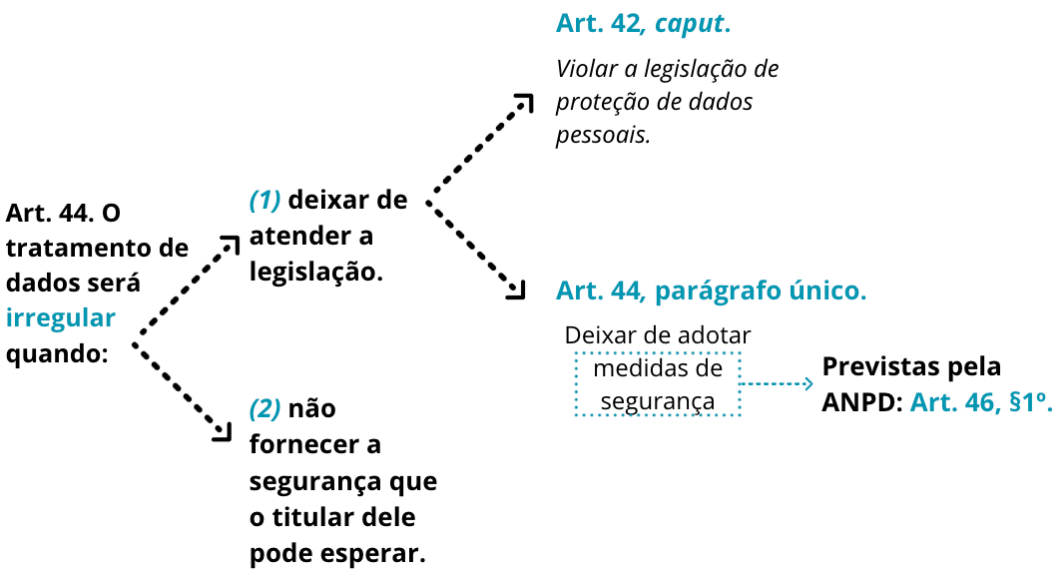

Figura 19 - Distinção de modalidades de tratamento irregular por deixar de atender a legislação. Descrição de medidas de segurança como aquelas previstas pela ANPD.

Esclareça-se que as *medidas de segurança*, entendidas como aquelas regulamentadas pela ANPD, não esgotam a *tutela à segurança* do titular de dados. Consoante o raciocínio desenvolvido, o art. 44, caput, da LGPD, também tutela a *legítima expectativa de segurança* do titular de dados. Trata-se da segunda hipótese de tratamento irregular de dados pessoais prevista na norma.

As diferenças da disciplina pela LGPD quanto à tutela da segurança dos dados pessoais demonstra que as "*medidas de segurança*" (art. 44, parágrafo único c/c art. 46, §1º, LGPD) não se confundem com a "*legítima expectativa de segurança*" do titular de dados. Pela primeira, avalia-se a adequação da conduta do agente de tratamento a um aspecto objetivo definido por regulamento editado pela ANPD. Quanto à segunda, analisa-se a influência das circunstâncias do caso concreto para a formação da expectativa subjetiva de segurança do titular dos dados.

<table>
<tr><th colspan="3">Tutela à segurança dos dados pessoais pela LGPD</th></tr>
<tr><td rowspan="2">"Medidas de Segurança"</td><td>São aquelas definidas pela ANPD.</td><td rowspan="2">Se insere na espécie de tratamento irregular (1) por violação à legislação pela modalidade "omissão na adoção de medidas de segurança"</td></tr>
<tr><td>Art. 44, parágrafo único c/c art. 46, §1º, LGPD</td></tr>
<tr><td rowspan="2">"Legítima expectativa de segurança"</td><td>Avaliada in concreto pela perspectiva do titular de dados.</td><td rowspan="2">Espécie de tratamento irregular (2) por violação à legítima expectativa de segurança do titular.</td></tr>
<tr><td>Art. 44, caput, segunda parte.</td></tr>
</table>

Tabela 13 - Tutela à segurança pela LGPD. Diferença entre "medidas de segurança" e tutela à "legítima expectativa de segurança do titular de dados pessoais".

A LGPD não detalha qual é a expectativa de segurança do titular cuja violação é apta a atrair a responsabilidade civil do agente de tratamento. No entanto, a expressão "*expectativa de segurança*" se aproxima (ou mesmo coincide) com o disposto no Código de Defesa do Consumidor a respeito da responsabilidade pelo fato do produto ou do serviço (arts. 12 a 17). O art. 45, da LGPD, se apresenta como reforço argumentativo para essa aproximação, uma vez que prevê que as hipóteses de violação de direitos do titular de dados que ocorram no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

O art. 45, da LGPD, também ganha relevância em vista do fato de que a funcionalidade de diversas tecnologias que permeiam o convívio social e modelos de negócio depende do processamento de um grande fluxo de dados que identifiquem ou tornem identificável uma

pessoa. A formação de relações consumo que coincidam com uma atividade de tratamento de dados pessoais se tornou fato do cotidiano. A ampliação de relações reguladas de forma simultânea tanto pelo CDC quanto pela LGPD (bem como por outras legislações específicas) acompanha essa tendência. Tal integração normativa gera benefícios recíprocos, tanto pela ampliação da tutela ao consumidor/titular em relações que envolvam novas tecnologias – pela aplicação da LGPD –, como pela utilização do histórico doutrinário e jurisprudencial consolidado pela tutela efetivada por meio da aplicação do CDC às relações que envolvam o tratamento de dados pessoais.

Tomar o art. 44 como gênero de duas espécies de tratamento irregular é a base para constatar um regime dual de responsabilidade civil previsto na LGPD. Trata-se de uma proposta de *lege lata* que permite uma interpretação ordenada e sistematiza dos artigos 42 a 45 da LGPD de forma integrada e coerente com outros diplomas normativos porventura incidentes sobre um mesmo caso concreto.

A interpretação sistematizada dos dispositivos do capítulo próprio da responsabilidade civil tratada pela LGPD também permite uma coerência interna na classificação da responsabilidade civil. A remissão ao art. 46, inserido em capítulo próprio (da segurança e das boas práticas) é considerada nessa classificação. No aprofundamento dessa categorização, vislumbra-se a distinção entre tratamento irregular, tratamento ilícito e tratamento indevido. Tratam-se de nomenclaturas empregadas pela própria LGPD que, no contexto da classificação defendida, apresentam peculiaridades próprias e têm a aptidão de facilitar a interpretação e aplicação da norma pelo intérprete.

8. TRATAMENTO IRREGULAR (GÊNERO) POR VIOLAÇÃO À LEGISLAÇÃO (ESPÉCIE).

A responsabilidade civil pelo tratamento irregular caracterizada pela *violação à legislação* é abordada em dois dispositivos na LGPD: no art. 42, *caput*, e no art. 44, parágrafo único. Para ambos, exige-se, como requisitos para o dever de indenizar, que o dano decorra de uma violação à legislação (*lato sensu*) e que haja nexo de causalidade entre esta e uma atividade (conduta) exercida pelo agente de tratamento. A responsabilidade é objetiva, ou seja, independe da verificação de culpa ou do dolo do agente (dispensa-se, nesse ponto, a análise do elemento volitivo do agente).

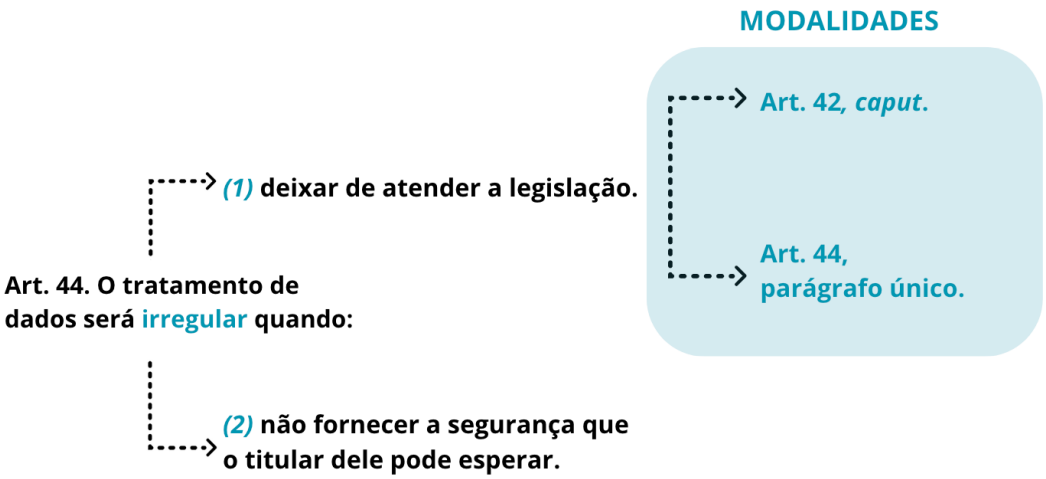

Tabela 14 - Destaque para as modalidades de tratamento irregular na espécie violação à legislação.

O traço distintivo entre as modalidades tratadas nesses dispositivos reside na identificação do *tipo* de conduta (omissiva ou comissiva) e, em especial, quanto à incidência ou não das excludentes de responsabilidade civil previstas no art. 43, da LGPD.

A comprovação de uma excludente de responsabilidade tem como consequência afastar o dever de indenizar, ainda que de um tratamento de dados decorra um dano. Uma vez provada uma hipótese excludente, à vítima cabe suportar a própria lesão, indicar outro responsável ou buscar fundamentação jurídica diversa para mitigar seus prejuízos.

Há três hipóteses que afastam a responsabilidade civil previstas no art. 43, da LGPD:

> 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 terceiro.

Pela primeira hipótese, não haverá responsabilidade uma vez provado que o controlador ou operador não realizaram o tratamento de dados pessoais que causou o dano ao titular. Da mesma forma, não será imputado o dever de indenizar caso provado que o dano decorreu de culpa exclusiva do titular de dados ou de terceiro. Tais hipóteses (art. 43, I e III) são baseadas no entendimento de que há quebra do nexo de causalidade entre o dano e um *efetivo* exercício de atividade pelo agente de tratamento. A excludente prevista no inciso II, do art. 43 (LGPD), evidencia a intenção da norma em regular a *conduta* dos agentes de tratamento pois exclui a responsabilidade daquele cuja atividade, ainda que tenha causado danos, não ofenda algum dever imposto pela legislação de proteção de dados.

Essas excludentes são condizentes com a responsabilidade civil prevista no art. 42, *caput*, da LGPD. Por essa modalidade, o dano deve estar vinculado ao exercício *efetivo* de uma atividade de tratamento de dados pelo controlador ou operador apontado e tal exercício *deve* corresponder a uma violação à legislação de proteção de dados pessoais. Se o agente de tratamento realizou alguma atividade de tratamento de dados pessoais (art. 5º, X, LGPD) mas não exerceu aquela que causou o dano, não poderá ser responsabilizado (art. 43, I, LGPD). Da mesma forma, não será responsável pelo dano causado por terceiro – como um *hacker* – ou se não descumpriu preceitos da LGPD (art. 43, II e III, LGPD).

Por outro lado, a responsabilidade civil pelo tratamento irregular tutelada no art. 44, parágrafo único, da LGPD, restaria esgotada caso fossem aplicadas as mesmas excludentes previstas no artigo antecedente. Por essa modalidade, o responsável não será aquele que realizou o tratamento danoso, mas sim, aquele que se omitiu no dever de implementar medidas de segurança determinadas pela ANPD. Pressupõe-se que o dano seja causado por uma terceira pessoa, que se aproveita de uma brecha de segurança causada pela conduta omissiva do agente de tratamento. Seria o caso, por exemplo, de um vazamento de dados por um *hacker* que se aproveita de uma fragilidade de um sistema ou de um software utilizado em desacordo com medidas de segurança definidas pela ANPD.

Nessa circunstância de falha de segurança, caso incidentes as mesmas regras excludentes do dever de indenizar, o agente de tratamento poderia facilmente eximir-se de sua responsabilidade ao alegar não ter realizado o tratamento de dados que causou o dano ao titular

de dados ou sustentar que o dano decorreu de conduta exclusiva de terceiro (art. 43, I e III, da LGPD).

Por outro lado, é possível vislumbrar a aplicabilidade da excludente prevista no segundo inciso (art. 43, II, da LGPD) qual seja, provar que não houve violação à legislação *lato sensu* de proteção de dados. Nesse ponto, são semelhantes as hipóteses de quebra do nexo de causalidade por ausência de previsibilidade de conduta na legislação *lato sensu* tanto nos termos do art. 42, *caput*, como nos do art. 44, parágrafo único (ambos da LGPD).

Por "*legislação*" *lato sensu*, compreende-se tanto a lei de proteção de dados quanto os regulamentos emitidos pela ANPD. O art. 44, *caput*, da LGPD, por exemplo, ao conceituar tratamento irregular que viole a legislação, adota posição coerente com o sentido *lato sensu* do termo, de modo a abranger tanto a modalidade de responsabilidade civil prevista no art. 42, *caput* (violação à legislação de proteção de dados)[65] quanto a disciplinada no art. 44, parágrafo único (omissão quanto às medidas de segurança determinadas pela ANPD). Por esse entendimento, caso o agente de tratamento prove ter adotado todas as medidas de segurança impostas pela Autoridade Nacional, poderá, em tese, eximir-se do dever de indenizar.

A utilidade da classificação em modalidades do tratamento irregular (gênero) por violação à legislação (espécie) se refere tanto à análise da conduta que eventualmente causou um dano quanto das excludentes de responsabilidade potencialmente incidentes em um caso concreto. Para ambas as modalidades (art. 42, *caput* e art. 44, parágrafo único) exige-se a previsibilidade da conduta esperada pelo agente de tratamento para que eventual dano seja ressarcido. No entanto, as diferentes condutas (por ação ou omissão) atraem excludentes diversas, o que impacta diretamente na análise de eventual imputação de responsabilidade civil.

8.1 Inobservância das medidas de segurança (art. 44, parágrafo único): excludentes de responsabilidade.

Pode-se compreender que a disposição topográfica do art. 43 indica que as excludentes previstas nesse dispositivo dizem respeito apenas à hipótese de responsabilidade civil do artigo antecedente (ou seja, do art. 42, da LGPD). Ainda que cabível esse entendimento, não há que se falar que qualquer falha de segurança atrairá a responsabilidade civil disciplinada pelo art. 44, parágrafo único. Os próprios requisitos da responsabilidade civil desta hipótese exigem que

[65] Note-se que o art. 42 especifica tratar-se da legislação de proteção de dados, motivo pelo qual compreende-se que adota um sentido estrito do termo.

o dano esteja vinculado a uma conduta omissiva do agente de tratamento – a qual somente se verifica quando não atendidos os padrões técnicos definidos pela Autoridade Nacional (conforme exigido pelo art. 46, §1º, da LGPD).

Nessa orientação, ainda que de um fato decorra um dano, caso não constatada uma conduta omissiva do agente de tratamento frente a uma violação de segurança dos dados pessoais por ele gerenciados, não serão preenchidos os requisitos necessários para configurar a responsabilidade civil prevista no art. 44, parágrafo único (LGPD). A configuração de uma conduta omissiva, por essa hipótese, exige a previsibilidade de uma obrigação correspondente pela Autoridade Nacional.

Não há diferença prática quanto à consideração da incidência ou não da excludente de responsabilidade prevista no art. 43, II, da LGPD, à modalidade de responsabilidade prevista no art. 44, parágrafo único. Isso porque a previsibilidade de uma conduta em um regulamento administrativo emitido pela ANPD é uma das exigências para configurar eventual dever de indenizar. Ausente o regulamento que discipline medida de segurança, restará ausente o requisito da conduta diversa esperada pelo agente de tratamento. Não há dúvida, por outro lado, que a hipótese tratada no art. 43, I da LGPD, não se aplica à responsabilidade civil prevista naquele dispositivo.

Quanto à aplicabilidade da culpa exclusiva do titular de dados como excludente à responsabilidade (art. 43, III, LGPD), pode-se, por um lado, considerar que tal fato rompe com o nexo de causalidade necessário para imputar um dever de indenizar nos moldes previstos pelo art. 44, parágrafo único, da LGPD. Por outra perspectiva, é possível constatar que o dano, ainda que por culpa exclusiva da vítima, somente se tornou possível diante da conduta omissiva do agente de tratamento. Em outras palavras, ao se considerar que o dano decorreu de um risco criado pelo agente, o fato de ter sido propiciado pela vítima não poderá ser alegado para excluir sua responsabilidade diante dos prejuízos sofridos.

A questão delineada é simples, mas não simplória, pois ambos os posicionamentos são defensáveis. Em princípio, levando-se em conta a intenção de regular a *conduta* do agente de tratamento, indica ser mais adequada a noção de que, se o dano decorre de um risco criado pelo próprio agente, não se admite suscitar a culpa da vítima como excludente de sua responsabilidade.

Cabe ponderar se o contexto no qual o dano, ainda que por culpa da vítima, poderia ser evitado caso adotadas as medidas de segurança definidas pela ANPD. Se o contexto indicar o atendimento aos regulamentos da ANPD, incidirá a excludente do inciso II, seja o dano causado por culpa exclusiva da vítima ou de terceiro. Por outro lado, haverá nexo de causalidade se

verificado que o dano, ainda que causado pela conduta da vítima, não ocorreria caso adotadas as medidas de segurança pautadas pela Autoridade Nacional.

8.2 Da denominação das modalidades de tratamento irregular por violação à legislação: tratamento ilícito (art. 42, *caput*) e tratamento indevido (art. 44, parágrafo único).

A distinção das modalidades de responsabilidade pelo tratamento irregular na espécie violação à legislação tem utilidade prática, pois há avaliação distinta tanto da conduta do agente (por ação ou omissão) quanto da incidência ou não das excludentes de responsabilidade previstas no art. 43 da LGPD.

A lei nacional de proteção de dados brasileira, por outro lado, não é didática quanto às nomenclaturas empregadas. Além de qualificar o tratamento *irregular* no art. 44 e não o mencionar em outros dispositivos, utiliza-se de outros adjetivos no art. 46, *caput,* ao se referir que os agentes de tratamento devem adotar medidas aptas a evitar qualquer forma de tratamento *inadequado* ou *ilícito*. Para agravar a dificuldade de conceituação, tais adjetivos são empregados de forma exemplificativa por esse dispositivo:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento **inadequado** ou **ilícito**. – **grifos da autora.**

Em uma leitura sistematizada, ainda que o mesmo rigor não tenha sido adotado pelo legislador, é possível verificar que o §1º, do art. 46, exige a definição prévia de medidas de segurança pela ANPD para tornar aplicável o seu *caput*. Dentro da mesma lógica, pode-se compreender que as expressões empregadas exigem a previsibilidade de uma conduta a ser adotada pelo agente de tratamento:

> Art. 46. §1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos **para tornar aplicável o disposto no caput deste artigo**, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. – **grifos da autora.**

A previsibilidade, ou seja, a definição de uma obrigação específica, é inerente à configuração do tratamento irregular por violação à legislação. Para fins didáticos e de coesão

da norma, defende-se a atribuição da nomenclatura *tratamento ilícito* aos danos decorrentes da atividade que viole a legislação de proteção de dados (art. 42, *caput*, da LGPD) e *tratamento inadequado* ao danos consequentes à omissão quanto às medidas de segurança definidas pela ANPD (art. 44, parágrafo único, da LGPD).

Essa proposta também privilegia o pressuposto de que a lei não contém palavras inúteis. Nesse sentido, cabe mencionar a explicação de Carlos Maximiliano (2022, pág. 244):

> Dá-se valor a todos os vocábulos e, principalmente, a todas as frases, para achar o verdadeiro sentido de um texto; porque este deve ser entendido de modo que tenham efeito todas as suas provisões, nenhuma parte resulte inoperativa ou supérflua, nula ou sem significação alguma. [...] *interpretatio in quacumque dispositione ne sic facienda, ut verba non sint superflua, et sine virtute operandi*: "Interpretem-se as disposições de modo que não pareça haver palavras supérfluas e sem força operativa.

Não se pode olvidar que os adjetivos para qualificar um tratamento de dados como irregular são, por grande parte da doutrina, indistintamente utilizados (ROSENVALD e NETTO, 2022; TEIXEIRA, 2022; PECK, 2021). Importante defender que a proposta aqui defendida não se trata propriamente de uma divergência doutrinária, mas sim de uma perspectiva de interpretação diferenciada da norma. Por isso é possível afirmar que se defende uma classificação de forma distinta, mas não necessariamente contraposta a outros posicionamentos.

Assim, em vista da importância da distinção entre as modalidades tratadas para fins de apuração da responsabilidade civil na LGPD – em especial pela avaliação distinta tanto da conduta do agente (por ação ou omissão) quanto da incidência das excludentes de responsabilidade –, pode-se acrescentar as duas nomenclaturas à estruturação do tratamento irregular para facilitar na distinção das circunstâncias em análise, conforme assim delineado:

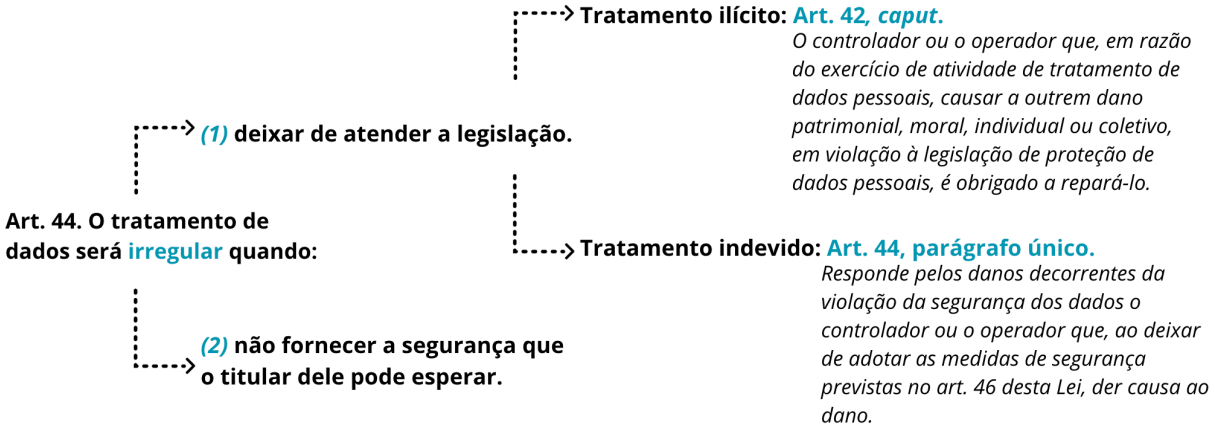

Figura 20 - Espécies de tratamento irregular e modalidades de tratamento irregular por violação à legislação. Distinção de tratamento irregular, ilícito e indevido.

A utilidade prática da distinção entre tratamento irregular, tratamento ilícito e tratamento indevido reside na identificação dos pressupostos da responsabilidade civil e na análise das excludentes de responsabilidade de cada espécie ou modalidade. A proposta contribui para a análise estruturada e coesa dos artigos 42 a 45 da LGPD e, conforme aprofundado, é coerente com a aplicação do diálogo das fontes a respeito da responsabilidade civil disciplinada por normativas diversas.

8.3 Comparativo: espécies de tratamento irregular e modalidades de tratamento ilícito e inadequado.

Pela proposta de estruturação do conteúdo dos arts. 42 a 45, que disciplinam a responsabilidade civil na LGPD, extrai-se, do art. 44, *caput*, que a configuração de um tratamento irregular é o fator que motiva a análise da responsabilidade civil de um agente. O tratamento irregular, por sua vez, é gênero que se desdobra em duas espécies, cujos respectivos amparos legais atendem à seguinte estruturação:

GÊNERO:	**TRATAMENTO IRREGULAR DE DADOS PESSOAIS**	
Fundamento legal:	**Art. 44, *caput,* da LGPD.**	
Espécie:	*(1)* Tratamento irregular por **deixar de observar a legislação**	*(2)* Tratamento irregular por **não atender à expectativa de segurança que o titular possa esperar**.

Fundamento legal:	**Art. 44, caput, primeira parte:** "O tratamento de dados pessoais será irregular *quando deixar de observar a legislação*"	**Art. 44, caput, segunda parte:** "*O tratamento de dados pessoais será irregular quando [...]não fornecer a segurança que o titular dele pode esperar.*"

Tabela 15 - Tratamento irregular de dados pessoais.

A primeira espécie de tratamento irregular prevista no art. 44, *caput*, primeira parte, define a responsabilidade civil do agente de tratamento que deixar de observar a legislação. Tal responsabilidade tem por foco a conformação da *conduta* do agente de tratamento quando no exercício da atividade de processamento de dados pessoais. Essa hipótese é tratada, na LGPD, nos artigos 42, *caput,* e 44, parágrafo único:

Espécie de tratamento irregular:	**(1) Por deixar de observar a legislação**	
Fundamento legal:	**Art. 44, *caput,* primeira parte, da LGPD.**	
Dispositivos correspondentes:	*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.*	*Art. 44, 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.*

Tabela 16 - Dispositivos correspondentes à espécie de tratamento irregular por violação à legislação.

A diferença entre os dispositivos refere-se à especificação da "legislação violada" – considerada em sentido *lato sensu* pelo art. 44, *caput*, primeira parte, da LGPD. O art. 42, *caput*, especifica a vinculação de um dano a uma conduta do agente que viole a lei de proteção de dados (legislação *stricto sensu*). Por outro lado, o art. 44, parágrafo único, atribui o dano a uma inobservância, pelo agente de tratamento, de regulamentos administrativos expedidos pela Autoridade Nacional de Proteção de Dados.

Ambos os dispositivos elencam a vinculação de um dano a uma conduta ilegal do agente de tratamento de dados. O art. 46, *caput* e §1º (LGPD), reforça tal vinculação. O dispositivo trata do dever de segurança dos agentes de tratamento, os quais devem tomar medidas aptas a evitar o tratamento *inadequado* ou *ilícito*. A partir das nomenclaturas empregadas pelo art. 46, *caput*, é possível estruturar o *tipo* de violação normativa que deve ser evitada: seja pela

desobediência à LGPD (tratamento ilícito) seja pela inobservância de regulamentos de segurança emitidos pela ANPD (tratamento inadequado).

Espécie:	**(1) Tratamento irregular por deixar de observar a legislação**	
Fundamento legal:	**Art. 44, *caput,* primeira parte, da LGPD.**	
Modalidades	**Tratamento Ilícito**	**Tratamento indevido**
Dispositivos correspondentes:	*Art, 42, caput*.	*Art. 44, parágrafo único*.
Conduta do agente de tratamento	Violar a LGPD	Violar regulamentos da ANPD

Tabela 17 - Especificação da conduta do tratamento ilícito em face do tratamento indevido de dados pessoais.

Os regulamentos de segurança que devem ser adotados são aqueles expedidos pela Autoridade Nacional, tendo em vista que o §1º, do art. 46, da LGPD, vincula a aplicação do respectivo *caput* à disposição prévia de padrões técnicos mínimos pela entidade, como se observa, *in verbis*: *"§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo*".

Evidencia-se que a adoção de medidas de segurança exige previsibilidade pela Autoridade Nacional, o que não se confunde com a expectativa de segurança que o titular pode esperar de um tratamento de dados. Distintos, portanto, o cumprimento de uma medida de segurança (art. 44, parágrafo segundo) do que se compreende como o efetivo atendimento à uma expectativa de segurança do titular de dados (art. 44, *caput*, segunda parte).

Em síntese, a responsabilidade civil pelo descumprimento da legislação desdobra-se em duas modalidades (ou subespécies): o tratamento ilícito e o tratamento inadequado. Há distinção de condutas, excludentes e consequências entre ambas. O tratamento ilícito exige que a conduta do agente de tratamento designe um desatendimento à LGPD. Nesse sentido, serão analisados, em especial, se a atividade se adequou ao menos a uma das bases legitimadoras do tratamento de dados (consentimento, autorização legal ou legítimo interesse), bem como se foram respeitados os direitos do titular de dados. O tratamento inadequado, por sua vez, se refere à omissão que propicia uma conduta lesiva por terceiro.

A respeito da natureza objetiva da responsabilidade civil, cabe reforçar que a descrição do tipo de conduta de um agente de tratamento não implica em uma necessidade de verificar seu dolo ou culpa. O elemento volitivo do agente de tratamento não consta no rol elencado pela norma. Não pode, portanto, ser um pressuposto presumido ou tomado como implícito na norma (BESSA, 2022).

A responsabilidade objetiva, por outro lado, não se confunde com uma responsabilidade integral. A enumeração dos requisitos do dever de reparar configura fato constitutivo do direito do autor, de modo que à vítima incumbe o dever de comprovar o dano sofrido e o seu nexo de causalidade com um exercício da atividade de tratamento de dados pessoais pelo agente de tratamento.

Ademais, não basta a comprovação do nexo de causalidade entre uma conduta e o dano. Conforme a LGPD, para configurar um tratamento irregular nas modalidades descritas pelos arts. 42, *caput* e 44, parágrafo único, a vítima também deve comprovar que a atividade de tratamento de dados foi realizada em violação a um dever imposto pela legislação de proteção de dados pessoais.

Diante do exposto, são elementos do tratamento ilícito de dados pessoais, conforme art. 42, *caput*, da LGPD: (i) a conduta do agente de tratamento; (ii) o dano vinculado a uma violação de um dever imposto pela LGPD e (iii) nexo de causalidade entre ambos.

Por sua vez, são pressupostos do tratamento indevido de dados pessoais, nos termos do art. 44, *parágrafo único,* da LGPD: i) a omissão do agente de tratamento; (ii) o dano vinculado a uma omissão de um dever imposto pela ANPD e (iii) o nexo de causalidade entre ambos. Traço distintivo dessa modalidade é presumir a atuação de um terceiro, que se aproveita de uma falha de segurança decorrente de conduta omissiva do controlador ou operador.

A diferença entre os requisitos e consequências práticas da distinção entre tratamento ilícito e tratamento inadequado são assim estruturadas:

Requisitos da responsabilidade civil por violação à legislação.		
Modalidade:	**Tratamento ilícito**	**Tratamento inadequado**
Base normativa:	*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.*	*Art. 44. 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. 46. Os agentes de tratamento devem adotar medidas de segurança [...] aptas a proteger os dados pessoais de [...] qualquer forma de tratamento inadequado [...]* *§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo [...]*
Fator causal:	Conduta do controlador ou do operador. Não alcança conduta de terceiros	Omissão do controlador ou do operador. Presume conduta de terceiro

Nexo de causalidade:	Exigida entre a conduta agente de tratamento e o dano.	Entre a omissão do agente de tratamento e o dano.
Dano:	Correlacionado à violação de um dever imposto pela LGPD. Exige previsibilidade – na legislação de dados.	Correlacionado à ausência de adoção de medida de segurança determinada pela ANPD Exige previsibilidade – em regulamento pela Autoridade Nacional.
Excludentes:	i) quebra do nexo de causalidade pelo fato de o controlador ou o operador não terem realizado o tratamento que causou o fato danoso;	Quebra do nexo de causalidade pela ausência de correlação do dano a um dever imposto por regulamento emitido pela ANPD.
	ii) quebra do nexo de causalidade pela ausência de vinculação do dano a um dever previsto pela LGPD;	
	iii) quebra do nexo de causalidade pelo fato de o dano decorrer de culpa exclusiva da vítima ou de terceiro.	

Tabela 18 - Estruturação das características do tratamento inadequado e do tratamento ilícito de dados pessoais.

As excludentes de responsabilidade previstas no art. 43 (LGPD) são condizentes com a intenção do legislador em conformar a atuação dos agentes de tratamento. Isso porque os danos decorrentes de conduta perpetrada por terceiros não ensejarão, por essa hipótese, a responsabilidade do agente (inciso I). Tampouco haverá responsabilidade se comprovado que o dano decorre de conduta exclusiva do titular de dados ou de terceiro (inciso III). Por fim, o artigo indica que, ainda que ocorra um dano, o agente de tratamento não será responsabilizado caso tenha atendido à legislação de proteção de dados. A esse respeito, cabe citar o entendimento de Lucas Simão e Priscilla Costa (2020):

> A partir da interpretação conjunta dos arts. 44 e 46, nos parece que, no âmbito de incidência da LGPD, caso seja demonstrado que as medidas de segurança que venham a ser estabelecidas pela Autoridade Nacional foram observadas, e tendo o controlador e o operador agido de acordo com a técnica e tecnologia disponível, os agentes de tratamento de dados não serão responsabilizados ainda que haja dano aos titulares dos dados.

Pela lógica do art. 42, *caput* (tratamento ilícito), na hipótese de dano causado por uma invasão de sistemas por um *hacker*, por exemplo, seria aplicável a excludente de responsabilidade prevista no inciso I, do art. 43 – ou seja, comprovado que o agente de tratamento não realizou o tratamento de dados danoso, não haveria responsabilidade a ser imputada. Se a disciplina da LGPD se limitasse ao previsto nesse dispositivo, caberia à vítima identificar o *hacker* para reparar ou compensar os danos sofridos ou enquadrar a conduta do agente de tratamento em outra modalidade de responsabilidade civil.

Ocorre que o exemplo acima citado atrai, a priori, disciplina diversa da prevista no art. 42, *caput* (LGPD). Ainda no intuito de regular a conduta dos agentes de tratamento, a LGPD

incluiu uma responsabilidade por ato de terceiro, ou seja, na qual não incide a excludente prevista no art. 43, I ou III (parte final). O art. 44, *parágrafo primeiro* (tratamento inadequado), determina que os agentes de tratamento devem responder por danos que decorram não de uma conduta ativa – como um tratamento realizado sem base legitimadora – mas sim de uma conduta omissiva caracterizada pela ausência de implementação de uma medida determinada pela ANPD. Nesse caso, verificado um dano por ato de terceiro, o agente de tratamento responderá, ainda que não por sua conduta direta, mas por demonstrar a vinculação entre o dano e a respectiva conduta omissiva.

Em outras palavras, o fato de um terceiro se aproveitar de uma brecha de segurança não pode ser utilizado como argumento para excluir sua responsabilização na hipótese do tratamento inadequado (art. 44, parágrafo único, LGPD).

Para ambos os casos de tratamento irregular por violação à legislação exige-se a previsibilidade de um dano, seja no âmbito legal estrito (tratamento ilícito) seja no regulamentar (tratamento inadequado). Caso um dano não decorra de uma conduta ativa ou omissiva prevista e regulada pela LGPD ou pela ANPD, não será o caso de imputação de responsabilidade civil por essas hipóteses.

Nesse sentido, a excludente de responsabilidade prevista no art. 43, II, da LGPD, demonstra muito mais uma quebra do nexo de causalidade ou ausência de pressuposto de responsabilidade civil do que propriamente uma hipótese excludente de responsabilidade. Em outras palavras, se verificado que o dano não decorre de uma fragilidade criada pela omissão do agente de tratamento, não há responsabilidade, seja por constatar a ausência de preenchimento de requisito legal, seja por compreender pela incidência da excludente de responsabilidade prevista no art. 43, II, da LGPD.

	Incidência da Excludente de responsabilidade. (*Art. 43*) Provar que:		
	I. Não realizou o tratamento que lhes é atribuído	II. Não violou legislação de proteção de dados.	III. Culpa exclusiva do titular ou de terceiro
Tratamento ilícito *Art. 42,* caput.	Sim.	Sim. (*quanto às regras da LGPD*)	Sim.
Tratamento inadequado *Art. 44, parágrafo único*	Não.	Sim* (quanto às medidas de segurança reguladas pela ANPD)	Não.

Tabela 19 - Comparação das excludentes de responsabilidade do tratamento ilícito e do tratamento inadequado.

O tratamento ilícito e inadequado, nos moldes apresentados, representam uma definição dos termos elencados pelo art. 46, §1º, da LGPD, mas não exprimem a descrição de algum rigor classificatório adotado pelo legislador. Trata-se de abordagem classificatória para evidenciar as diferenças de aplicação da responsabilidade civil prevista nos arts. 42, *caput* e 44, parágrafo único, da LGPD, especialmente quanto à análise dos seus pressupostos e respectivas excludentes.

De toda forma, tais modalidades não esgotam a disciplina da responsabilidade civil regulada pela LGPD. Outra utilidade da classificação apresentada é evidenciar que há diferença entre as hipóteses previstas no art. 44, parágrafo único e a parte final do *caput* do mesmo dispositivo. Demonstra-se que a adoção de "medidas de segurança" exige previsibilidade pela Autoridade Nacional, o que não se confunde com a "expectativa de segurança" que o titular pode ter por um tratamento de dados. O primeiro tem por foco a avaliação da conduta do agente de tratamento, enquanto o segundo considera as expectativas do titular, com um evidente foco da proteção do titular de dados sob a perspectiva de tutela da pessoa humana.

Distintos, portanto, o cumprimento de uma medida de segurança (art. 44, parágrafo segundo) e o que se compreende como o efetivo atendimento à uma expectativa de segurança do titular de dados (art. 44, *caput*, segunda parte).

Em defesa à estrutura classificatória da responsabilidade civil apresentada, destaca-se que a alternativa conferida pelo art. 44, *caput*, da LGPD não se apresenta no sentido de sinonímia (pois o texto seria redundante – em ofensa ao art. 11, II, b, da LC 95/1998[66]) mas sim no sentido aditivo. O intérprete, portanto, não pode olvidar da ambivalência do tratamento irregular de dados prevista no *caput* do art. 44, da LGPD, especialmente na análise da responsabilidade civil do agente de tratamento.

Verificada a existência das duas espécies de tratamento irregular, é preciso diferenciar os parâmetros legais que singularizam a análise da responsabilidade civil pela violação da expectativa de segurança do titular de dados, conforme art. 44, *caput*, segunda parte, da LGPD.

[66] A LC 95/1998 dispõe sobre a consolidação das leis. Ao regular a articulação e redação das normas, define, em seu art. 11, II, "*b*", que as disposições normativas devem ser redigidas com clareza, precisão e ordem lógica e, para obter precisão, a norma deve "*expressar a ideia, quando repetida no texto, por meio das mesmas palavras, evitando o emprego de sinonímia com propósito meramente estilístico*".

9. TRATAMENTO IRREGULAR (GÊNERO) POR VIOLAÇÃO À EXPECTATIVA DE SEGURANÇA DO TITULAR (ESPÉCIE).

A proposta de categorização do regime de responsabilidade previsto na LGPD permite o alcance da tutela da normativa a diferentes condutas que importem dano ao titular dos dados pessoais. Conforme sustentado, há duas esferas de proteção de dados distintas, mas não excludentes, previstas na LGPD. Uma garante que os tratamentos de dados pessoais sejam adequados à legislação e a outra assegura que o tratamento forneça a segurança que o titular deles possa esperar (art. 44, *caput*, da LGPD).

	Esferas de proteção da LGPD	
	Foco:	**Parâmetro:**
Esfera 1.	Regular/conformar a conduta do agente de tratamento (controlador ou operador)	Normas de proteção de dados *lato sensu*: LGPD e regulamentos de segurança emitidos pela ANPD.
Esfera 2.	Tutelar a pessoa natural	Expectativa de segurança do titular de dados pessoais

Tabela 20 - Descrição das duas esferas de proteção da LGPD.

Para as duas esferas de proteção, a LGPD prevê três enquadramentos possíveis de responsabilidade civil. A responsabilidade pelo tratamento ilícito (art. 42, *caput*) alcança danos decorrentes de violações à legislação de proteção de dados pessoais causados pelo controlador ou operador. A responsabilidade pelo tratamento indevido (art. 44, parágrafo único), por sua vez, disciplina os danos decorrentes de omissão dos agentes de tratamento quanto ao dever de adotar medidas de segurança estabelecidas pela Autoridade Nacional de Proteção de Dados. Por fim, há a responsabilidade pelo tratamento irregular por violação à expectativa de segurança do titular de dados (art. 44, *caput*, segunda parte, da LGPD).

Em relação aos danos causados em um tratamento irregular de dados pessoais, o dever de segurança imputável aos agentes de tratamento assume duas feições. Por um lado, a segurança tutelada pela LGPD traduz o dever de adotar medidas de segurança impostas pela ANPD, sob risco de configurar um tratamento inadequado de dados pessoais (art. 44, parágrafo único c/c art. 46, *caput* e §1º). Por outro lado, esse dever traduz a exigência de atender à legítima expectativa de segurança esperada daqueles que exercem a atividade de tratamento de dados

pessoais em caráter profissional (MARQUES, MIRAGEM, 2023), cuja inobservância apresenta conformidade com a espécie de tratamento de dados irregular prevista no art. 44, *caput*, segunda parte.

Quanto ao conteúdo do dever de segurança dos dados abordado pela LGPD, demonstra-se que as situações acidentais são tuteladas por duas vertentes de proteção. Identificar a espécie ou modalidade de responsabilidade civil que se enquadra em determinada hipótese de violação de um dever de segurança exige a compreensão do próprio conteúdo de "segurança de dados" disciplinada pela LGPD.

Importante desdobramento da análise do art. 44, caput, segunda parte, é constatar que, diferentemente do tratamento irregular por violação à legislação (art. 44, caput, primeira parte), não se exige a demonstração de vínculo do dano a uma violação de conduta específica e previamente definida imputável ao agente de tratamento. Em outras palavras, comparando-se com o regime de tratamento indevido, a violação da expectativa de segurança revela possibilidade mais abrangente de imputar a responsabilidade civil por atos de terceiros. O foco dessa responsabilidade não é a parametrização da conduta do agente de tratamento, mas sim a tutela do dano suportado pela vítima.

O fato de a tutela à expectativa de segurança do titular ser mais abrangente que as demais modalidades acompanha a necessidade de serem definidos limites ainda mais específicos para conferir objetividade na análise de casos concretos. A responsabilidade civil pela violação à expectativa de segurança não pode ser tomada como uma responsabilidade integral, sob pena de subverter os próprios propósitos da responsabilidade civil: o de garantir proteção ao titular de dados sem que isso implique obstáculo ao desenvolvimento tecnológico e à circulação de informações que pautam as relações da sociedade moderna (fundamentos do art. 2º, da LGPD).

9.1 Conteúdo do dever de segurança nas atividades de tratamento de dados pessoais.

O conteúdo do dever de segurança exigido nas atividades de tratamento de dados pessoais assume nítido propósito de impor, aos agentes de tratamento, a obrigação de considerar os riscos de sua atividade e o correspondente dever de adotar medidas aptas a evitar incidentes de segurança (MENKE; GOULART, 2023) ou que sejam aptas a mitigar danos ou riscos diante de sua ocorrência (art. 48, §2º[67]).

[67] Art. 48. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.

Cabe especificar que o emprego dos termos "incidente de segurança" para se referir a situações de violação da segurança de dados pessoais se deve ao fato de ser a expressão utilizada no art. 48, da LGPD: "*o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares*." Ademais, a normativa tangencia também essa expressão ao mencionar o dever de evitar "situações acidentais" no art. 6º, VII e art. 46, *caput*.

O art. 46, *caput*, da LGPD, reforça o propósito preventivo do dever de segurança, pois determina aos agentes de tratamento o dever de adotar medidas de segurança, técnicas e administrativas *aptas* a proteger os dados pessoais de situações acidentais ou ilícitas. A segurança compreendida como o dever de adotar medidas *aptas* a proteger os dados pessoais desses tipos de situações também é abordada como princípio no art. 6º, VII, da LGPD (princípio da prevenção). A compreensão do que seria uma medida *apta* nem sempre se mostra evidente diante de casos concretos. Uma das formas de preencher seu conteúdo pode ser extraído do §1º, do art. 46, da LGPD, o qual atribui à autoridade nacional a incumbência de estabelecer guias e parâmetros que devem ser adotados em um tratamento de dados pessoais.

Dessa exposição, cabe o seguinte questionamento: uma atividade de tratamento de dados pessoais que se adeque aos guias e parâmetros adotados pela ANPD atende a todo conteúdo do dever de segurança imposto pela LGPD? Em outras palavras, a conformação de uma atividade aos regulamentos da ANPD esgota o conteúdo do dever de segurança para fins de imputação de responsabilidade? A análise integrada dos dispositivos da LGPD indica uma resposta negativa a esses questionamentos.

Fabiano Menke e Guilherme Goulart (2023) ressaltam que o art. 46, da LGPD, prevê o dever de observar medidas de segurança tanto na fase de concepção quanto na fase da execução da atividade de tratamento de dados. O dever de segurança na fase de *concepção* envolve o que se convencionou denominar de *privacy by design*, o que, de modo geral, implica o compromisso do agente de tratamento com padrões de proteção muitas vezes mais rigorosos do que os impostos pelas próprias regulamentações de proteção de dados[68].

Ademais, os autores apontam que o dever de segurança também integra a seção que trata das Boas Práticas e da Governança (arts. 50 e 51, LGPD). Para o estabelecimento de boas práticas, são elencados critérios para o preenchimento do dever de segurança, como a consideração da natureza, escopo, finalidade, probabilidade e gravidade dos riscos (art. 50, §1º)

[68] Informação sobre o conteúdo de *privacy by design* disponível em: https://getprivacy.com.br/privacy-by-design-lgpd/ Acesso em 24/05/2023.

e da estrutura, escala e volume das operações, bem como a sensibilidade dos dados tratados e a probabilidade e gravidade dos danos para o titular dos dados (art. 50, §2º). Tais dispositivos relacionam a segurança dos dados com o dever de controle dos riscos da própria atividade – o que demonstra o envolvimento de um conteúdo muito mais abrangente e não limitado aos regulamentos definidos pela ANPD.

O dever de segurança, portanto, traduz a imposição de uma postura proativa e preventiva de danos aos agentes de tratamento os quais devem, por meios próprios e não limitados aos guias e parâmetros estabelecidos pela ANPD, realizar a avaliação e gestão de riscos tanto na concepção de uma atividade de tratamento de dados como durante todo o ciclo de processamento dos dados pessoais.

Nesse sentido, de fato há uma intensa correlação entre o dever de segurança (art. 6º, VII) e o dever de prevenção (art. 6º, VIII) – abordado pela LGPD como a obrigação de adotar medidas aptas a prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. O conhecimento do risco e a previsão das medidas de controle e de mitigação de riscos também são requisitos estipulados na LGPD em outros dispositivos para efetivar o cumprimento do dever de segurança – como no art. 38, quanto à elaboração do relatório de impacto à proteção de dados pessoais.

Ocorre que só se previne aquilo que é previsível. A despeito da adoção de medidas técnicas e administrativas de segurança de dados para evitar tratamentos inadequados ou incidentes de segurança, a exemplo de um vazamento de dados (*data breaches*), é possível que estes ocorram sem a possibilidade de tomar medidas para contê-los.

Para esses casos, o conteúdo da segurança dos dados disciplinado pela LGPD também envolve a previsão de medidas para mitigar danos, como o dever de notificação à autoridade nacional de proteção de dados bem como ao titular dos dados pessoais (art. 48) para que aquela possa tomar medidas administrativas de controle posterior e este possa adotar medidas particulares de proteção de seus dados.

Para a finalidade de conceituar as situações que impõem esse dever de notificação, cabe notar que o artigo que elenca os conceitos utilizados pela LGPD (art. 5º) não traz a definição de incidente de segurança, vazamento ou violação de dados pessoais. É possível extrair da LGPD expressão equivalente a essas hipóteses e retratar esses casos como uma "situação acidental", descrita (exemplificadamente e não de modo taxativo) como acessos não autorizados e situações de destruição, perda, alteração ou comunicação não autorizada dos dados pessoais (art. 46, *caput*).

Ressalte-se que, para fins de comunicação à ANPD e ao titular, não é todo incidente que deve ser noticiado pelo agente de tratamento, mas apenas aquele que "*possa acarretar risco ou dano relevante aos titulares de dados*" (art. 48, *caput*, LGPD). Portanto, o dever de comunicação surge quando há um "incidente relevante" (MENKE, GOULART, 2023), o qual exige um juízo de ponderação da gravidade da situação. A avaliação da gravidade, por sua vez, é realizada mediante avaliação e comprovação de que foram adotadas medidas técnicas adequadas para tornarem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los (art. 48, §3º).

Nesses termos, um incidente que envolva um vazamento de dados criptografados cuja legibilidade por terceiros se torne impossível ou uma situação acidental na qual os sistemas de acesso fiquem fora do ar por um curto período de tempo não seriam, em tese, relevantes e dispensariam sua comunicação à autoridade nacional ou ao titular.

Fabiano Menke e Guilherme Goulart (2023, pág. 353) densificam essa noção e apresentam o conceito de "incidente relevante" como aquele que atinja os titulares dos dados pessoais por meio da divulgação ou alteração não autorizada dos dados pessoais, ao que definem como o comprometimento da confidencialidade e da integridade dessas informações. Nesses termos, incidente relevante é aquele que acarreta o comprometimento da confidencialidade ou da integridade dos dados pessoais.

Cabe notar que o conteúdo do dever de segurança, pela exposição apresentada, se volta à finalidade de descrever o dever de prevenção, imputável ao agente de tratamento, e delinear os parâmetros para aferir a relevância de um incidente de segurança para adoção de correspondentes medidas para mitigação de riscos e danos, tais como o dever de notificação e implementação de medidas protetivas posteriores pela ANPD.

Para fins de imputação de responsabilidade, tais parâmetros são exigidos da autoridade nacional tanto para aferir a gravidade de um incidente como para graduar a aplicação de sanções administrativas (art. 52, LGPD). Para além da natureza administrativa, cabe o questionamento: esse conteúdo de segurança é extensível e suficiente para fins de atribuição de responsabilidade civil ao agente de tratamento?

Esse simples questionamento abrange diversos desdobramentos. O tema envolve o próprio conteúdo de segurança dos dados tutelado pela LGPD para fins de responsabilização civil, aspectos que conduzem à configuração do dano e à comprovação de nexo de causalidade para imputar eventual dever de indenizar a um agente de tratamento.

Em primeiro lugar, cabe notar que o tratamento inadequado (art. 44, parágrafo único) e o tratamento que viola a expectativa de segurança do titular de dados (art. 44, *caput*, segunda

parte) envolvem circunstâncias distintas. Há tratamento inadequado quando o dano decorre de inobservância de regulamentos estabelecidos pela ANPD (art. 46, *caput* e §1º). Nesse sentido, há uma correlação do dever de segurança imputável aos agentes de tratamento com o aspecto preventivo de um tratamento de dados e com o dever de mitigação de riscos e danos diante de um incidente.

Por outro lado, a técnica legislativa empregada pela LGPD para o tratamento irregular que viola a expectativa de segurança do titular de dados se aproxima notoriamente daquela adotada pelo Código de Defesa do Consumidor ao disciplinar o regime do fato do produto e do serviço (artigos 12 a 17), em especial na definição de critérios a serem considerados para a determinar o atendimento do dever de segurança (artigos 12, §1º e 14, §1º, CDC). Tratando-se de danos decorrentes do tratamento irregular de dados pessoais, o art. 45, LGPD, conduz tais situações ao regime de responsabilidade pelo fato do serviço (art. 14, CDC).

Por essa perspectiva, ao conteúdo do dever de segurança com foco na prevenção e mitigação de danos e riscos soma-se, sob a tutela da LGPD, à perspectiva de segurança do titular, pautada não apenas por guias e parâmetros da ANPD (art. 46, §1º), pela segurança na concepção e durante todo o ciclo de tratamento de dados (art. 46, §2º) e pela formulação de boas práticas e da Governança (art. 50 e 51), mas também pelas circunstâncias relevantes descritas nos incisos do art. 44, da LGPD. Por essa última perspectiva, pela proximidade de técnicas legislativas entre a LGPD e o CDC, a descrição da segurança de produtos e serviços pela disciplina da proteção ao consumidor pode ser utilizada para densificar o conteúdo de segurança esperado pelos titulares de dados, com especial importância para as consequências de sua violação e análise de excludentes de responsabilidade.

É preciso reforçar que a análise da legítima expectativa de segurança de um produto ou serviço, conforme tratada pela disciplina direito do consumidor, é útil, mas deve ser utilizada com cautela para pautar os contornos da expectativa de segurança do titular de dados pessoais. Não pode ser feita a mera transposição de conceitos. A tutela da expectativa de segurança da pessoa natural é ampla, mas não pode ser ilimitada, sob o risco de subverter o progresso tecnológico ou os próprios propósitos da LGPD. Até porque os fundamentos previstos no art.

2º, da LGPD, determinam a conciliação da tutela do titular de dados (art. 2º, incisos I, II, III, IV e VII)[69] com o desenvolvimento tecnológico e a livre iniciativa (art. 2º, incisos V e VI)[70].

Em última análise, o regime de responsabilidade civil que tutela a proteção dos dados pessoais, especialmente quanto à tutela de sua legítima expectativa de segurança, não pode estabelecer uma *ditadura do titular de dados* a converter todo e qualquer dano ao titular como uma violação de sua legítima expectativa de segurança. A própria LGPD determina parâmetros para sua aferição (art. 44, incisos) como o modo pelo qual é realizado; o resultado e os riscos que do tratamento razoavelmente se esperam e as técnicas e tecnologias disponíveis à época em que foi realizado.

9.1.1 Situações acidentais: vertentes de proteção à Segurança de Dados pela LGPD.

Pela perspectiva da responsabilidade civil, a análise da segurança de dados tutelada pela LGPD pode ser direcionada a duas vertentes: uma traduz o dever de adotar medidas de segurança impostas pela Autoridade Nacional de Proteção de Dados (ANPD) e a outra tutela a expectativa de segurança do titular. A adoção de medidas de segurança se liga à obrigação geral de atender à legislação, cujo propósito é voltado a regular a conduta do operador ou controlador de dados. A expectativa de segurança, por sua vez, tem por foco a proteção do titular de dados e é pautada pelas bases de proteção à pessoa pelo ordenamento jurídico, ou seja, a consideração da tutela de dados pessoais como direito da personalidade ou expressão de sua dignidade.

A despeito de a LGPD não conceituar o que seria um "vazamento" de dados, é possível extrair o que a norma entende por situações acidentais a partir de seu art. 46, *caput*. O dispositivo trata do dever de adoção de medidas de segurança pelos agentes de tratamento que sejam aptas a "*proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito*." Situações ilícitas são aquelas que decorrem de uma conduta que viola a legislação de proteção de dados (nesse caso, faz-se referência à disciplina do tratamento ilícito). Situação acidental, por sua vez, é compreendida como as hipóteses em que ocorrem acessos

[69] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
[70] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;

não autorizados ou hipótese não intencional de destruição, perda, alteração ou comunicação de dados pessoais. A expressão "situação acidental" traduz o alcance da responsabilidade civil às situações de dano não intencionais ou não causadas diretamente pelos agentes de tratamento.

O art. 46 descreve duas formas de situações acidentais. A primeira vincula o dano porventura causado a uma omissão do agente de tratamento quanto ao seu dever de adotar medidas de segurança aptas a evitá-las, conforme padrões técnicos mínimos definidos pela ANPD. Há, nesse caso, a incidência da disciplina do tratamento inadequado de dados pessoais.

A segunda forma não atrai essa vinculação. Trata-se de uma circunstância em que o dano também decorre de acesso não autorizado ou de perda, alteração ou comunicação de dados pessoais, mas que não se vincula a uma conduta (por ação ou omissão) do agente de tratamento e não envolve, necessariamente, conteúdo regulado pela ANPD. A essa segunda forma de situação acidental que incide a disciplina o tratamento irregular por violação à expectativa de segurança do titular de dados.

Nesse sentido, panorama normativo de acordo com a proposta interpretativa e classificatória apresentada pode ser assim visualizada:

<table>
<tr><th colspan="4">Responsabilidade civil na LGPD</th></tr>
<tr><td>Esfera de proteção:</td><td colspan="2">Garantir que o tratamento de dados pessoais seja adequado à legislação</td><td>Assegurar que o tratamento forneça a segurança que o titular deles possa esperar</td></tr>
<tr><td>Consequência da violação:</td><td colspan="3">Tratamento Irregular (art. 44, caput)</td></tr>
<tr><td>Espécie de tratamento irregular:</td><td colspan="2">(1) Por deixar de observar a legislação (lato sensu).</td><td>(2) Por não atender à expectativa de segurança que o titular de dados possa esperar</td></tr>
<tr><td>Dispositivo:</td><td colspan="2">Art. 44, caput, primeira parte.</td><td>Art. 44, caput, segunda parte.</td></tr>
<tr><td>Modalidade de responsabilidade:</td><td>Responsabilidade pelo tratamento ilícito</td><td>Responsabilidade pelo tratamento indevido</td><td>Responsabilidade por tratamento que viola expectativa de segurança</td></tr>
<tr><td>Dispositivo</td><td>Art. 44, caput, primeira parte e art. 42, caput</td><td>Art. 44, caput, primeira parte, art. 44, parágrafo único e art. 46, §1º.</td><td>Art. 44, caput, segunda parte.</td></tr>
</table>

Atuação do agente de tratamento:	Ação	Omissão	*Sem vinculação específica*.
Causa do dano:	Dano por situação comissiva	Dano por situação acidental (art. 46) Ex.: "Vazamento de dados" (*data breach*)	
Tipo de dano:	Dano por ato próprio	Dano por ato de terceiro	
Fato danoso:	Controlador ou operador viola disposição da LGPD	Controlador ou operador deixa de adotar medida de segurança definida pela ANPD.	Controlador ou operador não atende a uma expectativa subjetiva do titular avaliada *in concreto*.

O tratamento ilícito decorre de uma violação de deveres decorrentes de normas de proteção de dados (LGPD). O dano decorre de ato próprio. No caso de lesão ao titular de dados, consequente de um tratamento realizado pelo agente de tratamento, incide a responsabilidade prevista no art. 42, caput. Por outro lado, o tratamento inadequado configura-se quando houver uma situação de acesso não autorizado e de situações acidentais (como um *data breach*) decorrentes da omissões ne adoção de padrões técnicos de segurança parametrizados pela Autoridade Nacional de Proteção de Dados. O dano é causado por ato de terceiro, vinculado a uma omissão imputável ao agente de tratamento. Nesse caso, a responsabilidade pelos danos atrai a incidência do art. 44, parágrafo único, da LGPD .

A descrição do tipo de fato danoso para a classificação proposta se presta a evidenciar a confrontação de uma situação danosa a uma conduta esperada pelo agente de tratamento. Para configurar o tratamento ilícito ou indevido, deve haver uma definição prévia de conduta esperada pelo controlador ou operador – seja na lei, seja em regulamento pela ANPD. A ausência de uma definição prévia de conduta descaracteriza a responsabilidade civil por essas modalidades. Essa exigência, por outro lado, não é replicada para a configuração da responsabilidade civil por violação à expectativa de segurança do titular de dados (art. 44, *caput* , segunda parte).

Identificadas possíveis vertentes de tutela a situações acidentais, nas quais os danos são comumente causados por terceiros, essa exposição auxilia na compreensão das distintas circunstâncias que atraem a incidência da responsabilidade civil seja pela perspectiva de um tratamento inadequado, seja pela do tratamento que não atende a uma expectativa de segurança

do titular. Quanto à última, a especificação do que seria uma expectativa cuja violação enseja o dever de indenizar exige a consideração de sua proximidade legislativa com o conceito de defeito do serviço, disciplinado pelo CDC (art. 14, §1º). É o que se passa a analisar.

9.1.2 Da expectativa relevante e do potencial lesivo de um tratamento de dados: quais os riscos tolerados pela LGPD?

A violação ou incidente de segurança é muitas vezes anunciada como "*vazamento de dados pessoais*" ou "*data breach*". Desafio que se coloca nesse ponto é definir se a violação aos direitos do titular de dados é uma consequência inerente vazamento de dados – ou seja, se os danos são *in re ipsa*, isto é, decorrentes do próprio fato de constatar um vazamento. A importância desse aspecto reflete diretamente na composição do dano e na configuração de um dever de indenizar.

Fabiano Menke e Guilherme Goulart ressaltam que, para atrair consequências previstas na LGPD, tal como o dever de notificação à Autoridade Nacional (art. 48, da LGPD) e comunicação às potenciais vítimas, o incidente deve ser *relevante*. Para os autores, relevante é o incidente que atinge os titulares por meio da divulgação (comprometimento da confidencialidade) ou alteração (comprometimento da integridade) dos dados pessoais. Para reforçar que não é todo incidente que caracteriza risco ou dano relevante aos titulares, os autores trazem exemplo elucidativo (2023, págs. 352-353):

> Dessa forma, a comunicação [à Autoridade Nacional ou aos titulares] deve ser realizada em situações em que o incidente "possa acarretar risco ou dano relevante aos titulares", o que significa que não é todo incidente de segurança que deve ser comunicado. [...]
> Isso significa que um incidente no qual os dados tenham vazado, mas estejam criptografados de tal forma que sua leitura fique impossibilitada, torna o incidente menos grave.
> [...]
> Um incidente de segurança que deixe os sistemas informáticos fora do ar por algumas horas, mesmo que torne os sistemas indisponíveis, não precisa ser comunicado aos clientes se não houver comprometimento de dados pessoais. No entanto, um incidente que tenha como efeito a perda irreversível de dados pessoais deve ser comunicado, eis que prejudica (ou impede o exercício) (d)os direitos do titular, conforme o art. 18, da LGPD.

Nesses termos, é coerente inferir que, se um incidente de dados não assume relevância suficiente para ser comunicado à Autoridade Nacional de Dados Pessoais ou aos titulares de dados envolvidos, também não assumirá relevância para acarretar danos suscetíveis a atrair a

responsabilidade civil do agente de tratamento. Pelo raciocínio exposto, a violação da expectativa de segurança deve ser *relevante*, ou seja, acarretar o comprometimento da confidencialidade ou da integridade dos dados pessoais para ensejar um dever de indenizar.

Esse cenário revela que a LGPD não proíbe o tratamento de dados que, por sua natureza, envolvam riscos e potencial lesivo aos titulares. O CDC complementa esse entendimento ao tutelar tanto a funcionalidade quanto a segurança dos produtos e serviços colocados em circulação no mercado de consumo. A qualidade não é comprometida pelo mero fato de um produto ou serviço oferecer periculosidade inerente. Isso porque uma faca deve cortar, um inseticida deve dedetizar e uma solução de água sanitária (hipoclorito de sódio) deve destruir microrganismos patogênicos. O dever de qualidade é atendido quando tanto a funcionalidade quanto a segurança são satisfeitas. Tem qualidade, portanto, o produto ou serviço que atende à finalidade que lhe é inerente (funcionalidade) e não oferece risco *exagerado* à saúde ou ao patrimônio do consumidor (segurança). (BESSA, 2022).

O dever de qualidade não se confunde com uma proibição de comercializar produtos cuja periculosidade seja inerente ao seu propósito ou funcionamento (como uma faca, produtos de limpeza pesada ou inseticidas). Tratam-se de riscos normais e previsíveis. A responsabilidade pelo fato do produto e do serviço tutela o que foge dessa normalidade, ou seja, tutela a violação da expectativa de segurança que configura o *defeito* de um produto ou serviço (periculosidade adquirida). Nesse sentido (BESSA, 2022, pág. 114):

> existem produtos e serviços que trazem riscos intrínsecos (periculosidade inerente) e outros que, por falhas no processo de produção ou comercialização, tornam-se defeituosos (periculosidade adquirida). Ao direito do consumidor importam principalmente as situações de dano concernentes à periculosidade adquirida.
> [...]
> O produto ou serviço que não atende à exigência de segurança possui *vício de qualidade por insegurança* ou, como preferem alguns autores, *defeito*. A noção de *defeito*, para fins de caracterização da responsabilidade em questão, nem sempre coincide com sua ideia vulgar. O defeito do produto é conceito normativo que se vincula basicamente com a compreensão de legítima expectativa de segurança.

A maior periculosidade de produtos não implica na proibição de sua circulação, mas incrementa o dever de informação sobre os riscos de seu uso. A noção pode se refletir na disciplina de tratamento de dados, na medida em que o dever de informação se volta a atender ao fundamento da autodeterminação informativa do titular de dados (art. 2º, II, da LGPD), ou seja, posiciona a centralidade do titular na tomada de decisões que influenciem o exercício de

seus direitos e o livre desenvolvimento de sua personalidade (art. 2º, VII, da LGPD). Quanto maior o perigo de exposição ou de comprometimento da confidencialidade ou da integridade dos dados, maior o correspondente dever de informação sobre os riscos de um tratamento de dados.

Para o CDC, portanto, o fato de uma faca causar um corte a uma pessoa durante seu manuseio não tem, em princípio, aptidão para se conformar a um dano imprevisível, que foge da normalidade de seu uso regular e, nesses termos, não há configuração de defeito do produto. Afasta-se, nesses casos, a responsabilidade civil do fornecedor. Da mesma forma, a LGPD tolera riscos pelo tratamento de dados pessoais. Ocorre que os parâmetros para aferir o dano indenizável ainda são nebulosos. Ao contrário das modalidades de tratamento irregular por violação à legislação (seja na modalidade ilícita ou inadequada), a LGPD não indica, de forma expressa ou direta, os pressupostos, desdobramentos ou consequências para o que denominou como "*violação à expectativa de segurança do titular de dados pessoais*."

Questões como o conteúdo da expectativa de segurança. da solidariedade dos agentes de tratamento e excludentes de responsabilidade indicam a necessidade de se realizar uma análise conjunta dos diplomas legais incidentes sobre o tema, em especial, o Código de Defesa do Consumidor e o Código Civil, com vistas a oferecer respostas consistentes não apenas com as disposições internas da própria LGPD, mas coerentes com as demais normativas do sistema jurídico.

A ausência de delimitações específicas e consolidadas incentiva a multiplicidade de ações judiciais e com a probabilidade de gerarem decisões com resultados diferentes para situações similares. Na busca da definição e limites da tutela à expectativa de segurança do titular de dados, as respostas podem ser encontradas (ou ao menos delineadas) com base na integração normativa proporcionada pelos arts, 45 e 64, da LGPD. Trata-se de buscar não apenas a convergências de conceitos de normativas distintas (CDC e LGPD), mas também da própria disciplina de responsabilidade civil. Nesses termos, o propósito de conferir efetividade da tutela à expectativa de segurança do titular de dados revela-se como um dos pontos mais importantes da aplicação do diálogo das fontes à responsabilidade civil disciplinada pela LGPD.

A tutela de danos por essa modalidade é mais ampla do que as demais previstas na LGPD, mas a identificação de cada pressuposto apresenta dificuldades. Sobre o evento danoso, abre-se a possibilidade de imputar a responsabilidade àquele que não realizou, ao menos diretamente, o tratamento de dados pessoais. À par da responsabilidade pelo fato do serviço, (art. 14, do CDC), qualquer fornecedor que tenha integrado a cadeia de fornecimento pode ser acionado para responder pelos danos sofridos pelo consumidor. Eventual ressarcimento deve

ser buscado pelo exercício do direito de regresso. Como paralelo, seria possível imputar o dever de responder por danos àquele agente de tratamento que estivesse em "guarda" dos dados pessoais violados – ainda que tenha cumprido todos os requisitos previstos na legislação *lato sensu*.

O dano, por sua vez, é muitas vezes de difícil percepção e comprovação. A utilização de dados pessoais é notadamente difusa e dispersa-se para os mais variados propósitos. A exposição indevida, o processamento sem base legitimadora e outras formas clandestinas de tratamento de dados nem sempre são sentidos pelo titular e, muitas vezes, representam um incômodo "*normalizado*" no cotidiano, como o *mailing list*, caracterizado pela venda de cadastros de clientes – como aqueles registrados em supermercados ou lojas – para a prospecção de serviços ou produtos de outras empresas. A venda nem sempre é autorizada de forma expressa na momento em que os dados são espontaneamente oferecidos pelo titular. Ligações ou e-mails incômodos são consequências muitas vezes toleradas, mas ainda assim decorrem, em princípio, de um tratamento irregular de dados pessoais.

A definição de uma expectativa de segurança que seja legítima compõe esse cenário de desafios para aquele que busca indenização pelos prejuízos sofridos. Quando um cliente fornece dados a um supermercado para participar de um sorteio ou facilitar futuras compras pode até não esperar que seus dados sejam vendidos para outras empresas. No entanto, para efeitos de comparação, a expectativa de segurança na tutela de dados pessoais processados por uma rede de supermercados é notadamente menor do que a esperada pelo tratamento de dados realizados por uma instituição financeira.

No caso de um vazamento de dados ou de um ataque *hacker*, a tolerância quanto à efetividade das medidas de segurança adotadas pela rede de supermercado será significativamente menor do que a esperada por uma instituição financeira. Para o caso do supermercado, é possível que a extensão de tolerância de danos seja maior e que a ausência da disponibilidade de tecnologias tenha mais peso para aferir sua responsabilidade. Caso não constatada uma legítima expectativa de segurança ou uma omissão quanto às medidas que deveriam ser adotas, não haverá responsabilidade nos moldes definidos pela LGPD.

Ocorre que, mesmo que constatada a violação de segurança, há decisões que compreendem que o vazamento de dados em si não é circunstância que atrai o dever de indenizar. É o exemplo de caso enfrentado pelo Tribunal de Justiça do Estado de São Paulo

(TJSP),[71] no qual foi constatada a quebra de segurança no acesso de dados de clientes preservados por uma empresa concessionária de energia elétrica.

Ainda que tais dados tenham sido compilados e disponibilizados para comércio não autorizado ou fins ilícitos, o TJSP afastou a tese de que a responsabilidade da *possuidora* de dados (controladora ou operadora) decorre da simples quebra do dever de guardo dos usuários. Em outras palavras, para essa turma do TJSP, eventual responsabilidade não decorre da mera constatação do vazamento de dados, como o seria caso uma vez considerado que o dano fosse *in re ipsa*. Exigiu-se a comprovação de danos efetivos (não hipotéticos). Ausente a indicação específica de transtornos do vazamento de dados, não haveria dever de indenizar, tratando-se o caso como hipótese de mero aborrecimento.

Pelo exposto, demonstra-se que, no contexto de um tratamento irregular por violar a expectativa de segurança de dados, surgem diversas perguntas que ultrapassam a consideração da relevância dessa expectativa, mesmo que o tema encontre inspiração no modelo de tutela ao fato do serviço, pelo CDC). Da análise da responsabilidade civil na espécie violação da expectativa de segurança do titular dos dados pessoais, desdobram-se inúmeros questionamentos sobre os seus elementos.

De início, cabe considerar como pressuposto inafastável para eventual imputação de um dever de indenizar que a responsabilidade civil pressupõe a ocorrência de um dano (CAVALIERI, 2007). No entanto, para fins de responsabilidade por quebra à legítima expectativa de segurança do titular de dados, cabe a compreensão e resposta a diversos questionamentos sobre o que ou de que modo restará configurado esse elemento, tais como: a colocação dos dados em risco implica dano indenizável? O comprometimento da confidencialidade dos dados implica no reconhecimento de violação suscetível de reparação aos titulares de dados? Em outras palavras, a constatação de um vazamento de dados é evento suficiente para ensejar um dever de indenizar? Ademais, como vincular um incidente de segurança a um agente de tratamento de dados? Para essa finalidade, seria possível presumir um vazamento de dados pessoais?

Ainda sobre os pressupostos da responsabilidade civil por violação à legítima expectativa de segurança do titular de dados e possíveis excludentes de responsabilidade, exsurgem questionamentos a respeito dos parâmetros necessários para avaliar uma violação de segurança. Nesse sentido, cabem as seguintes perguntas: o atendimento ao dever de prevenção

[71] (TJ-SP - AC: 10009305420218260005 SP 1000930-54.2021.8.26.0005, Relator: Lavínio Donizetti Paschoalão, Data de Julgamento: 30/03/2022, 14ª Câmara de Direito Privado, Data de Publicação: 31/03/2022)

afasta a responsabilidade civil do agente de tratamento? Na medida em que só se previne o que é previsível, é possível imputar o dever de indenizar diante de danos imprevisíveis ou inevitáveis? Em caso afirmativo, qual o conteúdo que ultrapassa o dever de prevenção (aferido antes de um incidente) e o de mitigar danos e riscos após um incidente? É o que se passa a detalhar.

9.2 Parâmetros para aferir a expectativa de segurança: do defeito do serviço

A expressão "*expectativa de segurança*", prevista no art. 44, *caput* (segunda parte), da LGPD, encontra nítida inspiração na disciplina de responsabilidade civil pelo fato do produto e do serviço prevista no CDC (MARQUES, MIRAGEM; 2023). A norma de proteção ao consumidor conceitua como defeituoso o produto que não oferece a segurança que dele legitimamente se espera, levando-se em conta os usos e riscos que razoavelmente são esperados (art. 12, §1º, CDC). Por sua vez, o conceito de serviço defeituoso é ainda mais explícito quanto à vinculação de expectativa subjetiva de uma pessoa, pois é caracterizado como aquele que "*não fornece a segurança que consumidor dele pode esperar*" levando-se em conta, ainda os resultados e riscos razoavelmente esperados (art. 14, §1º, do CDC).

A proximidade da técnica legislativa com a disciplina do fato do produto ou do serviço do CDC é amparada pelo disposto no art. 45, da LGPD[72], o que reforça a natureza objetiva da responsabilidade civil em análise – ou seja, prescinde-se da análise de culpa ou dolo do agente para sua configuração. Nesse sentido se posicionam Cláudia Lima Marques e Bruno Miragem (2023, p. 800 e 812):

> [...] a própria LGPD remete às leis especiais, o CDC, no art. 45 [...] hoje há que se priorizar a harmonia e a coordenação entre as normas do ordenamento jurídico (concebido como sistema unitário) e a 'coerência derivada ou restaurada' (*cohérence dérivée ou restaurée*), que se fará pelo 'di-a-logos' (uso derivado das várias lógicas) e não pela exclusão de uma lei superada pela lógica de outra [...]
> [...] Exige-se a falha do controlador ou do operador, que caracteriza o nexo causal do dano. Contudo, não se deve perquirir se a falha se dá por dolo ou culpa, senão que apenas sua constatação é suficiente para atribuição da responsabilidade, [...].
> A técnica legislativa empregada pela LGPD aproxima-se notoriamente daquela adotada pelo CDC ao disciplinar o regime do fato do produto e do serviço, em especial na definição dos critérios a serem considerados para determinação do atendimento ao dever de segurança.

[72] Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

É preciso levar em conta que os incisos do art. 44 impõem ao intérprete o dever de considerar as circunstâncias relevantes, dentre as quais destaca-se a necessidade de levar em conta as técnicas de tratamento disponíveis à época em que essa atividade foi realizada (art. 44, inciso III, da LGPD) – o que sinaliza, inclusive, uma opção legislativa pela não imputação dos riscos do desenvolvimento[73] ao agente de tratamento.

É possível pautar o que seria e quais os limites da expectativa de segurança do titular de dados – nos termos da LGPD – com base na consideração da vasta jurisprudência e doutrina a respeito da *legítima expectativa de segurança* dos produtos e serviços prevista no CDC. A segurança de um produto desconsidera, em um primeiro momento, a conduta do fornecedor e verifica apenas o produto em si, ou seja, se este não ofende a saúde, a segurança, os direitos da personalidade ou o patrimônio do consumidor (BESSA, 2022). A conduta do fornecedor é relevante em um segundo momento, se comprovada a incidência de alguma excludente de responsabilidade prevista na norma (art. 12, §3º, do CDC). Situação similar é a prevista na LGPD.

A delimitação conceitual da violação da expectativa de segurança é essencial para definir sua aptidão como argumento jurídico para gerar a responsabilidade civil. Não se trata de um novo conceito para a responsabilidade civil privada, tendo em vista que a expressão já é empregada para identificar defeitos para fins de apuração da responsabilidade pelo fato do produto ou do serviço (CDC). Ainda que a mera transposição de conceitos para incidências normativas distintas não seja recomendada, a LGPD propicia diálogos interdisciplinares em seu art. 45 e 64, o que viabiliza o emprego de parâmetros da tutela da expectativa de segurança pelo CDC também para atribuição de responsabilidade pela violação da expectativa de segurança do titular de dados pessoais, nos moldes previstos na LGPD.

A preocupação básica e central da disciplina da responsabilidade civil do fornecedor por acidentes de consumo é garantir que produtos e serviços lançados no mercado de consumo sejam seguros. No conceito de Leonardo Bessa (2022, p. 141), seguros são os produtos e serviços que "*não ofendam a saúde, a segurança, os direitos da personalidade e o patrimônio do consumidor*." Disciplinado nos arts. 12 a 17 do CDC, a denominada responsabilidade por fato do produto e do serviço estabelece o regime indenizatório quanto aos danos oriundos de

[73] Riscos de desenvolvimento são aqueles defeitos que, à época de sua concepção e colocação no mercado, eram desconhecidos pelos estudos científicos disponíveis pela comunidade acadêmica. (BESSA, 2022).

defeitos (também referidos como vícios de qualidade por insegurança ou, simplesmente, por vício de insegurança).

Para aferir um dever de indenizar por vício de qualidade por insegurança, é fundamental, portanto, compreender o significado de defeito na prestação de um serviço. Para o art. 14, §1º, do CDC, defeituoso é o serviço que não fornece a segurança que o consumidor dele pode esperar ou, como também se refere a doutrina, aquele que não atende a uma *legítima* expectativa de segurança do consumidor (BESSA, 2022). A legitimidade de uma expectativa é definida de acordo com as circunstâncias relevantes do caso, como a época em que fornecido ou o modo de fornecimento. Essas disposições encontram eco na LGPD, que estabelece parâmetros similares para definir qual expectativa de segurança pode ensejar o dever de reparar (incisos do art. 44):

CDC	**LGPD**
Art. 14. § 1° O serviço é defeituoso quando não fornece a **segurança** que o consumidor dele pode esperar, levando-se em *consideração as circunstâncias relevantes*, entre as quais:	Art. 44. O tratamento de dados pessoais será irregular quando [...] não fornecer a **segurança** que o titular dele pode esperar, *consideradas as circunstâncias releva*ntes, entre as quais:
I - o **modo** de seu fornecimento;	I - o **modo** pelo qual é realizado;
II - o **resultado e os riscos** que razoavelmente dele se esperam;	II - o **resultado e os riscos** que razoavelmente dele se esperam;
III - a **época** em que foi fornecido.	III - as técnicas de tratamento de dados pessoais disponíveis à **época** em que foi realizado.

Tabela 21 - Comparação entre os parâmetros de segurança previstos no CDC e na LGPD.

Tanto o CDC quanto a LGPD aceitam níveis de riscos nas atividades que regulam. Em outras palavras, esses diplomas normativos não proíbem atividades pelo simples fato de apresentarem algum tipo de periculosidade. O art. 14, §2º, do CDC, estabelece que o serviço não é considerado defeituoso pela adoção de novas técnicas. A LGPD, de modo similar, afirma que a apuração da violação de segurança depende das técnicas disponíveis à época em que o tratamento foi realizado (art. 44, III). Para Leonardo Bessa, pela perspectiva da proteção ao consumidor, tal opção normativa é adequada pois permite a promoção da competitividade e atendimento de interesses de consumidores com menor renda (BESSA, 2022, p. 142).

Pela perspectiva da tutela de dados, pode-se afirmar que reprodução dessa opção, na lei nacional de proteção de dados pessoais, visa fomentar o emprego de tecnologias inovadoras sem atribuir carga de responsabilidade excessiva ao agente de tratamento o que, em última análise, promove e incentiva o desenvolvimento tecnológico e a inovação. Primeiro ponto

relevante para aferir a *legítima* expectativa de segurança do titular de dados, portanto, é considerar a tecnologia disponível à época em que o tratamento foi realizado.

Em segundo momento, deve-se aferir se a superveniência de novas técnicas de segurança foi incorporada ao setor ou ao propósito do tratamento realizado pelo agente. Em outras palavras, a superveniência de uma nova tecnologia deve se apresentar como exigência *que se tornou* inerente ao tratamento de dados na área em que é exercido. Isso porque a disponibilização de um método mais avançado tradicionalmente se apresenta como medida de alto custo.

O barateamento decorre da "normalização" do que já foi considerado como novidade e que, com o passar do tempo, se torna uma condição inerente ao exercício da atividade (BESSA, 2022). A exigência de arcar com tecnologias de alto custo pode ser desproporcional ao tratamento de dados por uma rede de supermercados, por exemplo, mas, ao mesmo tempo, ser compatível com o nível de segurança exigido na atividade exercida por instituições financeiras. Trata-se, portanto, de análise que envolve não apenas a constatação de disponibilidade de uma tecnologia de segurança no mercado, mas se também é possível identificar um dever de atualização técnica imputável.

A aferição da legítima expectativa de segurança, portanto, não é estanque: varia de acordo com o tempo e com o risco inerente à atividade exercida. Em outras palavras, a segurança que legitimamente pode ser esperada pelo titular de dados depende tanto da tecnologia disponível à época do tratamento de dados quanto da periculosidade da área ou propósito da atividade para a qual é exercida.

O dever de segurança da informação integra a regulação da atividade de tratamento de dados. Pelo viés do dever de observar a legislação *lato sensu*, o regime de responsabilidade civil previsto na LGPD define as *circunstâncias* e *propósitos* que legitimam o tratamento de dados, o que é complementado pela perspectiva do dever de segurança nessa atividade, ou seja, a delimitação de *critérios* para controle de riscos na produção, coleta e utilização de informações relacionadas às pessoas naturais.

Em síntese, a correlação dos regimes de responsabilidade na forma do diálogo das fontes com a proteção do consumidor definida em legislação específica propicia ampla tutela ao titular de dados pessoais, mas não de forma ilimitada.

Como sustentado, a violação à expectativa de segurança é verificada caso a caso e deve atender a parâmetros indicados pela norma: 1) a disponibilidade da tecnologia à época em que os dados foram tratados e 2) a internalização da medida de segurança de acordo com as possibilidades e necessidades relativas ao propósito da atividade de tratamento e aos riscos da

área. Há um terceiro ponto relevante na identificação do dever de indenizar pela violação à expectativa de segurança. Trata-se da avaliação da participação da vítima nos prejuízos sofridos.

A contribuição da pessoa que sofre danos pelo tratamento irregular de dados pessoais influencia tanto na configuração da responsabilidade civil quanto na definição do *quantum* ressarcitório que será imputado ao responsável. Essa premissa influencia na mensuração de segurança esperada e, por consequência, na análise de responsabilidade civil em casos práticos. Ponto central na tutela da pessoa pela perspectiva de desequilíbrios entre as partes nas relações de consumo ou nas de tratamento de dados pessoais passa, portanto, pela consideração dos reais riscos que foram assumidos pela vítima (consumidora e/ou titular de dados).

Nesse sentido, os parâmetros para aferir a legítima expectativa de segurança do titular de dados pode ser assim representada:

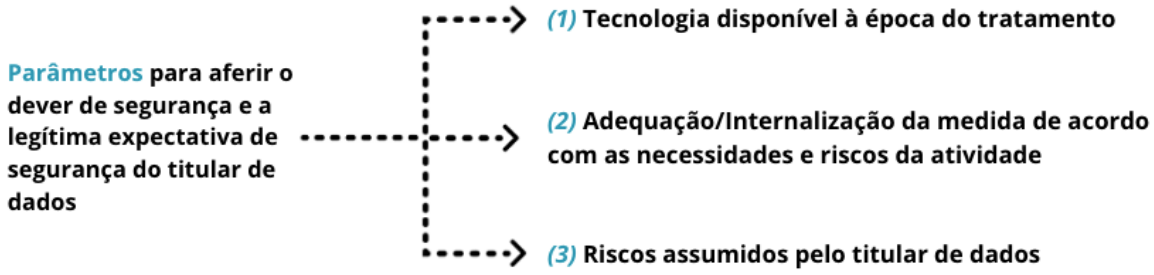

Figura 21 - Parâmetros para aferir a legítima expectativa de segurança pelo titular de dados pessoais

Nota-se, que o conteúdo do dever de segurança envolve a noção de que a segurança que se espera não é a dos dados em si, mas dos sistemas que os mantém. Nesse sentido, para Fabiano Menke e Guilherme Goulart (2023), ultrapassa o dever de segurança aquilo que não é previsto, uma vez que só se pode evitar aquilo que é previsível. Ocorre que essa perspectiva é diferente da tratada no presente tópico, uma vez que a segurança da expectativa, nos moldes do definido pelo CDC, corresponde à configuração do defeito. Inseguro é aquele produto ou serviço que apresenta riscos à incolumidade do consumidor e de terceiro (BESSA, 2022). A responsabilidade civil, para esses casos, não é afastada diante da imprevisibilidade de um dano, mas pela avaliação de sua periculosidade ser a esperada de acordo com os parâmetros definidos.

Por esse raciocínio, a responsabilidade civil pela violação à expectativa de segurança do titular exige a comprovação de que essa expectativa seja adequada ou, porque não dizer, *legítima* – como se refere a disciplina de direito do consumidor quanto ao fato do produto ou serviço.

9.3 Da comprovação do dano à expectativa legítima de segurança de dados: posicionamento dos tribunais.

Quanto à responsabilidade civil disciplinada pela LGPD, configura violação à expectativa de segurança o incidente *relevante*, compreendido como aquele que compromete a confidencialidade ou integridade dos dados pessoais ou, por outra perspectiva, aquele apto a causar danos aos direitos da personalidade ou ao patrimônio do titular.

A noção de dano aos direitos da personalidade é controvertida na jurisprudência, especialmente quanto à tutela de dados pessoais. O uso não autorizado de imagem para fins comerciais, por exemplo, gera dever de indenizar independentemente de prova do prejuízo (Súmula 403-STJ), ao que se denomina como dano *in re ipsa* – decorrente do próprio fato de publicar sem autorização imagem de pessoa para atender a fins econômicos ou comerciais.

Por outro lado, o Superior Tribunal de Justiça concluiu, em 07/03/2023, que o vazamento de dados, apesar de ser uma falha indesejável, não tem capacidade de gerar dano moral indenizável de forma presumida. O Tribunal Superior diferenciou o caso de vazamento de dados pessoais de natureza comum (art. 5º, I, LGPD) daqueles classificados como sensíveis (art. 5º, II, LGPD) e sinalizou que a comprovação de um dano somente seria dispensável para o último. Tratando-se de dados comuns (entendidos pelo tribunal como aqueles que não digam respeito à intimidade da pessoa natural, mas apenas à sua identificação), eventual pedido de indenização exige comprovação de efetivo prejuízo gerado pela exposição ao passo que o dano *in re ipsa* apenas seria reconhecido aos dados sensíveis. Destaque-se trechos da ementa desse julgado:

> I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.
> [...]
> 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 moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.
> (STJ - AREsp: 2130619 SP 2022/0152262-2, Data de Julgamento: 07/03/2023, T2 - SEGUNDA TURMA, Data de Publicação: DJe 10/03/2023)

No caso apresentado, o STJ compreendeu que o dever de indenizar restou afastado pela ausência de comprovação pressuposto da responsabilidade civil, qual seja, o dano.

Em sentido similar, o TJDFT considerou que dados como número telefônico e endereço de e-mail podem ser obtidos por mera pesquisa na internet de modo que a oferta de produtos e serviços por meio de ligações telefônicas não violam, por si só, os atributos da personalidade da pessoa (arts. 12 c/c 186 do Código Civil) tampouco configuram uso ilícito de dados pessoais. A oferta de serviço por ligações telefônicas não se trata de fato passível de reparação ou que viola a LGPD. Nesse sentido, o TJDFT assim pontuou:

> VII. Por fim, por inexistir indício de prova de que o número telefônico do requerente tenha sido obtido por meio de vazamentos de dados ou utilizado de forma ilícita, não se constata potencial violação à Lei Geral de Proteção de Dados Pessoais - LGDP atribuível às empresas." (grifo nosso)
>
> Acórdão 1635070, 07248075720228070016, Relator: FERNANDO ANTONIO TAVERNARD LIMA, Terceira Turma Recursal dos Juizados Especiais do Distrito Federal, data de julgamento: 9/11/2022, publicado no DJe: 17/11/2022.

Acrescente-se a esses casos o entendimento da 27ª Câmara de Direito Privado do TJ-SP que, mesmo reconhecendo a falha na segurança de sistema da empresa como a causa que permitiu que terceiros (por ação de hackers) tivessem acesso a esses dados, negou qualquer ofensa aos direitos da personalidade dos consumidores afetados. Foi utilizado o argumento de que dados "comuns", amplamente ou comumente divulgados no cotidiano, não são aptos a ensejar, "*nem de longe*", ofensa aos direitos da personalidade de seus titulares. (TJ-SP - AC: 10083083520208260704 SP 1008308-35.2020.8.26.0704, Relator: Alfredo Attié, Data de Julgamento: 16/11/2021, 27ª Câmara de Direito Privado, Data de Publicação: 16/11/2021)

A dificuldade de se conceituar um *fato* danoso (como o vazamento de dados pessoais) pode ser mitigada pelos parâmetros que delimitam a expectativa de segurança do titular. No entanto, é comum que a *origem* de um vazamento seja de difícil constatação, ainda mais quando se considera que os dados pessoais podem obtidos de diversas fontes e pelos mais diferentes modos (sejam lícitos ou ilícitos). Cabe notar que, mesmo que obtidos de forma legítima, o tratamento de dados ainda pode ser irregular a depender do propósito para o qual é executado.

Quanto ao *dano*, há precedentes diversos que demonstram a dificuldade de sua comprovação. A despeito de ser tratado em alguns casos como dano *in re ipsa* (como na utilização de imagem não autorizada para fins comerciais), em outros, a efetiva demonstração de prejuízo não é reconhecida como um desdobramento evidente do próprio fato. Aliás, as vítimas podem nem ter conhecimento de que a integridade ou confidencialidade de seus dados

foram comprometidas. A demonstração de qual seria o prejuízo apto a demonstrar o dano necessário para a responsabilidade civil ainda não é bem delineada pela jurisprudência.

A contribuição da vítima com o próprio dano é considerada na aferição do dever de indenizar com parâmetros variáveis caso a caso. O fato de uma pessoa ter exposto seus dados na internet, por exemplo, já foi utilizado como argumento para afastar qualquer indenização pela utilização dos dados publicizados para propósitos distintos – ainda que utilizados para satirizar o titular. Em outro, a mudança de contexto da republicação de uma imagem, com a ridicularização da orientação sexual do titular, foi reconhecida como tratamento de dados para finalidade diversa da que motivou sua divulgação e determinada a responsabilidade civil daquele que realizou a postagem ofensiva.

Quanto ao primeiro exemplo, em 2015, o TJDFT afastou a responsabilidade de uma plataforma de rede social (*Facebook*) pelo compartilhamento de dados inseridos pelo próprio usuário, como imagens e informações identificadoras, no respectivo perfil virtual. No caso, um outro aplicativo criou perfis a partir da sincronização entre redes sociais, de modo a permitir que perfis do sexo oposto realizassem avaliações sobre os mais diversos aspectos de outra pessoa, como comentários sobre relacionamentos anteriores ou avaliações sobre sua personalidade, inclusive negativas e depreciativas. O Tribunal considerou que a perda da privacidade e a exposição de uma pessoa são consideradas como decorrências ínsitas da conta criada pelo próprio titular de dados. Restou vencido o voto minoritário no sentido de que haveria ofensa à imagem e à privacidade do usuário em razão da sincronização de dados sem prévia autorização. (Relator: Fábio Eduardo Marques, Relatora Designada: Sandra Reves Vasques Tonussi, 1ª Turma Recursal dos Juizados Especiais do Distrito Federal, Data de Julgamento: 18/08/2015, Publicado no DJE: 04/09/2015. Pág.: 251).

O segundo exemplo, por outro lado, envolveu a republicação, com legendas depreciativas, de fotografia tornada manifestamente pública pelo titular em seu próprio perfil no Facebook. A chacota de cunho homofóbico não foi tolerada pelo TJDFT como fator inerente a quem torna pública uma imagem em seu perfil. No caso, o tribunal reconheceu que o fato de os próprios usuários terem postado foto em suas redes sociais não significa permissão para que outras pessoas a republiquem, ao argumento de liberdade de expressão:

> DIREITO CIVIL. RESPONSABILIDADE CIVIL. PUBLICAÇÃO DE FOTO E COMENTÁRIOS OFENSIVOS EM REDE SOCIAL (FACEBOOK). INTENÇÃO DE RIDICULARIZAR E PROPAGAR AVERSÃO À ORIENTAÇÃO SEXUAL. OFENSA AO DIREITO À IMAGEM E À HONRA. DANOS MORAIS CARACTERIZADOS. RECURSO CONHECIDO E PROVIDO.

1. Trata-se de recurso inominado interposto pelos autores contra a sentença que julgou improcedente o pedido inicial, sob o fundamento de que, analisando o contexto no qual a foto e a mensagem foram postadas pelo réu em sua rede social, não haveria danos morais, na medida em que somente não teria tido abuso da liberdade de manifestação de pensamento.
2. Em suas razões recursais, os autores defendem que a publicação da foto com os comentários realizados na rede social Facebook ultrapassaram o limite da livre expressão, uma vez que o objetivo era difundir preconceito em relação aos homossexuais, atribuindo adjetivo negativo em nítido intuito difamatório e injuriador, devendo, por consectário, responder, o réu, pelo abuso que cometeu.
3. No caso em análise, os autores, que são noivos, fizeram uma foto em que ambos se vestiam de noivas e a publicaram em seu Instagram. Narram que o réu teve acesso ao registro e fez a **republicação da fotografia em sua própria rede social Facebook, utilizando-se de uma legenda ofensiva e discriminatória**, a que somou um comentário igualmente ofensivo de sua parte. Salientam que o requerido ainda se utilizou de *emojis* em seus comentários que expressam nojo, ódio e estranheza e que vários comentários foram incluídos por outras pessoas na postagem do réu, também homofóbicos e violadores da honra dos autores.
4. **O fato de os próprios autores terem postado a foto em suas redes sociais não significa permissão para que outras pessoas a republiquem e, ao argumento de liberdade de expressão, ridicularizem no Facebook a orientação sexual deles**. 5. O acervo probatório dos autos demonstra que a republicação da foto feita pelo réu em sua rede social gerou diversos comentários preconceituosos e ofensivos aos autores. Citem-se alguns desses comentários: ?Reflexão profunda: um cara que não gosta de mulher tem mais é que tomar no c.. mesmo!...kkk. É inaceitável essas coisas de homem se vestir de noivinha! Ecaaaa! Ser gay não é desmunhecar. O jeito é rir para não chorar meu amigo, o mundo está perdido.
6. Merece destaque o fato de que o réu, ao ser confrontado em um comentário realizado na postagem da foto, sobre vir a responder na justiça pelos seus atos, ter respondido: resolvo fácil. E ainda diz que: eu gosto da resenha, bjao (ID 5244873). Tais comentários reforçam a ideia de que o réu realmente abusa de seu direito de expressar, fazendo menoscabo, até mesmo, da Justiça.
7. Por óbvio que foi a atitude do réu de ter postado em sua rede social a foto dos autores com a utilização da mencionada legenda, ela por si já bastante depreciativa, o fator que desencadeou os comentários igualmente depreciativos e homofóbicos das outras pessoas, devendo ser responsabilizado pelos prejuízos gerados pela sua conduta.
8. **A situação vivenciada pelos autores, independentemente da preexistência de postagem da mesma foto em sua própria rede social, certamente que superou os limites do mero aborrecimento**. Inegavelmente, foram eles submetidos à situação vexatória, humilhante, com potencial de causar forte dor íntima e transtornos de ordem emocional.
9. A liberdade de manifestação e de expressão é constitucionalmente assegurada a todos, mas o limite claro dela é não atingir os atributos da personalidade alheia injustamente. Nesse sentido, comentários em redes sociais que extrapolam o *animus narrandi*, ou seja, aquele de apenas relatar e informar a coletividade, com o fito apenas de promover a divulgação de ofensas morais devem ser indenizados. [...]
(TJ-DF 07100353120188070016 DF 0710035-31.2018.8.07.0016, Relator: Gabriela Jardon Guimaraes de Faria, Data de Julgamento: 07/11/2018, 2ª Turma Recursal dos Juizados Especiais Cíveis e Criminais do DF, Data de

Publicação: Publicado no DJE : 12/11/2018 . Pág.: Sem Página Cadastrada.) – **grifos da autora**.

Os casos foram julgados em períodos diferentes e envolveram questões sociais distintas. No entanto, é possível verificar que, entre os possíveis casos que podem se aproximar das circunstâncias de um ou do outro exemplo, há uma miríade de possibilidades que podem culminar em decisões díspares, apesar da potencial semelhança dos critérios colocados em análise.

Fato é que incidentes de segurança e mudanças na destinação de informações tornadas públicas acompanham a inovação digital e a incorporação das tecnologias no cotidiano. Casos como vazamento de dados, estelionato em meio digital, golpes de engenharia social e destinação diversa ou mudança de contexto de dados públicos ou divulgados pelo próprio titular serão mais recorrentes. A importância da definição dos riscos e eventos tolerados se tornam mais evidentes para avaliar a extensão da responsabilidade civil pelo tratamento irregular de dados pessoais.

Isso porque, a título de exemplo, a expectativa de segurança quanto ao tratamento de dados pessoais por uma academia é menor do que a esperada por uma instituição financeira. Ainda que em ambos os casos os respectivos dados se refiram a informações semelhantes (como nome, endereço e CPF), a circunstância e a finalidade do tratamento da última é sensivelmente maior do que a da primeira. Na hipótese de um vazamento de dados ou de um ataque *hacker*, caso a academia tenha adotado todas as medidas de segurança – como a utilização de *softwares* atualizados e medidas de controle de acesso adequadas – a ausência de disponibilidade de tecnologia ou de instrumentos no mercado aptos a evitar a situação danosa pode ser tomada como um fator suficiente para afastar a responsabilidade civil dessa prestadora de serviços.

Por outro lado, um ataque *hacker* a uma instituição financeira pode ser inevitável e ainda assim gerar o dever de indenizar. A expectativa de segurança dos titulares de dados pela perspectiva de tutela ao consumidor é tema que encontra jurisprudência consolidada no âmbito dos Tribunais Superiores, como no caso da súmula 479-STJ, editada em 2012: "*as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias*.".

Há farta jurisprudência que imputa a responsabilidade à instituição financeira por danos cometidos por terceiros, ainda que o fato seja inevitável:

> **Não basta, portanto, que o fato de terceiro seja inevitável para excluir a responsabilidade do fornecedor**, é indispensável que seja também imprevisível. [Há] ***previsibilidade*** **quanto à possibilidade de ocorrência de furtos e roubos de malotes do banco**; em que pese haver imprevisibilidade em relação a qual (ou quais) malote será roubado. [...] Portanto, o roubo de malote contendo cheques de clientes **não configura fato de terceiro, pois é um fato que, embora muitas vezes inevitável, está na linha de previsibilidade** da atividade bancária, o que atrai a responsabilidade civil da instituição financeira.
> (REsp 685662/RJ, Terceira Turma, DJ 05/12/2005, p. 323) – grifos da autora.

As instituições financeiras e administradoras de cartão de crédito diuturnamente reforçam suas práticas de segurança diante de novas e mais elaboradas tentativas de fraudes. Ainda que adotem todas as medidas disponíveis no mercado para garantir a proteção de seus clientes, fraudes ainda ocorrem, como a clonagem de cartões ou empréstimos e saques indevidos. Os Tribunais consideram que o risco do empreendimento determina a responsabilidade objetiva nesses casos e enquadram os danos como fortuito interno a ser arcado pela entidade financeira.

Os temas ainda são tratados de forma setorizada. A alegação de culpa exclusiva da vítima ou de fato exclusivo de terceiro como argumentos de defesa geram resultados distintos nem sempre coordenados. O dever de segurança atribuído às instituições financeiras há tempos consolidado no âmbito de aplicação da legislação de consumo é paradoxalmente relativizado ao se considerar o dever de segurança na tutela de dados pessoais. Presunções de vazamentos de dados pessoais não acompanham o mesmo rigor dos parâmetros estabelecidos para reconhecimento de fato do serviço (muitas vezes amparado na distinção entre fortuito interno e externo). Exemplos de enfrentamento de golpes de engenharia social pelos tribunais são representativos do assunto.

9.3.1 Aproximação CDC e LGPD: violação da expectativa de segurança (LGPD) e vício de qualidade por insegurança (CDC).

A LGPD não prevê de forma expressa as hipóteses que afastam o dever de indenizar os danos para os casos de violação à expectativa de segurança do titular de dados. A leitura integrada da norma, conforme art. 45, da LGPD, remete ao CDC. A violação da expectativa de segurança do titular de dados se correlaciona com a disciplina do *vício de qualidade por*

insegurança (ou simplesmente *defeito*) cuja tutela abrange tanto a saúde e segurança quanto o patrimônio do consumidor. Trata-se da responsabilidade por *acidente de consumo* (nota-se a proximidade com o que a LGPD denomina como "*situação acidental*").

A preocupação básica dessa espécie de responsabilidade é que os produtos e serviços lançados no mercado de consumo sejam seguros, ou seja, não ofendam a saúde, segurança, direitos de personalidade ou o patrimônio do consumidor (BESSA, 2022, p. 122).

No entanto, Leonardo Bessa faz a seguinte ressalva:

> a responsabilidade civil decorrente do disposto no art. 12 da Lei 8.078/1990 refere-se exclusivamente aos casos em que o evento danoso já tem ocorrido (acidente de consumo). Antes disso, ainda que o problema no produto seja de alta potencialidade lesivo à integridade psicofísica do consumidor (interesses existenciais) e ao seu patrimônio, não tem cabimento invocar o referido dispositivo (art. 12): resolução deve ocorrer com base na disciplina constante do art. 18.

Nesse ponto se verifica a maior dificuldade de transportar o conceito de violação de qualidade por insegurança do produto ou serviço (CDC) para violação da expectativa de segurança do titular de dados (LGPD). Conforme afirma Leonardo Bessa (2022), a responsabilidade civil decorrente do acidente de consumo somente se verifica diante de um evento danoso. O alto potencial lesivo à integridade da saúde e patrimônio consumidor não permite invocar a responsabilidade civil por esse enquadramento. A resolução da caso deve ocorrer com base na disciplina da responsabilidade civil pelo vício, ou seja, pelo aspecto de tutela à funcionalidade do produto.

Como exemplo da aproximação do CDC e da LGPD, especialmente para constatar a responsabilidade independentemente de culpa do agente de tratamento, cabe citar a decisão proferida pela quarta câmara de direito privado do Tribunal de Justiça do Estado de Mato Grosso (TJMT) em julgamento no qual se constatou a contratação fraudulenta propiciada por um vazamento de dados. No caso, o TJMT considerou como objetiva a responsabilidade da empresa de investimentos que realizou cobrança relativa a contrato ilegal negociado em nome da autora. O colegiado aliou a incidência dos arts. 42, 44, parágrafo único e 45, da LGPD, com o art. 14, do CDC para definir tanto a solidariedade quanto a responsabilidade independentemente de culpa da empresa ré:

> MÉRITO – FRAUDE NA CONTRATAÇÃO EM RAZÃO DO VAZAMENTO DE DADOS - FALHA NA PRESTAÇÃO DE SERVIÇOS CARACTERIZADA - DANO MORAL CONFIGURADO.
> [...]
> 3. Logo, restando caracterizada a existência de fraude em nome da autora, em razão de vazamento de dados, resta evidenciado o dever de indenizar, a teor do que dispõem os artigos 42, 44, parágrafo único, e 45, todos da Lei Geral de Proteção de Dados Pessoais (LGPD).
> 4. Como se não bastasse a incidência da referida legislação, incide também o artigo 14 do CDC.
> 5. Portanto, considerando o vazamento de dados da autora, que culminou com a contratação indevida, tem-se que, a teor do dispositivo acima transcrito, a responsabilidade do réu/apelado é objetiva, independentemente da existência de culpa.
> 6. Neste contexto, configurado o evento danoso, resta configurado também o dever de indenizar.
> [...]
> (TJ-MT 10002015920208110044 MT, Relator: SERLY MARCONDES ALVES, Data de Julgamento: 06/04/2022, Quarta Câmara de Direito Privado, Data de Publicação: 07/04/2022)

Ocorre que a LGPD não repetiu uma preocupação com a funcionalidade dos dados como fez o CDC. A opção é coerente com os objetivos da norma. A *funcionalidade* do tratamento de dados não atende ao titular de dados (ao menos não de forma direta), mas sim aos interesses do agente de tratamento. Este é o maior interessado no sentido de garantir que o tratamento de dados atenda à finalidade para o qual é exercido. O foco da lei de proteção de dados é outro: reside na adequação normativa do tratamento de dados (conformação normativa) e proteção aos direitos do titular de dados (conformação à expectativa de segurança).

Para as hipóteses em que haja o oferecimento de produtos ou a prestação de serviços que envolvam o tratamento de dados pessoais, ainda que pela perspectiva de proteção ao titular de dados, a funcionalidade da atividade – ou seja, o atendimento à finalidade que lhe é inerente – será tutelada pela disciplina da responsabilidade pelo vício do produto e do serviço (art. 18 a 25 do CDC) ou pela cláusula geral de responsabilidade prevista no art. 6º, VI, do CDC. A exemplo da responsabilidade civil por danos causados por entidades que gerenciam bancos de dados e cadastro de consumidores (arts. 43 e 44, CDC), é equivocado enquadrar tais situações como vício ou fato do serviço. Para esses casos, incide a cláusula geral de responsabilidade prevista no art. 6º, VI, do CDC (BESSA, 2022).

No entanto, para fins de aferir o dano no âmbito de tratamento de dados pessoais que viole a expectativa de segurança do titular, a lógica adotada pelo STJ é outra. O Tribunal Superior abre espaço para considerar que o dano é constatado a partir do fato danoso (dano *in*

re ipsa), como no caso do vazamento de dados sensíveis, e também para afirmar que a divulgação não autorizada de dados pessoais configura mera colocação em risco não indenizável, como no caso de vazamento de dados pessoais "comuns" ou não sensíveis (ARESP 2130619, DJe 10/03/2023). Nota-se que o vazamento de dados é mais uma circunstância do que uma conduta. No entanto, a linha que divide a constatação do dano *in re ipsa* e de mera colocação de dados pessoais em risco ainda é tênue.

Nota-se que a violação da expectativa de segurança, mesmo quando reconhecida por um tribunal para fins de imputar o dever de indenizar, ainda é apenas tangenciada, mas não utilizada como argumento principal para reconhecer a responsabilidade civil de um agente de tratamento. Os casos que envolvem emprego de dados pessoais em uma relação de consumo são importantes para reconhecer a aproximação prática do CDC e da LGPD. No entanto, a responsabilidade civil ainda recai fundamentalmente no reconhecimento do fato do serviço (art. 14, §1º, CDC).

Como exemplo dessa hipótese, o Tribunal de Justiça de Minas Gerais (TJMG) reconheceu, em 2019, a quebra da expectativa de segurança do consumidor que, após o cancelamento regular da linha de telefone, descobriu que o terceiro a quem a linha foi revendida teve acesso aos seus dados pessoais, agenda de contatos e ainda pôde utilizar o WhatsApp como se fosse o antigo titular. No caso, o Tribunal reconheceu que:

> **escapa à normalidade e à previsibilidade inerente** aos contratos de telefonia móvel e, consequentemente, **às legítimas expectativas do consumidor**, a possibilidade de terceiro, em decorrência do cancelamento e revenda do número de telefone celular, ter acesso a dados pessoais e, ainda, gerenciar os aplicativos, tal qual o WhatsApp, como se fosse o antigo titular da linha.
> (TJ-MG - AC: 10000180946691001 MG, Relator: Otávio Portes, Data de Julgamento: 23/01/2019, Câmaras Cíveis / 16ª Câmara Cível, Data de Publicação: 24/01/2019)

O acesso a dados pessoais do autor da ação por um terceiro (novo titular da linha) foi o ponto determinante para reconhecer a quebra da legítima expectativa do consumidor. Interessante notar que a rescisão do contrato de telefonia móvel foi válido e regular, mas, ainda assim, foi reconhecida a manutenção da relação de consumo para fins de apuração do defeito do serviço.

Em outras palavras, a rescisão contratual não desconstituiu a relação de consumo. O TJMG, no caso, poderia ter ido além e suscitar que as obrigações da telefonia não se restringem à legislação de proteção ao consumidor, de modo que o término do tratamento de dados do titular da linha não põe fim às responsabilidades da empresa de telefonia, especialmente diante

das obrigações previstas na LGPD a respeito do término do tratamento de dados pessoais (arts. 15 e 16).

A "*legítima expectativa do titular de dados pessoais*" é conceito (ainda) pouco explorado pela doutrina e jurisprudência, mas encontra farta base doutrinária e de aplicação jurisprudencial no âmbito da tutela do consumidor. De fato, no caso acima, foi o reconhecimento do defeito do serviço (por violação à intimidade do consumidor) o fundamento utilizado para impor o dever de indenizar pelo dano moral sofrido pelo titular inicial da linha. O reconhecimento do não atendimento à "*expectativa de segurança que o titular possa esperar*" foi apenas tangenciado no referido acórdão.

Se o reconhecimento do regime dual de responsabilidade civil na LGPD já é uma inovação (conforme defendido no presente trabalho), pode-se inferir que a exploração do conceito de "*quebra da expectativa de segurança do titular*" como fator relevante para determinar a responsabilidade civil de agentes de tratamento ainda é, no mínimo, incipiente.

9.3.2 Golpes de engenharia social: da imprevisibilidade do dano e do dever de indenizar.

Vazamentos de dados (*data leak* ou *data breach*) ocorrem quando dados são indevidamente acessados, coletados, divulgados ou repassados a terceiros. A origem do vazamento pode ser o acesso de dados por pessoas que usam de códigos maliciosos para explorar vulnerabilidades de segurança em sistemas; identificação de senhas fracas; ação ou negligência de funcionários ou ex-funcionários que permitem acesso ou repassam dados a terceiros.

É fato comum do cotidiano a utilização de dados pessoais para aplicar "golpes de engenharia social" – técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. O conceito é apresentado pela FEBRABAN (2020), a qual alerta que o aprimoramento de métodos usados por golpistas acompanha a inovação tecnológica:

> A cada inovação tecnológica, novas brechas de segurança também são criadas. E os hackers e golpistas se aproveitam dessas falhas usando a engenharia social para cometer crimes, causando prejuízo às vítimas e às empresas. Aquele que usa a influência e persuasão, com técnicas psicológicas de convencimento ou por meio da tecnologia para enganar e manipular pessoas a revelarem ou concederem acesso a dados pessoais e informações sigilosas, que serão usados na aplicação de golpes visando benefício financeiro ou fraudes contra terceiros, é chamado de engenheiro social.

A LGPD atribui diversos deveres de conduta que, em última análise, impactam na mensuração da responsabilidade dos agentes em eventual vazamento de dados. Ainda que reconhecida a dificuldade atribuída ao titular em identificar a origem ou autoria do vazamento de seus dados, o Superior Tribunal de Justiça compreende que os arts. 43 e 44 indicam que a LGPD se destina a indicar a responsabilidade dos agentes que *de fato* detêm os dados pessoais que foram vazados. Quanto às instituições bancárias, o Tribunal Superior já exigiu a demonstração da origem de um vazamento para imputar a responsabilidade civil dessas instituições:

> 22. Notório, portanto, que a fim de imputar a responsabilidade das instituições financeiras no que tange ao vazamento de dados pessoais, *deve-se garantir que a origem do vazamento foi o sistema bancário*, bem como observar se as devidas medidas protetivas quanto aos dados pessoais sob domínio da instituição financeira foram adotadas.
> (REsp 1.995.458/SP. Rel.: Ministra Nancy Andrighi. Julgamento: 09/08/2022. DJe: 18/08/2022.)

Ao mesmo tempo, o STJ considera que é dever da instituição financeira verificar comportamentos atípicos do consumidor no uso de um cartão de crédito, bem como de desenvolver meios a dificultar fraudes, independentemente de qualquer ato dos consumidores.

Nos casos de golpes de engenharia social, o reconhecimento da responsabilidade civil das instituições financeiras recai primordialmente sobre a consideração de seu dever em verificar comportamentos atípicos das atividades financeiras do consumidor. Não se reconhece, por outro lado, que os dados de posse de estelionatários recaem de um vazamento de dados por essa instituição financeiras.

Em geral, estelionatários em posse de dados do cartão de crédito realizam diversas operações em sequência, em um curto período de tempo e em altos valores – o que tende, em regra, a destoar do perfil de gastos do consumidor. No caso que serviu como pano de fundo no julgamento do REsp 1.058.221/PR, o golpe de engenharia social aplicado a um consumidor gerou prejuízo que superou R$ 25.000,00 (vinte e cinco mil reais) gastos pelos estelionatários no período de apenas 11 minutos, marcado entre o acesso ao cartão e senha e o efetivo bloqueio do cartão de crédito pela instituição financeira. A média mensal de compras do correntista era de apenas R$ 500,00. A decisão considerou quitada a fatura relativa ao mês do prejuízo e nula as cláusulas contratuais que imputam exclusivamente ao consumidor a responsabilidade por transações efetuadas com o cartão até o momento da comunicação de roubo, extravio, furto ou perda.

O dever de segurança das instituições financeiras, conforme aventado, envolve o alerta aos correntistas sobre movimentações estranhas e o bloqueio preventivo do cartão por movimentações atípicas até que se confirme a legitimidade das transações. Nesse sentido, a jurisprudência do STJ já reconhece que, independentemente da ocorrência de furto ou roubo ou de qualquer ato do consumidor, incumbe às administradoras de cartão e do restante da cadeia de fornecedores do serviço (proprietárias das bandeiras, adquirentes e estabelecimentos comerciais), a criação de medidas para verificar a idoneidade das compras realizadas com cartões magnéticos, utilizando-se de meios que dificultem ou impossibilitem fraudes e transações realizadas por estranhos em nome de seus clientes (REsp 1.058.221/PR, Terceira Turma, DJe de 14/10/2011; REsp n. 970.322/RJ, Quarta Turma, DJe de 19/3/2010).

Nesse sentido, há farta jurisprudência que imputa responsabilidade à instituição financeira por crimes cometidos por terceiros. Sobre os deveres de segurança para essas instituições, o STJ tem histórico de atribuir a responsabilidade a esses agentes por: (i) assaltos no interior das agências bancárias (REsp 787.124/RS, Primeira Turma, DJ 22/05/2006); (ii) inscrição indevida em cadastro de proteção ao crédito (REsp 1149998/RS, Terceira Turma, DJe 15/08/2012); (iii) desvio de recursos da conta-corrente; (iv) extravio de talão de cheques (REsp 685.662/RJ, Terceira Turma, DJ 05/12/2005); (v) abertura não solicitada de conta-corrente; (vi) clonagem ou falsificação de cartões magnéticos; (vii) devolução de cheques por motivos indevidos além de outros casos correlatos.

A distinção entre o fortuito interno ou externo é utilizada como argumento para verificar a configuração da responsabilidade civil e determinar se um dano decorre de um risco, ainda que inevitável, inerente à própria atividade desenvolvida:

> **Não basta, portanto, que o fato de terceiro seja inevitável para excluir a responsabilidade do fornecedor**, é indispensável que seja também imprevisível. Nesse sentido, é notório o fato de que furtos e roubos de talões de cheques passaram a ser prática corriqueira nos dias atuais. Assim, a instituição financeira, ao desempenhar suas atividades, tem ciência dos riscos da guarda e do transporte dos talões de cheques de clientes, **havendo *previsibilidade* quanto à possibilidade de ocorrência de furtos e roubos de malotes do banco**; em que pese haver imprevisibilidade em relação a qual (ou quais) malote será roubado. Aliás, o roubo de talões de cheques é, na verdade, um caso fortuito interno, que não rompe o nexo causal, ou seja, não elide o dever de indenizar, pois é um fato que se liga à organização da empresa; relaciona-se com os riscos da própria atividade desenvolvida. (cfr. Paulo de Tarso Vieira Sanseverino, Responsabilidade civil no Código do consumidor e a defesa do fornecedor, São Paulo: Saraiva, 2002, p. 293). Portanto, o roubo de malote contendo cheques de clientes **não configura fato de terceiro, pois é um fato que, embora muitas vezes inevitável, está na linha de previsibilidade** da atividade bancária, o que atrai a responsabilidade civil da

> instituição financeira. (REsp 685662/RJ, TERCEIRA TURMA, DJ 05/12/2005, p. 323) – grifos da autora.

Sob o fundamento de considerar o fato de terceiro como previsível, ainda que inevitável, as compras realizadas no lapso entre o furto e a comunicação do banco não afastam a responsabilidade da instituição financeira. (REsp 1.737.411/SP, Terceira Turma, DJe de 12/4/2019). Evidencia-se falha na adoção de medidas que, em tese, estão ao alcance da rede de fornecedores envolvidos na prestação de serviço e fornecimento de produtos.

Surge o questionamento: seria possível transpor a consideração e caracterização do fortuito interno para o caso da LGPD? Especialmente quanto aos casos de vazamento de dados?

A análise de casos enfrentados pelo STJ demonstram que os golpes aplicados podem se originar de atos de criminosos que, em posse de dados do titular, realizam atividade prejudicial ato titular (ao que se refere como caso de vazamento de dados) ou de uma indução, também por criminosos, para que o titular espontaneamente repassem informações ao transgressor que, de posse de dados pessoais relevantes (como senha de cartão magnético bancário) realiza operações criminosas contra o titular (os mencionados golpes de engenharia social).

No entanto, a responsabilidade das instituições financeiras não é reconhecida pela jurisprudência como desdobramento do fato de se constatar um vazamento de dados (ou outra perspectiva de tutela aos dados pessoais) mas sim pelo reconhecimento de que esses golpes compõem fortuito interno na hipótese de falha na identificação de movimentações atípicas e correspondente adoção de medidas para evitá-las.

A relevância do assunto detalhado se refere à avaliação da possibilidade de se utilizarem os mesmos argumentos para a quebra de expectativa de segurança do titular de dados. Em outras palavras, abre-se espaço para analisar uma divisão de fortuito interno ou externo para avaliar quais danos devem ser suportados pelo agente de tratamento. Note-se que a imprevisibilidade do dano e o fato de terceiro ser inevitável não é argumento a afasta a responsabilidade nos casos acima mencionados.

Pela primeira espécie, a violação à legislação na modalidade tratamento ilícito (desatendimento à LGPD) ou tratamento indevido (omissão aos regulamentos da ANPD) demonstra que a previsibilidade de uma conduta é determinante para sua configuração. Por outro lado, a impossibilidade de evitar um dano não seria argumento suficiente para afastar a segunda espécie de responsabilidade civil prevista na LGDP: a por violação à expectativa de segurança do titular de dados.

Da mesma forma que aplicada no âmbito da legislação de consumo, a determinação de que o fornecedor suporte danos inevitáveis ou por fato exclusivo de terceiro deve-se à rentabilidade da atividade e dos riscos determinados como inerentes à prestação do serviço, como no caso emblemático que envolve a prestação de serviços por instituições financeiras. Esse raciocínio, no entanto, não é refletido nas recentes decisões do Tribunal Superior quanto à ocorrência de danos pelo tratamento irregular de dados pessoais. A jurisprudência sinaliza que os danos não decorrem da mera quebra de segurança (ou seja, da constatação de vazamento de dados) ainda que por instituições financeiras.

Além da demonstração do dano se mostrar como elemento relevante e desafiador, o nexo de causalidade enfrenta dificuldades ante a possibilidade de se acatar argumentos que comprovam seu rompimento, em especial, a culpa exclusiva de terceiro e da vítima.

9.3.3 Golpe do motoboy e nexo de causalidade: da culpa exclusiva da vítima e de terceiro.

Sobre o nexo de causalidade na hipótese de golpes de engenharia social, entende-se que a inércia das instituições financeiras frente a transações de valores altos em curto espaço de tempo concorre para permitir a perpetração de golpes a seus correntistas. Há nexo causal ao se verificar que a instituição financeira poderia ter evitado ou mitigado o dano causado por fraudes caso adotasse medidas de segurança mais eficazes para identificar transações atípicas. Em outras palavras, não prospera a alegação de culpa exclusiva da vítima nesses casos, ainda que esta tenha fornecido informações relevantes de forma espontânea ao criminoso.

Isso porque integra a atividade bancária a criação de mecanismos que obstem movimentações atípicas que aparentem ilegalidade quando comparadas com o histórico do consumidor no que tange a valores, frequência e modo de compra. A falta de implementação de tais mecanismos revela vulnerabilidade do sistema bancário e configura violação do dever de segurança que às instituições financeiras cabe assegurar o que, por decorrência, configura falha na prestação do serviço. Constata-se, nesses casos, que é a falha na prestação do serviço que permite o golpe e consequentes prejuízos financeiros à vítima.

Sobre o tema, o STJ julgou se existe falha na prestação do serviço bancário quando o correntista é vítima do golpe do motoboy. Nessa prática criminosa, a vítima, geralmente uma pessoa idosa, recebe uma ligação ou mensagem de suposto preposto de instituição bancária. O estelionatário informa que o cartão da vítima foi clonado e solicita que ela digite a senha pessoal no teclado do telefone para que possa realizar suposto cancelamento do cartão. Em seguida, o estelionatário informa que um motoboy irá buscar o cartão da vítima e que ela pode até quebrá-

lo antes da entrega, devendo, no entanto, manter incólume o chip. Após a cessão, são efetuadas diversas compras com o cartão da vítima.

O tema envolveu a alegação de vazamento de dados pessoais sobre a vítima (que de posse dos estelionatários são utilizados para formar o seu convencimento) e a falha na prestação do serviço pela falta de adoção de mecanismos para obstar transações que fogem do padrão de consumo do cliente. Na oportunidade do julgamento do REsp 1995458/SP, em 2022, o Tribunal ressalta que é de fato grande a dificuldade de saber a origem do vazamento, importando a adoção de medidas para evitar este acontecimento (arts. 43 e 44, da LGPD). No entanto, conclui que, a fim de imputar a responsabilidade das instituições financeiras no que tange ao vazamento de dados pessoais, é imprescindível à vítima garantir que a origem do vazamento foi, de fato, o sistema bancário:

> 16. Não obstante essa triste realidade, para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais do sistema bancário no intuito de imputar responsabilidade à instituição financeira pelo vazamento de dados, seria preciso superar que (i) não se sabe com exatidão quais são as informações que os estelionatários detinham para efetuar o golpe e que (ii) a origem da obtenção de dados pessoais não é necessariamente a instituição financeira, pois os dados pessoais são passíveis de serem adquiridos em diversos meios.
> [...]
> 18. Os dados suscetíveis a vazamento são credenciais de acesso, como nomes de usuário e senhas; informações financeiras, como números de contas bancárias e de cartões de crédito; documentos, como CPF, RG e carteira de habilitação; informações de contato, como endereços e números de telefone; registros de saúde, como resultados de exames e prontuários médicos; além outros dados, como data de nascimento e nomes de familiares.
> [...]
> 22. Notório, portanto, que **a fim de imputar a responsabilidade das instituições financeiras no que tange ao vazamento de dados pessoais, deve-se garantir que a origem do vazamento foi o sistema bancário**, bem como observar se as devidas medidas protetivas quanto aos dados pessoais sob domínio da instituição financeira foram adotadas.
> (STJ. REsp 1995458/SP. Rel.: Ministra Nancy Andrighi. Julgamento: 09/08/2022. DJe: 18/08/2022.)

Para o STJ, a crescente difusão de golpes de engenharia social na sociedade impõe uma mudança de comportamento social que atribui à vítima o dever de tomar medidas de cuidado. Não há complacência quando se reconhece a negligência da vítima que se descuida de cartão e senha pessoal. Nesse sentido, é consolidado o posicionamento jurisprudencial que afasta a responsabilidade da instituição financeira o fato de o evento danoso decorrer de transações realizadas com a apresentação física do cartão original e mediante uso de senha pessoal do correntista:

> 3. De acordo com a jurisprudência do Superior Tribunal de Justiça, a responsabilidade da instituição financeira deve ser afastada quando o evento danoso decorre de transações que, embora contestadas, são realizadas com a apresentação física do cartão original e mediante uso de senha pessoal do correntista.
> [...]
> 5. O cartão magnético e a respectiva senha são de uso exclusivo do correntista, que deve tomar as devidas cautelas para impedir que terceiros tenham acesso a eles.
> 6. Demonstrado na perícia que as transações contestadas foram feitas com o cartão original e mediante uso de senha pessoal do correntista, passa a ser do consumidor a incumbência de comprovar que a instituição financeira agiu com negligência, imprudência ou imperícia ao efetivar a entrega de numerário a terceiros. Precedentes.
> (STJ - REsp: 1633785 SP 2016/0278977-3, Relator: Ministro RICARDO VILLAS BÔAS CUEVA, Data de Julgamento: 24/10/2017, T3 - TERCEIRA TURMA, Data de Publicação: DJe 30/10/2017)

Sobre o golpe do motoboy, o cartão e informações pessoais são espontaneamente repassados ao estelionatário. O convencimento da vítima é motivado pela exatidão dos dados pessoais informados pelos criminosos. Ainda que dados como credenciais de acesso e informações financeiras sejam em tese de conhecimento apenas do titular e da instituição financeira, o STJ não presume a ocorrência de vazamento desses dados para imputar responsabilidade a esta:

> 16. Não obstante essa triste realidade, para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais do sistema bancário no intuito de imputar responsabilidade à instituição financeira pelo vazamento de dados, seria preciso superar que
>
> (i) não se sabe com exatidão quais são as informações que os estelionatários detinham para efetuar o golpe e que
>
> (ii) a origem da obtenção de dados pessoais não é necessariamente a instituição financeira, pois os dados pessoais são passíveis de serem adquiridos em diversos meios.
>
> 17. [...] A origem do vazamento pode ser o furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas; o acesso a contas de usuários; as senhas fracas ou vazadas; a ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros; o furto de equipamentos que contenham dados sigilosos; os erros ou a negligência de funcionários, como descartar mídias (discos e pen drives) sem os devidos cuidados, e outros.
> (STJ - REsp: 1995458 SP 2022/0097188-3, Data de Julgamento: 09/08/2022, T3 - Terceira Turma, Data de Publicação: DJe 18/08/2022)

Nesses termos, o posicionamento adotado pelo tribunal foi no sentido de que o vazamento de dados pela instituição financeira não pode ser deduzido pelo fato de terceiros

terem acesso a dados relevantes. A vítima deve comprovar e garantir que a origem do vazamento foi de fato do sistema bancário. Pode-se dizer que essa prova é no mínimo excessivamente difícil (se não impossível) para o titular de dados.

No caso enfrentado, a instituição bancária foi condenada a ressarcir os prejuízos decorrentes do golpe do motoboy aplicado à vítima. O fundamento foi baseado na constatação falha do dever de segurança, não dos dados pessoais da vítima, mas da prestação do serviço bancário. Em outras palavras, foi chancelada a perspectiva de tutela ao consumidor (e não ao titular de dados pessoais).

Determinou o STJ que a ocorrência do evento danoso no golpe do motoboy exige a ocorrência das seguintes causas: (1) o fornecimento, pelo consumidor, do cartão magnético e senha pessoal ao estelionatário; e (2) violação do dever de segurança pelo banco, por não criar mecanismos que obstem transações bancárias com indícios de ilegalidades por destoarem do perfil de consumo do correntista. Não foi aventado, como elemento relevante desse raciocínio, a ponderação sobre como os estelionatários tiveram conhecimento de dados da vítima.

Na decisão (REsp 1995458/SP), a despeito da atribuição à vítima do ônus de comprovação do vazamento de dados pela instituição financeira, foi reconhecida a falha na prestação do serviço diante do não atendimento do dever de mitigar a vulnerabilidade do sistema bancário mediante o bloqueio de operações atípicas. Ademais, foi levado em conta a questão da vítima ser pessoa idosa e, portanto, considerada a peculiar situação de consumidor hipervulnerável:

> 8. A vulnerabilidade do sistema bancário, que admite operações totalmente atípicas em relação ao padrão de consumo dos consumidores, viola o dever de segurança que cabe às instituições financeiras e, por conseguinte, incorre em falha da prestação de serviço.
> 10. Na hipótese, contudo, verifica-se que o consumidor é pessoa idosa, razão pela qual a imputação de responsabilidade há de ser feita sob as luzes do Estatuto do Idoso e da Convenção Interamericana sobre a Proteção dos Direitos Humanos dos Idosos, sempre considerando a sua peculiar situação de consumidor hipervulnerável.
> (STJ - REsp: 1995458 SP 2022/0097188-3, Data de Julgamento: 09/08/2022, T3 - TERCEIRA TURMA, Data de Publicação: DJe 18/08/2022)

Pelo julgado, a qualidade do consumidor se mostra mais relevante do que o questionamento sobre como dados específicos e detalhados do titular de dados chegaram ao conhecimento dos estelionatários. Nota-se uma certa resistência dos tribunais em atribuir a violação de segurança dos dados pessoais, ou seja, estabelecer o nexo causal na análise de um vazamento de dados pessoais. Pode-se dizer que, para o tribunal, a consequência (acesso não

autorizado a dados pessoais) por poder ter diversas causas, não pode ser imputada à instituição bancária.

A vulnerabilidade não reside no fato de terceiros (estelionatários) terem conhecimento de dados específicos do titular. A vulnerabilidade do sistema bancário se revela ao admitir operações totalmente atípicas em relação ao padrão de consumo dos consumidores, o que viola o dever de segurança que cabe às instituições financeiras e, por consequência, configura falha na prestação de serviço.

Nota-se que há posicionamentos distintos de acordo com as perspectivas de análise do dever de segurança pelas instituições financeiras. De um lado, pela lógica pautada na lei de defesa do consumidor, o STJ considera que houve falha na prestação de serviço de modo que o nexo causal é evidenciado pela ausência de adoção de mecanismo que detectasse transações atípicas do consumidor. Pela lógica da LGPD, na análise de alegados vazamentos (*data breach*), o desatendimento ao dever de segurança não é reconhecido da mesma forma. Não há uma presunção de que houve uma falha de segurança. Paradoxalmente, o titular de dados – que em muitas vezes se confunde com o consumidor – tem o dever de comprovar a autoria do vazamento de dados.

Por outo lado, o TJDFT, por sua Turma Recursal, reconheceu a ocorrência de um vazamento de dados pessoais – ou, ao menos, a "*fragilização dos dados do correntista*" – em situação de fraude bancária. No caso, estelionatários se passaram por preposto da instituição correntista e, munidos de informações específicas sobre dados bancários da vítima, a induziram a instalar aplicativo de controlo remoto de celular o que possibilitou que realizassem transferências de grande vulto via Pix.

A despeito do reconhecimento do vazamento de dados e sujeição da instituição financeira ao regime de responsabilidade da LGPD, a responsabilidade civil foi determinada com base na falha do dever de atender aos critérios de segurança para monitoramento de quantias de grande vulto incompatíveis com o perfil de usuário da correntista. Foi reconhecido o nexo causal entre o fato danoso e a prestação de serviço defeituosa. Ademais, foi afastada a excludente de culpa exclusiva da vítima, pois o Tribunal compreende que as instituições financeiras deveriam investir em aparatos tecnológicos para detecção de fraudes:

> 5. A princípio, cabe destacar que a responsabilidade da instituição financeira é objetiva, somente podendo ser afastada quando ficar comprovado a existência de fatos que rompem o nexo causal, tal qual a culpa exclusiva do consumidor ou de terceiros. A n. sentenciante equiparou o golpe sofrido pela parte autora ao Golpe do Motoboy, no qual terceiros, se passando por prepostos da instituição financeira, contatam o cliente informando a existência

> de compras indevidas, só que neste caso induziram a parte autora a instalar um aplicativo de acesso remoto, o que permitiu que os fraudadores assumissem o controle do celular para realização da transferência via PIX, no valor de R$ R$ 19.000,00 (dezenove mil reais).
> 6. É incontroverso que os estelionatários tinham informações sobre os dados bancários da parte autora. Situação quase que rotineira para qualquer correntista de Banco é o recebimento de ligações, via celular, de prepostos dessas instituições financeiras, para ofertar produtos. Assim, a parte autora idosa não tinha como saber que se tratava de golpe. Diversas ações sobre golpes contra idosos aposentados e pensionistas do INSS são comuns nas Turmas Recusais, tal como o já mencionado o Golpe do Motoboy. Assim, há verossimilhança nas alegações da parte autora.
> 7. Diante da fraude, **restou provado que a recorrente deixou de atender aos critérios de segurança para monitoramento da quantia**, no valor de R$ 19.000,00, cuja transferência foi realizada via PIX, sendo incompatíveis com o seu perfil de usuário. **O recorrente possui aparato tecnológico para detecção de fraudes, restando caracterizada a falha na prestação do serviço,** a qual trouxe prejuízo à parte autora de ordem financeira. Havendo fragilização dos dados do correntista, tal como se extrai do caso concreto dos autos, porque os estelionatários, de antemão, já tinham os dados do autor, é de se aplicar os comandos da Lei Geral de Proteção de Dados, Lei 13.709/2018, arts. 42 e seguintes, confirmando a responsabilidade da instituição financeira em ressarcir os prejuízos comprovados pelo autor, de modo que não há falar em culpa exclusiva da parte autora.
> (Acórdão 1431274, 07049441820228070016, Relator: Juiz ARNALDO CORRÊA SILVA, Segunda Turma Recursal dos Juizados Especiais do Distrito Federal, data de julgamento: 20/6/2022, publicado no DJe: 28/6/2022).

Suscitar os comandos da LGPD serviu como reforço argumentativo para a responsabilidade objetiva da instituição financeira e para afastar a excludente da culpa exclusiva da vítima no caso enfrentado – o que já sinaliza uma positiva aplicação da LGPD em efetivação dos direitos do titular dos dados pessoais. No entanto, no mesmo padrão das decisões do STJ acima colacionadas, o dever de restituir prejuízos da vítima, no caso, decorreu do reconhecimento de violação do dever de segurança pela prestação de serviço bancário defeituoso – e não, propriamente, da violação de segurança dos dados pessoais da correntista.

Nesses casos, não sobressalta a violação ao direito de proteção aos dados pessoais. Há o reconhecimento de uma certa "normalização" de que as fraudes perpetradas por terceiros dizem respeito a dissabores cotidianos. Nesse sentido é fundamentado caso semelhante no qual é reconhecido o dever de reparar danos materiais à vítima, mas afastado o reconhecimento de um dever de compensar por danos morais:

> 9. É inquestionável que situação narrada nos autos se trata de golpe engenhoso e complexo comumente conhecido por "golpe do motoboy", [...]
> 11. Embora a instituição financeira alegue jamais solicitar aos seus clientes a entrega de cartão e senha pessoal, que tenha incorrido em falha na prestação

> de serviços ou agido em desconformidade com a lei e regulamentações bancárias, não fornece a segurança adequada em suas transações, pois realiza o mesmo tipo de serviço praticado pelos golpistas o que incute no consumidor a expectativa de estar tratando diretamente com a instituição financeira.
> 12. Ressalte-se, no caso, o banco, ora recorrente, também não se desincumbiu do ônus de demonstrar que todas as transações foram realizadas mediante impostação de cartão e digitação de senha, do mesmo modo, não comprovou que as transações volumosas e em curto período de tempo eram compatíveis com o perfil da cliente, ora recorrida. Pois é evidente que um correntista seria incapaz de realizar inúmeras transações em um curto período de tempo em diferentes estabelecimentos.
> 13. Deste modo, a instituição financeira, recorrente, deve responder de forma objetiva pelos danos materiais causados à recorrida. (art. 14 do CDC).
> 14. Quanto aos danos morais, além de **não se vislumbrar efeitos negativos à personalidade da autora**, eis que não houve sua inclusão em cadastros de inadimplentes, ou algo semelhante, o **fato originário dos dissabores vivenciados foi a conduta fraudulenta de terceiros**, da qual o banco recorrido também foi vítima. Assim, não há fundamento fático a justificar a reparação por danos morais
> (Acórdão 1391985, 07330320320218070016, Relator: Edilson Enedino das Chagas, Primeira Turma Recursal, data de julgamento: 3/12/2021, publicado no DJE: 17/12/2021. Pág.: Sem Página Cadastrada.) – *grifos da autora*.

Nota-se que o fato de a conduta fraudulenta ser perpetrada por terceiros não é argumento que afasta o nexo causal entre o dano e dever de segurança nos serviços prestados pela instituição financeira. No entanto, é elemento relevante para afastar o reconhecimento de afetação dos direitos da personalidade ou do dano de natureza moral.

9.3.4 Golpe do boleto falso: da presunção de vazamento de dados.

A sofisticação de estelionatos em meio digital[74] é uma prática crescente na sociedade. O estelionato digital é uma fraude na qual o criminoso engana alguém, por meio de redes sociais, contatos telefônicos, aplicativos de mensagens instantâneas, correio eletrônico falso ou qualquer outro meio fraudulento, a fornecer dados confidenciais, tais como senhas, logins e números de cartão de crédito ou débito.

[74] O crime previsto no art. 171 do Código Penal consiste em aplicar golpes nos quais o criminoso induz em engano uma vítima para obter algum tipo de vantagem, em geral, em dinheiro. Para tentar coibir a prática com o uso de meios tecnológicos, a Lei nº 14.155, de 2021 alterou o Código Penal para criar a figura da Fraude Eletrônica, § 2º-A, § 2º-B e § 3º do artigo 171, também conhecida por Estelionato Digital. Trata-se de uma forma qualificada do crime de estelionato, e por isso recebe pena mais severa. Enquanto no estelionato comum a pena é de 1 a 5 anos de prisão, na fraude eletrônica, ela vai de 4 a 8 anos e pode ser aumentada em até 2/3, caso o crime seja cometido com uso de servidor (computador para armazenar dados) que esteja fora do Brasil. A pena também pode ser acrescida em até 1/3, na hipótese de o crime ser cometido contra entidade pública, instituto de economia popular ou assistência social.

A análise pelos tribunais a respeito do dever de segurança é comumente realizada de forma setorizada. No caso de instituições financeiras, ponto relevante para atribuir responsabilidade por danos infligidos por meio de práticas de estelionato digital se volta a atribuir ao banco o dever de verificar a ocorrência de atividades financeiras atípicas e evitar novas transações não habituais. É o caso do "golpe do motoboy", cuja prática motivou a consolidação de entendimento pela Turma de Uniformização de Jurisprudência dos Juizados Especiais do TJDFT na súmula 28, cujo conteúdo aduz que "*as instituições financeiras respondem pelos danos decorrentes de fato do serviço nas fraudes bancárias conhecidas como "golpe do motoboy*".

Não é o mesmo entendimento aplicável a outros casos, como o golpe do boleto falso. A confrontação de dois casos julgados pelo TJDFT sobre esse mesmo tipo de estelionato teve desfechos distintos. Em uma situação, o tribunal presumiu a ocorrência de vazamento de dados e atribuiu responsabilidade para arcar com danos materiais sofridos por uma vítima a uma empresa de telefonia. No outro caso, o mesmo tribunal considerou que os dados utilizados pelos estelionatários poderiam ser obtidos de diversas formas e que, nas circunstâncias descritas, caberia à vítima o dever de evitar o próprio dano.

Quanto à primeira situação, uma empresa de telefonia foi condenada a abater do débito de uma consumidora o valor que esta arcou com o pagamento de um boleto falso. O documento de cobrança foi enviado por e-mail e emitido por estelionatários que se utilizaram do logotipo da empresa de telefonia e demonstraram conhecimento sobre os dados pessoais e contratuais da vítima. Confrontada, a empresa alegou desconhecer o modo pelo qual terceiros tiveram acesso aos dados cadastrais e contratuais da consumidora.

Nesse caso, o TJDFT reconheceu que os dados foram vazados, pois, além de nome, CPF endereço e data de nascimento, a indicação de número de contrato e dados sobre a dívida demonstraram que estas informações foram indevidamente difundidas, possibilitando a dissimulação da dívida por terceiros e o respectivo pagamento em prejuízo da consumidora. O caso foi enquadrado como falha na prestação de serviço, conforme o art. 14, do CDC, bem como foi reconhecida que o evento está ligado à organização do negócio explorado (fortuito interno), de modo a compreender que se aplica a teoria do risco da atividade. (Acórdão 1618586, 07017037520228070003, Relator: Rita De Cássia de Cerqueira Lima Rocha, Primeira Turma Recursal, data de julgamento: 16/9/2022, publicado no DJE: 10/10/2022)

Não foi o mesmo entendimento aplicado no caso de pagamento de boleto bancário fraudulento envolvendo o financiamento de veículo entre o consumidor e instituição financeira. A utilização de dados determinantes (como informações pessoais da autora, características do

veículo, número de contrato e valor do débito) não foram suficientes para comprovar defeito do serviço de financiamento prestado pela instituição financeira. No caso, a consumidora, em contato com terceiro estelionatário – que se passou por preposto da instituição financeira –, quitou boleto bancário supostamente relativo ao financiamento de seu veículo. Ocorre que o boleto foi adulterado para modificar os dados do beneficiário de modo a conferir legitimidade ao documento.

No caso, tribunal considerou que o fato de as informações específicas poderem ser coletadas de fontes diversas, inclusive pelo acesso ao processo judicial de busca e apreensão cujo acesso não sofreu de restrições da LGPD, não foi reconhecida falha no dever de proteção de dados (art. 42, da LGPD). Esse raciocínio culminou no reconhecimento da culpa exclusiva da vítima.

A fraude foi constatada, mas não se vislumbrou falha na prestação do serviço bancário (nos moldes do art. 14, do CDC). O Tribunal reconheceu a negligência da autora por não ter se utilizado os meios de comunicações oficiais fornecidos pelo banco ou por não ter conferido o real beneficiário do pagamento – o que, em tese, evitaria a fraude. A questão de fundo não foi tratada como segurança do serviço prestado, mas como atividade comum que se desenvolve na ~~rede mundial~~. Sem indícios da existência de defeito, não foi reconhecida a responsabilidade do fornecedor. (Acórdão 1639084, 07064918120228070020, Relator: Aiston Henrique de Sousa, Primeira Turma Recursal, data de julgamento: 10/11/2022, publicado no DJE: 29/11/2022).

Não há uma contradição evidente entre ambos os casos. Os meios de comunicação utilizados pelos infratores foram diversos e, no segundo caso, a divulgação de informações específicas em processo judicial cujo acesso não era restrito foi circunstância peculiar e relevante para o desfecho do caso.

O que se evidencia é que a fundamentação da responsabilidade civil com base nas disposições da LGPD ainda é tímida. Nota-se uma tendência dos precedentes em atribuir à vítima o dever de comprovar a origem de um vazamento de dados e a análise da responsabilidade ainda é adstrita à fundamentação de defeito do serviço (com base na legislação de consumo). Ademais, a vulneração dos dados pessoais de uma pessoa, como um direito da personalidade, é assunto tangenciado, mas não aprofundado. Temas relativos a danos morais ainda devem sofrer muitas modificações antes de se tornarem pacificado.

9.3.5 Violação da segurança por hackers: do fortuito interno e da assunção de riscos cibernéticos.

Sobre a atribuição da responsabilidade civil a provedores de internet por riscos cibernéticos, a análise da responsabilidade civil depende de aspectos circunstanciais. Ao provedor de conteúdo, por exemplo, não incumbe a responsabilidade de fiscalizar o teor das informações postadas por usuário, ainda que ofensivas a terceiro (LEMOS, 2015). No entender do STJ, o site que não examina ou filtra os dados e imagens nele inseridos não pode ser considerado defeituoso, pois não se trata de atividade intrínseca ao serviço prestado (REsp 1.316.921/RJ). Nesses casos, portanto, descabe invocar a aplicação do art. 14, do CDC, a respeito de defeito do serviço.

Aliás, de acordo com o Marco Civil da Internet, a responsabilidade civil do provedor de *internet* pelos danos decorrentes do conteúdo gerado por terceiro é subsidiária e ocorrerá em caso de descumprimento de ordem judicial (art. 19, MCI) que determinar a indisponibilização do conteúdo ilícito ou da permanência de imagens/vídeos íntimos após a ciência do ocorrido por pedido de exclusão do conteúdo pelo ofendido (art. 21, MCI). A omissão ilícita, portanto, é pressuposto necessário para ensejar a responsabilidade civil para esses casos (TJDFT. Acórdão 1369225, Relatora: Diva Lucy de Faria Pereira, 1ª Turma Cível, DJe: 16/9/2021).

A tutela ao titular de dados é mais limitada por esse diploma normativo, tendo em vista que o provedor de aplicações de *internet* somente será responsabilizado por publicações de terceiros na hipótese de omissão ilícita. Difere-se do foco da LGPD, pois o MCI privilegia, em princípio a garantia à liberdade de expressão, de forma a possibilitar a manifestação indiscriminada, sem censura ou monitoramento prévio. A apreciação de alegada violação à privacidade exige seu reconhecimento pelo Poder Judiciário pois somente a este caberia a determinação da remoção ou suspensão da veiculação de determinado conteúdo.

Em outras palavras, pela Lei 12.965/2014 (MCI), cabe ao Poder Judiciário, e não ao provedor de internet, a missão de analisar de determinada manifestação deve ou não ser excluída do ambiente cibernético – sob pena, inclusive, de caracterizar arbitrariedade por parte do provedor. Para Flávio Tartuce (2021, pág. 1447), o panorama jurídico geral a respeito do sistema delineado pelo Marco Civil da Internet, e pela interpretação que se faz a respeito dessa lei, é de amparo aos provedores – e não, propriamente, aos titulares de dados pessoais:

> A responsabilidade civil dos provedores de internet por atos de terceiros está restrita às hipóteses em que há desobediência à ordem judicial, o que conduz a uma responsabilidade subjetiva agravada, que raramente gera o dever de indenizar dessas empresas que atuam no setor. Assim, [...], a responsabilidade civil acaba recaindo sobre as próprias pessoas que realizam postagens ofensivas, respondendo elas por ato próprio e estando sujeitas aos preceitos gerais previstos no Código Civil, especialmente os seus arts. 186, 187 e 927.

Aliás, uma vez atendido determinação judicial de retirada de conteúdo ofensivo, considera-se que não há ato ilícito apto a ensejar reparação civil a título de danos morais. Essa conclusão é reforçada pela compreensão dos tribunais de que a fiscalização prévia de conteúdos de internet portadas no ambiente virtual por cada usuário não é atribuição intrínseca do serviço prestado pelos provedores de internet. Nesse sentido, reforça-se que o site que não examina e filtra os dados e imagens nele inseridos por cada usuário não se enquadra como serviço defeituoso, nos termos do art. 14, do CDC. (TJDFT. Acórdão 1164684, Relator: Carlos Rodrigues, 6ª Turma Cível, DJe: 24/4/2019).

Cabe acrescentar que a plataforma administradora de conta virtual tem obrigação de bloquear o perfil social invadido por terceiro para proteção do usuário cadastrado legitimamente. No entanto, para espaços que possuem o formato de *fanpages*, o espaço virtual se trata de domínio de terceiro destinado a interagir com pessoa pública de modo que somente se admite a remoção pontual dos conteúdos ilegítimos, e não a remoção integral dos endereços de indicação das URLs (*uniform resource locator*), sob pena de configuração de censura prévia, em ofensa ao interesse público. (TJDFT. Acórdão 1357579, Relatora: Desª. Diva Lucy de Faria Pereira, 1ª Turma Cível, publicado no DJe: 4/8/2021).

Em síntese, para as situações nas quais há inserção de conteúdo ofensivo por terceiro no ambiente virtual, a responsabilidade civil dos provedores de aplicações de internet é pautada pelos seguintes entendimentos fixados pela jurisprudência (AgInt no REsp 1504921/RJ):

> (i) não respondem objetivamente pela inserção em site, por terceiros, de informações ilegais;
> (ii) não são obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários;
> (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos;
> (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso;
> (v) a validade de comando judicial que ordene remoção de conteúdo na internet exige a indicação clara e específica do localizador URL do conteúdo infringente pelo requerente.

Situação distinta é o caso de invasão de contas (perfis online) efetuada por *hackers*. Nesse caso, não se avalia o grau de ofensa de conteúdo inserido por terceiro, mas a incumbência do provedor de implantar medidas de segurança efetiva e satisfatória contra riscos cibernéticos de seu empreendimento. Esses casos atraem a incidência da responsabilidade civil por fato do serviço uma vez que, conforme consignou a Ministra do STJ Nancy Andrighi, relatora no julgamento do REsp nº 1.193.764/SP, "*o fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração' contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor*". (STJ - Terceira Turma, DJe 08/08/2011).

Em caso enfrentado pelo Tribunal de Justiça de Minas Gerais (TJ-MG), usuária de plataforma digital (Instagram), que se autodenominou "Digital Influencer", mantinha perfil social com mais de 86.000 (oitenta e seis mil) seguidores, utilizada como ferramenta de trabalho. A conta em questão foi invadida por um *hacker*, que modificou suas informações e apagou suas publicações. Para o tribunal, o reconhecimento de gastos realizados pela usuária para impulsionar a visualização das postagens perante a plataforma reforçou a natureza a natureza da relação de consumo firmada entre as partes, o que ensejou a responsabilidade pelo fato do serviço prestado diante da ausência de provimento de mecanismos de segurança de suas atividades. No caso, a invasão de conta privada foi pontuada como risco cibernético inerente do empreendimento da plataforma, de modo a ensejar responsabilidade civil independentemente de culpa:

> A responsabilidade civil do provedor pela conduta dos invasores das contas dos seus usuários é objetiva, já que incumbe àquele a implantação de segurança efetiva e satisfatória contra os riscos cibernéticos do empreendimento
> A inexistência da gestão dos riscos ocorridos no meio virtual, e da adoção de mecanismos adequados fornecidos pela rede social aos seus usuários, indicando postura negligente e imperita que possibilita a atuação de "hackers", invadindo o perfil de quem utiliza a plataforma como ferramenta de trabalho, sem que haja a pronta resolução do fato, com a recuperação da conta pelo seu titular, materializa prática deflagradora de dano moral.
> [...]
> (TJ-MG - AC: 10000204763569001 MG, Relator: Roberto Vasconcellos, Data de Julgamento: 26/11/2020, Câmaras Cíveis / 17ª CÂMARA CÍVEL, Data de Publicação: 27/11/2020)

Pertinente anotar que, no caso, os danos morais se verificaram *in re ipsa*, ou seja, decorreram do reconhecimento dos próprios acontecimentos, de uma postura reconhecida como negligente e imperita da plataforma digital. A despeito de anotar que o dano moral é a lesão de

bem que integra os direitos da personalidade, o TJMG reconheceu que a lesão acarreta dos sofrimento, tristeza, vexame e humilhação, em referência ao posicionamento de Carlos Roberto Golçaves (2014) a respeito do dano moral. De toda forma, foi reconhecido ilícito suscetível de reparação a título de dano moral. Nota-se, portanto, que a responsabilidade civil objetiva recorreu à disciplina do Código de Defesa do Consumidor e não a lógica de responsabilidade civil pautada pelo MCI.

Ocorre que o entendimento do tema ainda é controvertido. No caso de estelionato digital realizado a partir de conta hackeada por terceiro, o reconhecimento da responsabilidade objetiva com base na constatação de uma falha no dever de segurança gera decisões com posicionamentos (e resultados) diversos a respeito da consideração do enquadramento do evento como fortuito interno ou externo. Por um lado, ao se considerar que a atuação indevida por terceiro (fraude) não rompe o nexo causal entre a conduta do fornecedor e os danos suportados pelo consumidor ou titular de dados, reconhece-se que a violação decorre de risco inerente ao exercício da atividade desempenhada pela prestadora de serviços, tratando-se de fortuito interno, de acordo com a teoria do risco da atividade. Por outro viés, ao se considerar tal atividade como fortuito externo, reconhece-se o rompimento do nexo causal entre o dano e o serviço prestado, de modo que os danos experimentados pela vítima serão por ela suportados (MIRAGEM, 2021).

A despeito das críticas a respeito da avaliação do nexo de causalidade do fornecedor a partir da distinção entre fortuito interno e externo (BESSA, 2022), o TJDFT apresenta relevante posicionamentos que retratam a dificuldade de se considerar o dano como risco inerente ou não à atividade desempenhada pelas plataformas de conteúdo, em especial, as de rede social. (TJDFT. Acórdão 1658370, DJE 14/02/2023 e acórdão 1629378, DJE 07/11/2020). No caso de conta social do Instagram hackeada por terceiro, o TJDFT reconheceu falha na prestação do dever de segurança com base nos artigos 6º, incisos VII e VIII (princípios da prevenção e da segurança), 42, *caput* e 44, incisos, I, II e III e parágrafo único combinados com o art. 14, *caput* e parágrafos seguintes do CDC, com base no art. 45, da LGPD (reforço autorizativo para aplicação do diálogo das fontes. (Acórdão 1658370, Relator: Rita De Cássia de Cerqueira Lima Rocha, 1ª Turma Recursal, DJE: 14/2/2023).

No caso, a despeito do relevante reconhecimento da falha no dever de segurança dos dados com remição à LGPD, a responsabilidade do provedor foi primordialmente baseada no reconhecimento do fato do serviço (art. 14, CDC) e com base na consideração de que esse tipo

de fraude (estelionato cibernético) é evento ligado à própria organização do negócio explorado, em aplicação à Teoria do Risco da Atividade do serviço prestado pelo provedor:

> REDE SOCIAL. INSTAGRAM. CONTA HACKEADA POR TERCEIRO. FRAUDE. ESTELIONATO CIBERNÉTICO OU VIRTUAL. RESPONSABILIDADE OBJETIVA. FALHA NO DEVER DE SEGURANÇA.
> 2. Incontroverso que a Recorrida teve seu perfil do Instagram hackeado por terceiros, que passaram a perpetrar golpes de vendas falsas pelo seu perfil, utilizando-se de sua credibilidade e imagem para auferir renda ilegal; incontroverso, também, que o Recorrente não enviou o e-mail para que a Recorrida possa recuperar a conta.
> 3. Legislação aplicável. **Em harmônico diálogo das fontes, com fulcro no art. 45 da Lei Geral de Proteção de Dados - LGPD, aplica-se ao caso o CDC e a LGPD,** concluindo-se ser, essa, relação consumerista e, o caso, de clara falha na prestação do dever de segurança que recai sobre o provedor de rede social, nos termos do art. 6º, incisos VII e VIII, 42, caput, e 44, incisos I, II e II e parágrafo único, todos da LGPD c/c art. 14, caput, e §§, do CDC.
> 4. Falha no dever de segurança dos dados. Na condição de agente de tratamento de dados, o Recorrente é responsável por cuidar dos dados por ele controlados, observando a boa-fé e os princípios da segurança e da prevenção, com a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. **O tratamento de dados pessoais será irregular quando não fornecer a segurança que dele se pode esperar, respondendo, o controlador ou operador dos dados, pelos danos decorrentes de sua violação, ao deixar de adotar as medidas de segurança indicadas e necessárias.**
> 5. Da responsabilidade pelo dano. O estelionato cibernético é aquele realizado por terceiros que invadem o banco de dados de grandes provedores e utilizam os dados obtidos para realizar obter dinheiro ilegalmente dos contatos e seguidores da pessoa titular do perfil violado. Uma vez que o Recorrente é quem detém os dados e realiza o seu tratamento sem cuidar da segurança esperada, deve responder objetivamente pelos danos que sobrevierem a partir da violação. Esse tipo de fraude é evento ligado à organização do negócio explorado - Teoria do Risco da Atividade - razão pela qual deve indenizar os prejuízos causados ao usuário, dado que compreende caso de fortuito interno.
> [...]
> (TJ-DF 07094063920228070009 1658370, Relator: Rita de Cássia de Cerqueira Lima Rocha, Data de Julgamento: 27/01/2023, Primeira Turma Recursal, Data de Publicação: 14/02/2023) – grifos da autora.

Por outro lado, o mesmo tribunal reconheceu – em caso distinto, mas sobre o mesmo tema (apropriação de conta usuário do Instagram por terceiros) – que a recuperação da conta hackeada pela rede social é suficiente para atender às obrigações da provedora. Insuscetível, no caso, o reconhecimento de dano moral ao caso, por ausência constatação de serviço defeituoso, antes a ausência, na Lei do Marco Civil da Internet, de regra que imponha a tais empresas responsabilidade objetiva por atos de terceiros.

No caso, ponderou-se que o defeito de segurança é caracterizado pelo que razoavelmente se espera de modo que não se mostra razoável exigir um nível de segurança com proteção absoluta. Trata-se, segundo esse posicionamento, de conhecimento geral que as redes sociais se destacam pela facilidade de acesso e por um nível de segurança meramente mediano. Nesses termos, a despeito do risco da atividade e da exploração comercial de serviços de internet, não há base legal que permita atribuir responsabilização civil do provedor (como no caso da rede social Instagram) em toda situação que houver violação do sigilo de informações por meio de ação de hacker nas contas individuais dos usuários restando afastada, por esse raciocínio, o reconhecimento de dano moral *in re ipsa* no caso enfrentado:

> RESPONSABILIDADE CIVIL. CONTA EM REDE SOCIAL. INSTAGRAM. APROPRIAÇÃO POR TERCEIROS (HACKERS). AUSÊNCIA DE DEFEITO NA PRESTAÇÃO DO SERVIÇO. DANOS MORAIS. NÃO CABIMENTO.
> 2 - Responsabilidade civil. Rede social. Segurança esperada. Fortuito externo. O fornecedor responde pelos danos decorrentes de defeito no serviço. O defeito de segurança é caracterizado pelo que razoavelmente se espera, de conformidade com as circunstâncias relevantes como o resultado, os riscos e o modo de fornecimento e época em que o serviço é fornecido (art. 14, § 3º., do CDC). As redes sociais se destinam a interação social, informação, comunicação e manifestação do pensamento, serviços que não se mostram como essenciais, nem vinculam obrigação de resultado. Não se mostra razoável exigir um nível de segurança com proteção absoluta. Ao contrário, é de conhecimento geral que as redes sociais se destacam pela facilidade de acesso e por um nível de segurança mediano. A propósito, não há, na Lei do Marco Civil da Internet (Lei n. 12.965/2014), regra que imponha a tais empresas responsabilidade objetiva por atos de terceiros. A jurisprudência sobre o tema: "4 - A despeito do risco da atividade e da exploração comercial dos serviços de internet, não há que se falar em responsabilização civil do provedor, no caso a rede social Instagram, em toda situação em que, por violação do sigilo de informações, houver ação de hackeamento nas contas individuais dos usuários.
> 5 - O controle possível ao provedor de serviços de serviço de internet se deu após o fornecimento de endereço eletrônico seguro e adequado pelo usuário, na conformidade com a política de privacidade e termos de uso da rede social. Além disso, os cuidados mínimos exigidos do provedor foram tomados, uma vez que houve informação prévia e especificada ao usuário sobre a tentativa de acesso em localidade diversa e, mais que isso, sobre a alteração cadastral efetivada por terceiros estranhos. Conquanto devida a determinação de restituição da conta da usuária, não existe falha no serviço que enseja a responsabilização a título de dano moral, porque inexistente o nexo de causalidade entre os danos alegados e a conduta do Réu em fornecer os instrumentos necessários para o controle da segurança e privacidade e da privacidade da conta da Autora na rede social, o qual só se estabelece em função de ação de terceiro (hacker) capaz de comprometer as funcionalidades e o sistema de segurança da conta, afastando-se, portanto, a responsabilidade civil reconhecida, nos termos do artigo 14, § 3º, II, do CDC." (Apelação 1341816, Relator: ANGELO PASSARELI).

> 3 - Defeito por informações insuficientes ou inadequadas. Não se vislumbra defeito por informações insuficientes ou inadequadas sobre fruição e riscos do serviço (art. 14, caput, do CDC). [...] Ademais, no caso em exame, a conta, inclusive, já foi recuperada. Assim, não vislumbro verossimilhança na alegação de que o serviço é defeituoso.
> 4 - Fato de terceiro. Fortuito externo. Na forma do art. 14, § 3º., inciso III, a culpa de terceiro, como fortuito externo, rompe o nexo de causalidade, com o que afasta a obrigação de indenizar. Sem a demonstração de que o serviço seja defeituoso, não há obrigação de indenizar.
> 5 - Danos morais. Para além da ausência de responsabilidade da ré por ato de terceiros, a privação de uso das redes sociais não afeta interesses essenciais da pessoa natural de modo a fundamentar a condenação por danos morais. É necessário que reste demonstrado fato que transborde para violação a direitos da personalidade. Precedente neste sentido: "A mera suspensão ou desativação indevida de perfil de rede social não é causa de dano moral, pois ele não se configura in re ipsa nestes casos. Cumpre observar que, no mais das vezes, as redes sociais são mera fonte de recreação e compartilhamento de conteúdo, cuja privação por tempo razoável, ainda que indevida, não configura qualquer ofensa relevante a direito de personalidade" (Acórdão 1424124, Relatora MARILIA DE AVILA E SILVA SAMPAIO). No caso em exame não ficou demonstrado fato que vá além da mera utilização do perfil, de modo que não há fundamento suficiente para indenização por danos morais. Sentença que se reforma para julgar o pedido improcedente. 6 - Recurso conhecido e provido. (Acórdão 1629378, 07012064320228070009, Relator: Aiston Henrique de Sousa, Primeira Turma Recursal, data de julgamento: 14/10/2022, publicado no DJE: 7/11/2022.)

A quebra da expectativa de segurança para casos de estelionato digital enfrenta debates e resultados distintos no âmbito dos tribunais. Nenhum dos casos acima, ressalte-se, atrelou a análise da responsabilidade com base na segurança esperada pelo titular de dados pessoais. De um lado, considerou-se a tutela mais paternalista do Código de Defesa do Consumidor a reconhecer que o estelionato digital praticado por terceiros que invadem constas de redes sociais atrai o reconhecimento de falha na prestação do serviço, tratando-se de fortuito interno da prestadora de serviços de modo que, mesmo diante de fato inevitável e imprevisível, liga-se à própria atividade do agente.

Tais considerações subsidiam o raciocínio de que a obrigação de segurança da plataforma não pode ser transferida ao consumidor. Nesse mesmo sentido, reconhecida a relação de consumo entre plataforma e usuário, o Tribunal de Justiça da Bahia considerou insuficientes as alegações da plataforma quanto à disponibilização de ferramentas de segurança como argumento apto a afastar a responsabilidade pela invasão de perfil da usuária. No caso, a conta hackeada apenas foi restabelecida por determinação do tribunal, o que, pela argumentação do relatório do acórdão, indica ser fator que contribuiu com a consideração de serviço defeituoso e correspondente dever de indenizar:

> "O acionado, ora recorrente, interpôs o presente recurso, almejando a reforma da sentença que julgou procedente a demanda para condenar a parte acionada a indenizar a autora pelo dano moral experimentado, pagando-lhe uma indenização de R$ 5.000,00, além de determinar o cumprimento da obrigação de fazer, consistente em restabelecer o acesso do autor à conta "@rebanho_di_lari" da plataforma INSTAGRAM. [...] Quanto à responsabilização da ré, sendo a plataforma de interação que oferece aos seus usuários o serviço prestado, deve este fornecer também a segurança que dele se espera. Está presente a hipótese do art. 14, § 1º, do CDC, segundo a qual "o serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar. Ora, **a obrigação de segurança na plataforma não pode ser carreada aos usuários, pois isso implica transferência de responsabilidade ao consumidor.** Assim, tratando-se de fato do serviço, é obrigação da ré indenizar a autora pelos danos causados. O uso indevido de perfil em redes sociais causa evidente dano moral, na medida em que resulta na invasão indevida à intimidade da parte autora, a qual é inviolável. [...]
> Relatório. (TJ-BA - Ri: 01805807520218050001 Salvador, Relator: Martha Cavalcanti Silva De Oliveira, 4ª Turma RecurSAL, Data de Publicação: 04/10/2022).- grifos da autora.

Por outro lado, considera-se a lógica de aplicação do MCI às fraudes exemplificadas, de modo a não reconhecer um dever imputável aos provedores de conteúdo da internet de garantir a inviolabilidade dos dados de seus usuários. Por esse raciocínio, resta afastado o reconhecimento de um dano moral decorrente da mera invasão de contas por terceiro. À vítima cabe suportar eventuais danos experimentados, uma vez não reconhecido ato ilícito imputável a esses provedores.

Nota-se, em síntese, que o tema ainda enfrenta posicionamentos pautados por justificativas distintas. Com base na proposta classificatória apresentada, o caso de invasão de contas de redes sociais de fato representa um tratamento irregular, pois há um acesso e uma atividade não autorizada pelo titular ou com base legal que a legitime. A espécie de responsabilidade civil nesses casos depende da perspetiva colocada em análise. Por um lado, a invasão pode representar a inobservância da LGPD ou de regulamento emitido pela ANPD – a configurar, respectivamente tratamento ilícito e indevido de dados pessoais.

Ao considerar o tratamento irregular por violação à expectativa de segurança de dados pessoais, há, como sustentado, uma nítida aproximação de técnica legislativa adotada pelo art. 44, *caput*, segunda parte, da LGPD, com a disciplina de fato do serviço do CDC (art. 14). No entanto, essa consideração não pode, de fato, culminar na conclusão de que toda e qualquer invasão ou violação de segurança de dados seja absolutamente atribuível ao provedor de conteúdo, sob pena de subverter a lógica da disciplina da LGPD, pautada pela conciliação de interesses contrapostos.

Nesses termos, propõe-se que, nos casos concretos, sejam considerados as medidas de segurança adotadas pela plataforma (como verificação de segurança em duas fases) e a prestabilidade e efetividade de serviços de auxílio à recuperação de contas de usuário. É possível, ademais, analisar a capacidade da plataforma em adotar medidas de segurança que levem em conta padrões de seus usuários, não com o propósito de examinar a legitimidade do conteúdo em si (em risco de incorrer em violação à liberdade de expressão) mas para avaliar comportamentos online que fujam do habitualmente exercido pelo titular usuário (em semelhança ao exigido às instituições financeiras).

Nesses termos se coaduna o entendimento do TJDFT, em caso de usuário que teve seu perfil de Instagram hackeado por terceiros que passaram a perpetrar golpes de vendas falsas em seu perfil. No caso, a despeito das tentativas de contato do usuário, a plataforma não enviou instrumentos de recuperação de conta (como e-mail) ou ofereceu soluções na via administrativa. Esse fator agravou o reconhecimento da situação como falha na prestação do serviço bem como no dever de segurança de dados. A gravidade da irregularidade do tratamento de dados, no caso, foi intensificada pela relutância da plataforma em adotar medidas determinadas judicialmente:

> AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZATÓRIA POR DANOS MORAIS. INVASÃO POR HACKER DO PERFIL DA AUTORA NA REDE SOCIAL INSTAGRAM. ALEGAÇÃO DE QUE SOFREU AMEAÇA.
> 2. Causa de pedir que se consubstancia em invasão do perfil da apelada, composto por 12 mil seguidores, na rede social Instagram, cujo hacker lhe exigiu o envio de dinheiro ou fotografia nua para que não deletasse a conta.
> 3. O conjunto probatório dos autos demonstrou que **diversas foram as tentativas frustradas de recuperação do perfil, vez que as respostas automáticas dadas pelo recorrente indicavam a necessidade de utilização do e-mail ligado à sua conta, que, contudo, também foi alvo de ataque do hacker, fato reiteradamente informado pela usuária ao provedor**.
> 4. O art. 19 da Lei nº 12.965/14 estabelece que "o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente".
> 5. Após a edição da referida lei, a responsabilização do provedor se caracteriza quando recebe notificação judicial acerca do conteúdo ofensivo a` honra ou imagem da pessoa, com a indicação clara e especifica da URL, e deixa de tomar as providencias cabíveis, sendo este o entendimento do STJ a respeito do tema - REsp 1694405/RJ - Ministra Nancy Andrighi - Terceira Turma - Data do Julgamento: 19/06/2018.
> 6. A responsabilidade solidária do apelante restou configurada, na medida em que **demorou mais de um mês, após a notificação judicial, para resolver a questão.**
> 7. Dano moral configurado, vez que a apelada sofreu lesão à sua imagem e honra, tanto pelas ameaças recebidas pelo hacker quanto pelo uso indevido de

> sua conta, na medida em que entrou em contato com seus seguidores, ocultou fotografias, publicou vídeo e alterou os dados do perfil. [...]
> 9. **Não prospera a alegação do apelante de que não deu causa à propositura da demanda, ante a frustração da resolução do problema na via administrativ**a, de modo que, restando vencido, deve arcar com o ônus da sucumbência, nos termos do art. 85, caput, do CPC. 10. Recurso conhecido e desprovido.
> (TJ-RJ - APL: 00081919320208190045, Relator: Des(a). Marianna Fux, Data de Julgamento: 02/06/2021, 25ª Câmara Cível)

Essas são as considerações que pautam a análise da segurança esperada pelo titular de dados pessoais (incisos do art. 44, da LGPD). A classificação e interpretação sugerida tem a aptidão de conciliar os interesses contrapostos em eventos danosos perpetrados por fraudadores, em diálogo sinérgico com o MCI e o CDC. De um lado, assegura-se a tutela aos interesses do titular, por exigir-se do provedor atuação ágil que facilite as interações do usuário para recuperar sua conta bem como a adoção de medidas de segurança aptas a evitar acessos indevidos e, se cabível, a análise de repressão de potenciais atuações ilegítimas de acordo com os padrões de interação do usuário. Por outro lado, assegura-se ao provedor o exercício de sua atividade sem imputação irrestrita de todo e qualquer evento danoso, consideradas as técnicas de tratamento de dados pessoais disponíveis e o modo pelo qual é realizado.

9.4 Síntese da proposta classificatória e crítica à hipernomia.

Há duas esferas de proteção de dados pessoais distintas – mas não excludentes – previstas na LGPD (art. 44, *caput*). Uma é voltada a assegurar que a conduta dos agentes de tratamento seja adequada às normas que regulam a atividade de tratamento de dados pessoais (primeira esfera). A outra tem como foco a tutela da expectativa de segurança dos titulares de dados no tratamento de informações que os identifiquem ou os tornem identificáveis (segunda esfera).

A primeira esfera de proteção atrai a análise responsabilidade civil quando ocorre uma violação normativa *lato sensu* da proteção de dados. Tal hipótese caracteriza o tratamento *irregular* por violação à legislação (art. 44, *caput*, primeira parte, da LGPD) a qual pode ser desdobrada em duas modalidades. A primeira denomina-se tratamento *ilícito*, que se configura quando o agente de tratamento, em uma violação de conduta, causa um dano ao titular de dados pela prática de um ato que infringe alguma exigência da Lei de Proteção de Dados Pessoais. Trata-se da hipótese de incidência do art. 42, *caput*, da LGPD. A segunda modalidade é descrita como tratamento *inadequado*, o qual se verifica na circunstância em que o agente de tratamento,

por omissão de conduta caracterizada pela ausência de adoção de medidas de segurança definidas pela ANPD, cria a oportunidade para que terceiro cause danos ao titular de dados. Cuida-se de modalidade de responsabilidade civil que atrai a incidência do art. 44, *parágrafo único*, da LGPD.

Essa estrutura não esgota o regime de responsabilidade por tratamento irregular disciplinado pela LGPD. A segunda esfera de proteção dessa normativa tutela a legítima expectativa de segurança do titular dos dados, conforme expresso na segunda parte do art. 44, *caput*. Trata-se do tratamento irregular na hipótese em que o agente de tratamento não fornece a segurança que o titular de dados possa esperar.

Pela exposição dessa síntese classificatória nos termos propostos, nota-se que a LGPD disciplina de modo específico as violações de conduta perpetradas pelos agentes de tratamento. Trata-se de uma tendência regulatória mundial que alia o dever de cuidado (ou de cautela) à livre circulação de informações – tão necessária para a sociedade pós-moderna.

A disciplina do tratamento irregular por violação da legislação tutela o dever de prevenir danos – imputável aos agentes de tratamento para o exercício de um tratamento de dados pessoais. Exige-se, por pressuposto, a definição prévia de regras, seja no âmbito legal seja no âmbito regulatório (pela ANPD). Assim, o tratamento será *lícito* na medida em que são cumpridos os deveres impostos pela norma de proteção de dados pessoais. Por sua vez, o tratamento é *adequado* quando o agente de tratamento adota as medidas de segurança determinadas pela Autoridade Nacional de Proteção de dados.

A tutela da responsabilidade civil pelo tratamento ilícito ou inadequado tem por propósito a regulação das condutas dos agentes de tratamento: os danos tutelados são aqueles decorrentes da inobservância de regras previamente definidas. Nesse sentido, melhorias tecnológicas ou a definição de melhores práticas posteriores a um evento danoso não devem ser utilizadas para pautar a responsabilidade dos agentes de tratamento. Tal dever de razoabilidade encontra-se amparado no art. 44, da LGPD, o qual imputa ao intérprete a necessidade de considerar circunstâncias relevantes do período na análise do tratamento irregular, entre as quais, "*as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado*."

Tal proposta de sistematização, além de demonstrar a coesão interna da disciplina da responsabilidade civil na LGPD, é apresentada como proposta apta a possibilitar o convívio entre regulação e a livre circulação de dados – elemento inerente e essencial que pauta as relações da sociedade moderna.

De acordo com a proposta classificatória apresentada, o tratamento de dados pessoais será regular quando for lícito (conformação com a lei) e adequado (adoção de medidas de

segurança definidas pela ANPD). Se irregular, a definição dos dispositivos aplicáveis e a respectiva identificação dos elementos e excludentes da responsabilidade civil pautar-se-á pelo art. 42, *caput* – para o caso de tratamento ilícito –, ou pelo art. 44, parágrafo único – se enquadrado como tratamento inadequado. Ocorre que que tal classificação não esgota os requisitos exigidos para qualificar um tratamento de dados como regular. O modelo apresentado apenas cuida da primeira parte do art. 44, *caput*, da LGPD. Pela perspectiva da coerência interna da LGPD, não é possível olvidar da segunda hipótese de tratamento irregular prevista na segunda parte desse dispositivo. Trata-se do tratamento irregular que não fornece a segurança que o titular dele possa esperar.

Em primeira leitura, seria possível compreender que tal hipótese é regulada pelo art. 46, da LGPD, na medida em que este imputa aos agentes de tratamento o dever de adotar medidas de segurança aptas a proteger os dados pessoais. A conclusão, no entanto, deve ser outra. Afinal, a conformidade com "medidas de segurança" previamente definidas pela Autoridade Nacional não se confunde com "expectativa de segurança" do titular de dados, expressão que demanda a análise de um caso pela perspectiva da pessoa natural – a qual também pode ser indicada como a vítima de um tratamento irregular. Em outras palavras, a adoção ou não de "medidas de segurança" é objetivamente verificável: importa considerar se houve a definição de padrões técnicos mínimos pela ANPD e se o agente de tratamento os cumpriu ou não. A "expectativa de segurança", por outro lado, importa a análise de um caso pela perspectiva do titular de dados, ou seja, da pessoa natural e diante de circunstâncias concretas.

Nesse ponto, a LGPD expande o âmbito de tutela dos dados pessoais dos titulares. O tratamento de dados, ainda que lícito e adequado (por não violar a legislação considerada em sentido *lato sensu*), se não atender à expectativa de segurança do titular de dados, será irregular.

Para fins exemplificativos, toma-se a atividade das instituições financeiras como representativa da mais alta expectativa de segurança pelos seus usuários no tratamento de seus dados. No cenário em que essa instituição, como agente de tratamento, realiza todo o processamento de dados pessoais de acordo com a LGPD e adota todas as medidas de segurança definidas para a sua área de atuação, a eventual invasão (*data breach*) dos dados de seus clientes não ensejaria a responsabilidade da instituição pelos termos da primeira parte do art. 44, *caput*. Afinal, se o tratamento é lícito e adequado, em que pese a ocorrência de um eventual dano, não se verificaria uma possibilidade de conduta diversa que a instituição poderia ter tomado.

Ocorre que o tratamento regular de dados pessoais exige que seja – além de ser lícito e adequado – seguro o suficiente para atender as expectativas do titular. Não se exige, para esse último caso, a possibilidade de conduta diversa previamente prevista. Essa exposição reforça

que a LGPD abre espaço para tutelar um tratamento lícito e adequado, mas, ainda assim, irregular.

Os limites dessa responsabilidade e a forma como deve ser interpretada exigem a demonstração da complexidade desse instituto. A despeito da maior abrangência de tutela, não é a ocorrência de qualquer dano no âmbito do tratamento de dados pessoais que atrai a responsabilidade civil. Se assim o fosse, viver-se-ia uma verdadeira ditadura do titular de dados. O agente de tratamento seria punido pelo mero fato de empregar novas tecnologias. Não é um cenário que atende aos seus fundamentos da LGPD, especialmente no que se refere a proteger a privacidade sem obstar o desenvolvimento econômico, tecnológico e a inovação (art. 2º, I e VI).

Não se olvida do caráter simplificado dessa proposta. Trata-se de um caminho que permite pautar o tema que está em discussão pelo intérprete ou até mesmo pelo agente ou titular de dados. Em última análise, propõe-se esse caminho interpretativo para identificar em que momento ou circunstância o tratamento de dados pessoais será qualificado como irregular e atrairá a incidência da responsabilidade civil nos moldes apresentados pela LGPD, em especial, pelo dever de reparar danos, previsto no art. 42, *caput*, e pelo dever de responder por seus atos, conforme previsto no art. 44, parágrafo único (bem como pelo art. 44, *caput*, segunda parte).

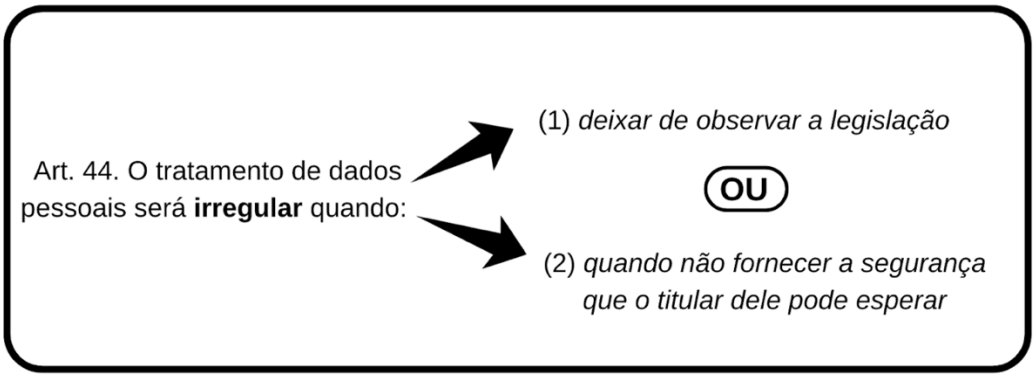

Figura 22. Demonstrativo visual do tratamento irregular como gênero de duas espécies. Elaborado pela autora.

Pelo quadro exposto, defende-se que, a par da decisão do Tribunal Constitucional Alemão, de 1983 – BVERFGE, 65, 1. (SCHWABE; MARTINS), a inovação tecnológica não é elemento, por si só, suficiente para tornar obsoleta a legislação de proteção de dados pessoais. É ultrapassada a noção de que a função legislativa acompanhe *pari passu* toda e qualquer modificação de contexto social. O quadro normativo da LGPD associado pelas outras

normativas específicas, como o CDC, é suficiente para a tutela de danos decorrentes de tecnologias disruptivas – como, em especial, pela Inteligência Artificial. É inconcebível considerar a necessidade de uma lei para regular cada novo aspecto social (ou cada inovação tecnológica). Afirma-se, inclusive, que o excesso de leis (ou hipernomia) equivale à inexistência de norma (SERRANO, 2020).

Para demonstrar a suficiência do quadro normativo de responsabilidade civil diante das inovações tecnológica, é preciso ressaltar a instrumentalidade da inteligência artificial (IA), tomada como exemplo representativo de tecnologias disruptivas. Diante a extensão do tema, essa análise é realizada em capítulo próprio.

PARTE III - RESPONSABILIDADE CIVIL NA PROTEÇÃO DE DADOS FRENTE A NOVAS TECNOLOGIAS: INTEGRAÇÃO NORMATIVA E INTELIGÊNCIA ARTIFICIAL.

10. COMO A IA MOLDA O MERCADO: REFERENCIAIS PARA ANÁLISE DA REGULAÇÃO E INFLUÊNCIA DA IA NA DEMANDA E NO CONSUMO.

A pandemia da COVID-19 acelerou o processo global de expansão do uso da Inteligência Artificial (IA). Avaliada em aproximadamente U$ 3 bilhões de dólares em 2019 – e com previsão de taxa de crescimento de mais de 29,7% no período de 2020 a 2027 – a IA se tornou componente-chave para a personalização da experiência do consumidor e para a criação de uma interação mais envolvente e célere entre empresas e consumidores.[75] Como a ação humana está sujeita a erros, o aumento do emprego da IA é também incentivado para eliminar as ineficiências que os humanos trazem para as operações, o que reforça a demanda pela utilização dessa tecnologia.

A título de exemplo, o Paypal utiliza a IA para detectar cobranças fraudulentas por meio de um mecanismo desenvolvido com ferramentas de *machine learning* (aprendizado de máquina), o que traz resultados de forma muito mais eficiente e eficaz do que uma análise realizada por pessoas. A PayPal é uma empresa norte-americana que opera como um processador de pagamentos para fornecedores online. A empresa utiliza o aprendizado de máquina (*machine learning*) para aprimorar seus recursos de gerenciamento de risco e detecção de fraude. Tradicionalmente, as instituições financeiras sinalizaram transações como de "alto risco" na elaboração de seus programas com base em um conjunto de regras claramente definidas para, em seguida, negar ou revisar manualmente as transações sinalizadas. No entanto, esta abordagem tradicional e manual para detecção de fraude está aquém das capacidades de identificação de fraudes por *machine learning* tendo em vista que a maior disponibilidade e complexidade de dados revela um deficit na revisão manual de pagamentos. Em 2019, por

[75] De acordo com a Conferência das Nações Unidas sobre o Comércio e Desenvolvimento (UNCTAD), as vendas globais de e-commerce representaram U$ 25,6 trilhões de dólares em 2018 – um aumento de 8% em relação a 2017. Para Indian Brand Equity (IBEF), o setor de e-commerce, avaliado em U$ 38,5 bilhões de dólares em 2017, deve crescer para quase U$ 200 bilhões até 2024. *in* Global Artificial Intelligence (AI) in Retail Market Size study, by Offering (Solution, Services), by Function (Operation-Focused, Customer-Focusing), by Technology (Computer Vision, Machine Learning, Natural Language Processing (NLP), Others) and Regional Forecasts 2020-2027. Research Report ID: MSR3357874. *Market Study Report*. Publicado em 15 de fevereiro de 2021.

exemplo, a rede de pagamentos Paypal realizou mais de 3.74 bilhões de transações, todas realizadas de forma rápida, de revisão praticamente instantânea e com baixos níveis de erros (também denominados como falsos positivos).[76]

O fenômeno que direciona a organização social com base no processamento de dados é paradoxal. Isso porque a empolgação com o desenvolvimento da IA para o mercado de consumo e sua incorporação nas relações sociais cotidianas é acompanhada pela preocupação com os riscos de sua utilização. Inúmeras iniciativas, em nível nacional e mundial, são fomentadas para a produção de estudos, regulamentos e orientações para assegurar a ética, promover a segurança de sua utilização e proteger a propriedade intelectual.

Como exemplo, cabe citar que o Parlamento Europeu está entre as primeiras instituições a apresentar recomendações sobre o que as regras da IA devem incluir no que diz respeito à ética, responsabilidade e direitos de propriedade intelectual. Em 2020, o Comitê de Assuntos Jurídicos (JURI) publicou três recomendações para estruturação de quadros legais para regular a IA. No mesmo ano, foi lançada a Parceria Global em IA (GPAI), desenvolvida no âmbito do G7, que visa apoiar pesquisas de IA e compatibilizar experiências com os Princípios Padrões da IA estabelecidos pela OCDE. No âmbito dos Estados Unidos, foi assinada uma Ordem Executiva para orientar a adoção da IA para as decisões governamentais de forma compatível com a proteção da privacidade e direitos civis. No Brasil, a atenção ao tema é representada pela Resolução do CNJ n.º 332/2020 – primeira iniciativa regulatória de IA para o Judiciário.

As abordagens são diversas, mas o objetivo é comum: compatibilizar a utilização segura da IA com a promoção da inovação. O estabelecimento de diretrizes decorrentes desses esforços tem papel fundamental para evitar acidentes e assegurar valores democráticos e de segurança nacional; mas não isenta a IA de riscos. Acidentes, como os de consumo, são inevitáveis e sujeitos à apreciação do Poder Judiciário (art. 5º, XXXV, CF/1988[77]). A análise do emprego da IA pela perspectiva das normas de responsabilidade civil torna-se inevitável. Ocorre que o fornecimento de respostas não acompanha o volume das dúvidas que são geradas pela complexidade de casos submetidos ao exame judicial.

A título de ilustração, em 2015, o promotor Marc R. Stanley, nos Estados Unidos, Califórnia, ajuizou ação coletiva contra a empresa Toyota Motor Corporation para defender usuários de carros alegadamente defeituosos sob o argumento de que as unidades de controle

---

[76] Disponível em <https://digital.hbs.edu/platform-rctom/paypals-use-of-machine-learning-to-enhance-fraud-detection/>. Acesso em 29/04/2021.

[77] Constituição Federal, art. 5º, XXXV – "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;".

dos veículos estariam vulneráveis a ataques de *hackers* – que permitiriam, à distância, acelerar, mobilizar freios e controlar a direção dos veículos. O caso ganhou repercussão pois, na época, o segmento *60 minutes*, da CBS News (rede americana de divulgação de notícias e conteúdo), supervisionou um *hacker* demonstrando como desativar freios de um carro usando apenas um laptop. Apesar da preocupação com ameaças à segurança e à privacidade dos consumidores, o processamento do caso foi indeferido por falta de comprovação de defeito ou dano efetivo.[78] De fato, nenhum veículo havia sido *hackeado*. Alegações de possíveis danos futuros não foram suficientes para o prosseguimento processual do feito.

Antes de avaliar o possível desfecho dessa situação se analisada sob a legislação brasileira[79], é possível notar que o caso representa a dificuldade de se identificar parâmetros legais claros para diferenciar receios especulativos de ameaças de lesões sujeitas à tutela jurídica. *Como caracterizar um defeito? Seria possível enquadrar danos causados pelo emprego da IA como vício? Como definir acidentes de consumo que envolvam a IA? Quais são os riscos tutelados?* Essas são algumas das questões que o atual sistema de responsabilidade civil deve responder a respeito de danos decorrentes do emprego da IA.

Como premissa de todo o trabalho desenvolvido sobre essa temática, toma-se que o restabelecimento do equilíbrio social violado pelo dano é o denominador comum de todos os sistemas de responsabilidade civil, "*estabelecendo-se, como norma fundamental, que a composição ou restauração econômica se faça, sempre que possível, à custa do ofensor*." (CAVALIERI, 2020, p. 39).

Ocorre que a convivência com a tecnologia tem expandido a função não apenas reparatória, mas também preventiva da responsabilidade civil. O acórdão da ADI nº 6387/DF é representativo dessa afirmação. No caso, o Supremo Tribunal Federal (STF) considerou que a Medida Provisória nº 954/2020 desbordou dos limites fixados pelos direitos fundamentais à proteção de dados e à autodeterminação informativa ao exigir que companhias telefônicas compartilhassem os dados de seus consumidores com o IBGE (Instituto Brasileiro de Geografia e Estatística). A conclusão pela inconstitucionalidade da norma impugnada se baseou mais na falta de estrutura de uma entidade para salvaguardar os direitos fundamentais do que no

[78] O magistrado William H. Orrick reconheceu a improcedência da ação, popularmente conhecida como "*The Defective Vehicle Class Action*", em novembro de 2015. *Cahen et al. v. Toyota Motor Corporation et al.,* Case No. 3:15-cv-01104, in the U.S. District Court for the Northern District of California.

[79] Pode-se adiantar que, pelo Código de Defesa do Consumidor, o caso não seria processado sob a alegação de fato do produto (art. 12, CDC) tendo em vista a ausência de danos efetivos. Poderia, no entanto, ser enquadrado como vício do produto, com amparo no art. 18 do diploma normativo.

conteúdo da normativa.[80] Em outras palavras, o risco de dano (e não propriamente sua ocorrência) foi determinante para afastar a constitucionalidade da normativa impugnada.

Esse posicionamento não inaugura uma nova preocupação do instituto da responsabilidade civil, mas direciona a posição que o Poder Judiciário tem tomado (e pode vir a tomar) ao tratar de questões relacionadas a dados e tecnologias de seu processamento – como a Inteligência Artificial. Para além dessa questão, identificar a legislação aplicável a determinado caso concreto envolve fatores complexos, pois abrange o conhecimento da IA e a análise da responsabilidade civil sob a regulação de diversas legislações – como o Código de Defesa do Consumidor (CDC), a Lei Geral de Proteção de Dados (LGPD), o Código Civil e o Marco Civil da Internet.

O enfrentamento do tema, portanto, não pode olvidar do conhecimento dos conceitos, riscos, aplicações e possibilidades dessa tecnologia. Afinal, viver na "Era da Inteligência Artificial" impõe que o indivíduo escolha entre ser cliente passivo da tecnologia ou titular do conhecimento que a impulsiona (HATMANN, 2020a). No fomento ao conhecimento, alinhar responsabilidade com o desenvolvimento da IA é preocupação central em todos os aspectos – sejam normativos, éticos ou sociais.[81] Como premissa do estudo da regulação de tecnologias, é indispensável estabelecer os elementos semânticos e semióticos[82] da IA, suas potencialidades, riscos, desafios e aplicações.

---

[80] No caso, a própria Ministra Rosa Weber afirmou que "*Não estou a afirmar que de modo algum os dados objeto da Medida Provisória nº 954/2020 possam ser compartilhados com o IBGE".* Interessante notar, que referida decisão representa posicionamento paradigmático para a proteção de dados pessoais no Brasil. Isso porque dela decorreu o reconhecimento da tutela constitucional do direito à autodeterminação informativa, alçado, nesse julgado, como direito fundamental e autônomo e também pelo fato de que foram definidos princípios e parâmetros para o tratamento e compartilhamento de informações pessoais. Por fim, cabe ressaltar que referida decisão foi publicada antes da vigência da Lei Geral de Proteção de Dados (LGPD), o que reforça a existência e um aparato normativo preexistente que ampara pretensões relacionadas à proteção à privacidade e aos dados pessoais. Supremo Tribunal Federal. ADI n.º 6.387/DF – Distrito Federal. Relatora: Min. Rosa Weber. Decisão de 07/05/2020, publicada no DJe em 02/06/2020.

[81] Para Fabiano Hartmann, pesquisas responsáveis em IA traduzem abordagens estratégicas da disciplina pois pressupõem a movimentação dos três espaços (governo, indústria e academia) bem como o domínio e difusão de conhecimento dessa tecnologia (potencialidades, riscos, desafios e aplicações) para então desenvolver aplicações da IA que apoiem soluções de problemas. PEIXOTO, Fabiano Hartmann. Direito e Inteligência Artificial. *Coleção Inteligência Artificial e Jurisdição*. Volume 2. Dr. IA: Brasília. 2020, p. 15.

[82] As terminologias e conceitos utilizadas para tratar da Inteligência Artificial não são unificados. Identifica-se que grande parte de problemas relativos a essa tecnologia se devem (ou ao menos se relacionam) com a falta de acordo terminológico de termos e definições. Fala-se em diferenciações semânticas e semióticas pois, conforme Benveniste sustenta, essas são as duas modalidades ou domínios de sentido. O sentido semiótico é o reconhecimento de uma unidade ser ou não dotada de sentido – o que se define por sim, não. Por sua vez, o sentido semântico resulta do encadeamento, da apropriação pela circunstância e da adaptação dos diferentes signos entre eles. AUGUSTINE, Cármen e RODRIGUES, Eduardo Alves. O conceito de língua em Benveniste. *Línguas e instrumentos linguísticos*. n.º 41. 2018.

11. ESTUDO ESTRATÉGICO DA IA E O DIREITO

A pesquisa relativa ao tema IA ***e*** Direito apresenta duas abordagens. A primeira diz respeito a preocupações com os parâmetros éticos no desenvolvimento de aplicações de IA ***para*** o Direito, ou seja, aquelas aplicações de IA destinadas (em especial) a atender fluxos de gestão processual e apoio à decisão. Nesse caso, a definição de parâmetros éticos é o meio que liga a eficiência proporcionada pela IA com a garantia de proteção a direitos fundamentais e a valores democráticos. A esse respeito, Fabiano Hartmann (PEIXOTO, 2020, pág. 12) reconhece que:

> não há que se falar em robustez, solidez, confiança e competitividade sem se levar em conta a dimensão ética e a capacidade de impacto da IA no Direito. [...] Sem referenciais éticos há um duplo risco: o primeiro de se fornecer elementos para a justificação de diversos mitos associados à aplicação da IA [...]; e o segundo, de se esvaziar o conteúdo positivo e benefícios de uma aplicação da IA

Especial exemplo dessa perspectiva é o Projeto Victor, realizado pela parceria Unb-STF. O Projeto Victor visa elaborar um algoritmo de classificação de peças processuais em temas de repercussão geral. Acerca do funcionamento e propósito do programa desenvolvido, Fernanda Lage (2021) sintetiza que:

> o Victor classifica dados: peças em temas de repercussão geral. Construiu-se um modelo baseado em um conjunto de treinamento e usa-se desse modelo para classificar novas observações. O objetivo é utilizar as variáveis de saída. Ele responde se uma determinada 'entrada' *(input* – peça processual) pertence a uma certa classe (tema de repercussão geral). [o projeto faz uma utilização do] *Machine learning* (aprendizado de máquina) [o qual] é a habilidade de sistemas de inteligência artificial (IA) de adquirir conhecimento próprio ao extrair padrões de dados não processados. Trata-se de uma área da inteligência artificial que permite que a máquina aprenda por meio de exemplos, semelhante ao que ocorre com os seres humanos.[83]

A segunda abordagem diz respeito aos efeitos das novas fronteiras das descobertas proporcionadas pela IA sobre a interpretação, compreensão e aplicação de institutos jurídicos. É o estudo da IA ***no*** Direito. Em outras palavras, o foco refere-se aos efeitos das modificações sociais (causados pela tecnologia da IA) sobre as disciplinas jurídicas, como as de direito penal,

[83] Para aprofundar o tema, ver PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. Revista Brasileira de Inteligência Artificial e Direito. Volume 1. RBDI. AID-IA. **2020**. Disponível em: <https://rbiad.com.br/index.php/rbiad>. Acesso em 02/05/2021.

empresarial, propriedade intelectual e até mesmo processual.[84] O estudo sobre a relação da IA com os institutos de responsabilidade civil se insere nessa linha.

Figura 23 - IA para o Direito e IA no Direito. Perspectiva visual. Elaborado pela autora.

Independentemente da perspectiva adotada, o debate que se estabelece no Direito tem como ponto central o fato de a IA provocar situações limites, seja na aplicação de institutos jurídicos "*seja com a execução de atividades fruto de sistemas de aprendizagem de máquina, restrição de liberdade e alteração de privacidade, delimitação de conteúdo e indução de preferências e a interconexão do raciocínio jurídico com o raciocínio matemático, forçando limites e resistência até então tidas como humanos*" (HARTMANN, 2020b, p. 38). Para qualquer seara mencionada, o debate relativo à IA e o Direito (seja IA ***para*** o Direito ou IA ***no*** Direito) inicia-se a partir da definição de *standards* conceituais com o propósito de realizar um acordo semiótico e semântico sobre o tema[85] bem como para diferenciar o tratamento que deve ser dado aos mitos associados a essa tecnologia.

[84] Para aprofundar a temática de aplicações de IA *para* o Direito, acessar portfólio do grupo de pesquisa DR.IA, liderado pelo Professor Dr. Fabiano Hartmann Peixoto (FD/PPGD/UnB) e pela Professora Dra. Debora Bonat (FD/PPGD/UnB). Disponível em: <http://dria.unb.br/> acesso em 03/05/2021. Para diversas abordagens da IA *no* Direito, ver LAGE; 2021, págs. 123 a 134.

[85] Benveniste sustenta que há duas modalidades ou domínios de sentido: o semiótico e a semântica. O sentido semiótico é o reconhecimento de uma unidade ser ou não dotada de sentido – o que se define por sim, não. Por sua vez, o sentido semântico resulta do encadeamento, da apropriação pela circunstância e da adaptação dos diferentes signos entre eles. (AUGUSTINE; RODRIGUES, 2018).

12. EMPREGO DOS DADOS PESSOAIS PARA A INTELIGÊNCIA ARTIFICIAL: *STANDARDS* CONCEITUAIS

O alto valor das informações pessoais decorre, em grande medida, de sua funcionalidade para o desempenho de tecnologias que manipulam informações para os mais diversos propósitos, como análises preditivas ou a tomada de decisões. É o caso de seu emprego como base de dados para a funcionalidade da Inteligência Artificial (IA) – tecnologia que se tornou componente chave para a personalização da experiência do consumidor e para a criação de uma interação mais envolvente e célere entre empresas e consumidores[86] tais como a sugestão de seriados e filmes com base no histórico de preferências anteriores do titular de dados.

O uso IA também é incentivado para eliminar as ineficiências e falhas humanas em operações cotidianas. A título de exemplo, reitera-se o exemplo do Paypal, o qual utiliza a IA para detectar cobranças fraudulentas por meio de um mecanismo desenvolvido com ferramentas de *machine learning* (aprendizado de máquina) cujos resultados se mostraram mais eficientes e eficazes do que os realizados por pessoas.[87]

O aumento da oferta e demanda por produtos que empregam IA ocorre em uma influência recíproca. Ao mesmo tempo que a IA proporciona aumento de eficiência para a indústria do varejo (por diminuir a necessidade de intervenção humana na produção de produtos ou na prestação de serviços), a expansão exponencial da IA no mercado de consumo é significativamente imputada ao fato de que as empresas influenciam a demanda por seus produtos e serviços quando buscam melhorar a experiência do cliente. Essa experiência e maior engajamento é proporcionada a partir da captação e tratamento de dados pessoais dos consumidores e potenciais clientes. A comodidade do comércio eletrônico e a demanda crescente de *chatbots* baseados em IA são apenas alguns dos exemplos que justificam o aumento no número de transações de comércio eletrônico.[88]

---

[86] De acordo com a Conferência das Nações Unidas sobre o Comércio e Desenvolvimento (UNCTAD), as vendas globais de e-commerce representaram U$ 25,6 trilhões de dólares em 2018 – um aumento de 8% em relação a 2017. Para a Indian Brand Equity (IBEF), o setor de e-commerce, avaliado em U$ 38,5 bilhões de dólares em 2017, deve crescer para quase U$ 200 bilhões até 2024. Global Artificial Intelligence (AI) in Retail Market Size study, by Offering (Solution, Services), by Function (Operation-Focused, Customer-Focusing), by Technology (Computer Vision, Machine Learning, Natural Language Processing (NLP), Others) and Regional Forecasts 2020-2027. Research Report ID: MSR3357874. *Market Study Report*. Publicado em 15 de fevereiro de 2021.

[87] Disponível em <https://digital.hbs.edu/platform-rctom/paypals-use-of-machine-learning-to-enhance-fraud-detection/>. Acesso em 29/04/2021.

[88] Global Artificial Intelligence (AI) in Retail Market Size study, by Offering (Solution, Services), by Function (Operation-Focused, Customer-Focusing), by Technology (Computer Vision, Machine Learning, Natural Language Processing (NLP), Others) and Regional Forecasts 2020-2027. Research Report ID: MSR3357874. *Market Study Report*. Publicado em 15 de fevereiro de 2021

O aumento de fluxo de dados na Sociedade da Informação decorre tanto da incorporação de tecnologias nas relações interpessoais cotidianas quanto na ampliação do leque de possibilidades proporcionado pelo avanço tecnológico. Motivações mercadológicas impulsionam a tecnologia, mas o fenômeno é acompanhado de preocupações com os riscos de seu emprego, especialmente no que concerne aos possíveis abusos na coleta e processamento de dados que identifiquem ou tornem uma pessoa identificável.

Esse cenário revela intensa correlação entre a disciplina de proteção de dados pessoais e grande parte das aplicações de Inteligência Artificial. No campo da responsabilidade civil, a interação dessas disciplinas demanda a análise específica da incidência da LGPD, em especial, de seus artigos 42 e 45. Há que se demonstrar que, longe de ser considerado um instrumento pautado por vontades próprias, a denominação *inteligência* para descrever a IA recai na sua capacidade de processamento para efetivar ajustes automatizados que aumentam a eficiência para os propósitos especificamente detalhados por humanos. O caráter instrumental da IA é determinante para apontar o regime de responsabilidade aplicável.

12.1 Compreensão da Inteligência Artificial (IA).

A Inteligência Artificial é subcampo da ciência da computação que tem como propósito reproduzir habilidades cognitivas tipicamente humanas. Esse é um conceito contemporâneo de IA e (de forma proposital) não exaustivamente delimitado. Contemporâneo (ou moderno) porque a ideia de dotar objetos com autonomia ou inteligência é tão antiga que encontra exemplos na Antiguidade Clássica, como na mitologia grega, com o gigante de bronze Talos – contemporâneo de Homero (século 8 ou 9 a.C.) – e nos robôs Ajatasatru e Asoka, guardiões das relíquias de Buda.[89]

O conceito também não é exaustivamente delimitado pois, conforme afirma Nils Nilsson (1983), "*simply put, there is wide disagreement in the field about what AI is all about*" o que, em tradução livre, implica reconhecer que, simplificadamente, há um grande desacordo sobre o conceito, o que é e do que se trata a IA. Em outras palavras, não há consenso quanto à

[89] Pela mitologia grega, Talos foi uma estátua criada por Hephaestus para defender a ilha de Creta de piratas. Dentro de outros exemplos históricos, Adrienne Mayor realiza paralelos entre mitos antigos e autômatos místicos que aparecem em contos sobre Medéia, Prometeu e Pandora, além de outras histórias de origem chinesa e indiana. (MAYOR, 2018). A esse respeito, Fernanda Lage aprofunda o tema ao lecionar que "a ideia do homem criar uma máquina que possa reproduzir suas habilidades contando com uma certa inteligência [...] remonta à Grécia Antiga, e estudos demonstram que aproximadamente no ano de 205 antes de Cristo foi construída a máquina (ou mecanismo) de Antícera, formada por um intrincado sistema de engrenagens de bronze capaz de prever posições celestes, fases da Lua, eclipses e calcular calendários." (LAGE, 2021, págs. 29 e 30).

sua definição. Por outro lado, é possível afirmar que seu propósito é ampliar as possibilidades do exercício de funções complexas desempenhadas por máquinas (robôs/programas/softwares).

Definir Inteligência Artificial é tarefa complexa. Para Fernanda Lage (2021, pág. 47), trata-se de“ *uma mistura de ciência da computação, matemática e outras ciências que busca que as máquinas repliquem as habilidades cognitivas dos seres humanos*.” Para Fabiano Hartmann (2020, pág. 17), IA é “*um ramo da ciência da computação que busca, com interação multidisciplinar com outras áreas do conhecimento, a reprodução de ações cognitivas tipicamente humanas*.”

Não há um conceito unívoco de IA. Pode-se, no entanto, reconhecer que a capacidade de integração de funções cognitivas artificiais e os variados graus de sua complexidade são pontos determinantes de seu estudo. Para as finalidades desse trabalho, inteligência artificial é a tecnologia empregada para mimetizar habilidades cognitivas tipicamente humanas. O conceito apresentado é suficiente tanto para especificar a IA como subcampo da ciência da computação como para identificar o propósito de seu desenvolvimento.

O termo *Inteligência Artificial* foi oficialmente cunhado em 1956, na Conferência de Darthmouth, organizada por John McCarthy (1995) – o que lhe garantiu o reconhecimento título de “pai da IA”.[90] A proposta de estudo a Conferência de Darthmout adotou como pressuposto a noção de que qualquer aspecto do aprendizado ou qualquer característica da inteligência pode ser descrito de uma forma tão precisa que uma máquina poderia simulá-lo.

Antes disso, o projeto de Warren S. McCulloch e Walter Pitts – em 1943 – criado para discutir a noção de redes neurais artificiais, é reconhecido como o primeiro trabalho publicado sobre máquinas inteligentes (MCCULLOCH, PITTS; 1943). É também relevante o trabalho de Alan Turing na publicação intitulada “*Computing Machinery and Intelligence*” (1950), pois foi utilizado como estrutura base de discussão para verificar se uma máquina poderia ou não demonstrar um comportamento inteligente. O “jogo da imitação”, como ficou reconhecido o Teste de Turing, marcou uma mudança de perspectiva: ao invés de verificar se uma máquina pode pensar, deve-se buscar meios para identificar se uma máquina pode agir de forma inteligente.

O histórico da ciência da Inteligência Artificial passou por ondas de grande entusiasmo e expectativas, mas também por prognósticos pessimistas e de cortes de investimento nos seus

[90] O documento oficial, em sua integralidade, pode ser acessado em <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>. Acesso em 14/04/2021

estudos (períodos conhecidos como "*Invernos da IA*", que ocorreram em 1974 a 1980 e, novamente, em 1987 a 1993)[91].

Eventos do início do século XXI – como os avanços no poder de processamento computacional e o aumento da capacidade de armazenamento e de captação de dados – impulsionaram o desenvolvimento da engenharia de *softwares* para processamento de dados e de técnicas de Inteligência Artificial, as quais se integraram à produção industrial e se tornaram elementos indispensáveis no cotidiano de sociedades.

A funcionalidade da IA recai sobre o uso de algoritmos e da qualidade dos dados. O algoritmo é uma sequência metódica e bem definida de instruções computacionais para resolver problemas por meio do processamento de dados. O termo "*descreve um procedimento computacional específico para obter uma saída* (resultado) *para uma determinada entrada*." (LAGE, 2021, p. 38). Em outras palavras, cuida-se de uma sequência metódica de instruções computacionais que, a partir de uma situação inicial (*input*), transita por diferentes etapas até produzir uma saída (*output*). A "entrada" (ou *input*) descreve o dado que será processado. A "saída" (ou *output*) é a informação que resulta do processamento metódico das etapas instruídas.

Um algoritmo é um conjunto de instruções, uma receita pré-definida, rígida (estática) e codificada que funciona a partir de um gatilho inicial (como um impulso ou comando). A IA, além de abranger uma miríade de especializações e subconjuntos, é uma tecnologia que opera a partir de algoritmos, mas com eles não se confunde. Isso porque a IA pode modificá-los e criar novos algoritmos em resposta aos *inputs* de treinamento e outras entradas de dados – ao invés de depender apenas do reconhecimento de uma entrada específica para servir como gatilho (ISMAIL, 2018). Essa capacidade de mudar, adaptar e expandir com base em novos dados é descrita como "inteligência".

Fernanda Lage acentua esse contraste ao indicar que o que difere a IA da automação é justamente a capacidade de "aprender" a partir do processamento dos dados (LAGE, 2021, p. 127): "*a automação resulta de um software programado para realizar funções repetitivas e específicas. Já a IA é dotada de cognição e capacidade de aprendizado, ou seja, não está presa às funções originais de seu algoritmo e pode se "autoprogramar" para executar novas tarefas*." A partir de regras ou resultados que funcionaram na fase de treinamento, os algoritmos da IA podem aprender novas heurísticas (estratégias) de processamento[92] ou desenvolver novos algoritmos de computação para alcançar o objetivo para o qual foi projetado.

---

[91] Para uma objetiva linha do tempo da IA, ver LAGE, 2021, págs. 29 a 37.

[92] O aprendizado pela IA pode ser adquirido por diversas técnicas, como pelo método bayesiano e árvores de decisões. Teoricamente, diante de todos os dados possíveis, tempo para processar e memória computacional, é

Há diversas técnicas que a IA pode utilizar como estratégia de performance ou como método para aprender e operar. Daí decorre a afirmação de que a IA é termo guarda-chuva que abrange uma miríade de subconjuntos e especializações. Dentro dos métodos instrucionais, ganham destaque o *machine learning* (aprendizado de máquina) e o *deep learning* (aprendizado profundo).[93]

Machine learning (ML) é um subcampo da IA que, por sua vez, abrange o subconjunto *deep learning* (DL). O aprendizado de máquina pode ser conceituado como o estudo de algoritmos de computador que se aprimoram automaticamente por meio da experiência e do uso dos dados. Aprendizado profundo (DL), por sua vez, é uma classe do ML que utiliza algoritmos para percepções não lineares (ou seja, com algoritmos de múltiplas camadas) para extrair informações de uma entrada bruta de dados (muito utilizado para reconhecer imagens, rostos e textos manuscritos). A distinção entre ambos pode ser assim sintetizada (LAGE, 2021, p. 84):

> Observa-se que a distinção existente é que o começo do fluxo de trabalho de aprendizado de máquina se dá com os recursos (ou dados) relevantes sendo extraídos de forma **manual** das imagens ou do texto. E, esses recursos são usados para criar um modelo que categorize os objetos na imagem. Já no fluxo de trabalho de aprendizado profundo esses recursos relevantes são extraídos **automaticamente** das imagens. Além disso, o *deep learning* realiza o chamado 'aprendizado de ponta a ponta' – em que uma rede recebe dados brutos e uma tarefa a ser executada, como a da classificação, e aprende como fazer isso automaticamente. – grifos da autora.

Independentemente da abordagem ou especialização, é notável a importância e centralidade dos dados para o processamento da IA, ML e DL. Seja como dados de treinamento (*dataset*), seja como dados para *input* em processamento, o tratamento de dados é o durame da IA. O incentivo econômico dessa tecnologia reflete nas relações de consumo, cujo maior foco, sob a ótica empresarial, é direcionar conteúdos ou oferecer bens e serviços de forma personalizada – o que, naturalmente, é atividade que demanda o tratamento de dados pessoais do consumidor. Daí a íntima correlação entre a IA e a Lei Geral de Proteção de Dados bem

---

possível que o algoritmo realize combinações de funções matemáticas para descrever o funcionamento do mundo e realizar previsões com altos níveis de precisão e de acerto. Na prática, no entanto, é quase impossível considerar todas as possibilidades e hipóteses possíveis, mesmo com a tecnologia e capacidade de processamento atualmente disponíveis (2023).

[93] Há diversas técnicas que podem ser utilizadas como estratégia de performance ou delegação de funções repetitivas e roboticamente praticáveis. (PEIXOTO, 2020, pág. 17). Disso decorre a afirmação de que "*objetivamente, a IA pode ser considerada como uma constelação de tecnologias – da machine learning ao processamento de linguagem natural, que permite à máquina, percepções, compreensões, aprendizado e ações*." (PEIXOTO, SILVA, 2019, pág. 20).

como entre a IA e as normas de defesa do consumidor, em especial, o Código de Defesa do Consumidor (CDC).

A ascensão da internet levou ao aumento exponencial da qualidade e quantidade de dados disponíveis, chegando-se ao ponto em que os sistemas de gerenciamento de conjuntos de dados por softwares estatísticos e referenciais passaram por dificuldades para processar e visualizar os dados coletados. A busca por novas correlações em dados supostamente aleatórios lançou luz ao termo *big data* para se referir ao uso de análises preditivas e analíticas de comportamento de usuários a partir da captação dos mais diversos tipos de dados.

A criação de uma série de empresas – como Google, Apple, Facebook e Amazon (conhecidos pelo acrônimo: GAFA) – recai sobre o uso do *big data* e sua atividade passou a levantar questionamentos, especialmente quando se considera que suas atividades se aproveitam do entusiasmo das pessoas quanto aos serviços oferecidos na internet como subterfúgio para coletar seus dados pessoais e utilizá-los para treinamento ou como *input* de algoritmos de Inteligência Artificial.

Por isso questões éticas circundam os debates acerca da IA. É o caso da reprovação de estratégia de *marketing* adotada por empresa concessionária de linha de metrô de São Paulo, a qual implementou sistema de reconhecimento facial a partir de imagens captadas de usuários do metrô para fins comerciais, sem prévia autorização ou outra base legal para legitimar essa atividade.

A captação de imagens buscava detectar as principais características dos indivíduos que circulavam em determinados locais e trabalhos. O Tribunal de Justiça de São Paulo reprovou a conduta e reconheceu a caracterização de dano moral coletivo, especialmente diante do incontável número de passageiros que transitaram (e transitam) pela plataforma gerenciada pela concessionária todos os dias. (TJ-SP - AC: 10906634220188260100 São Paulo, Relator: Antonio Celso Faria, Data de Julgamento: 10/05/2023, 8ª Câmara de Direito Público, Data de Publicação: 12/05/2023).

No caso, o TJ-SP considerou o reconhecimento do dano moral coletivo em aferição *in re ipsa*, de forma que sua constatação decorreu da apuração da prática ilícita que viola direitos de conteúdo extrapatrimonial da coletividade. Diante da condição de vulnerabilidade dos consumidores, o tribunal impôs a condenação ao pagamento de quinhentos mil reais (R$ 500.000,00) a título de reparação e prevenção do mesmo tipo de ilícito.

A empresa alegou que não realizou a coleta ou armazenamento de dados pessoais, mas tão somente a detecção facial para fins estatísticos, de modo que os dados gerados não identificariam especificamente o passageiro. Afirmou que a tecnologia instalada nas Portas

Interativas Digitais se limitava a contar as pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, fator de visão, horas de pico de visualizações e distância de detecção sem que, todavia, houvesse a coleta de qualquer dados pessoal de pessoa individualizada.

Ocorre que a empresa não logrou em comprovar tal limitação do sistema nos autos. Ausente prova pericial dos equipamentos e sistemas operacionais vinculados, o TJ-SP rejeitou o argumento de defesa, uma vez que não havia dúvidas de que ocorria a captação da imagem de usuários sem seu conhecimento ou consentimento para fins comerciais. Considerando a natureza sensível dos dados pessoais coletados (art. 5º, II, da LGPD) o Tribunal suscitou que, ainda que não houvesse a identificação concreta do indivíduo, os dados coletados se enquadravam como dados biométricos (conforme detalhado no art. 2º, II, Decreto nº 10.046/2019) e, portanto, foi constatada a proteção especial às informações tratadas.

De fato, nos casos de tratamento de dados sensíveis, descabe a alegação de legítimo interesse. Ausente o consentimento pelos usuários bem como o enquadramento da situação em alguma das hipóteses do inciso II, do art. 11, da LGPD, afastou-se a legalidade da atividade realizada. Diferente seria o desfecho, ressaltou o tribunal, se o propósito de tal captação fosse voltado a melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem dentro de suas dependências.

Nos fundamentos expostos em trechos do relatório do acórdão, é interessante ressaltar a preocupação externalizada quanto ao uso da inteligência artificial:

> O que vemos é que a IA não está sendo desenvolvida com os interesses da coletividade em mente. Na verdade, está sendo desenvolvida para usos comerciais, para gerar lucro. Bom se nossos ideais ocidentais de democracia estivessem arraigados na IA do futuro. Mas não parece que isso que vai acontecer. [...]
> [...] podemos fornecer muitos dados a algoritmos de aprendizagem da máquina, pedir que eles o classifiquem e funciona muito bem. Mas não entendemos bem por que funciona. Há erros que nós não compreendemos. E o assustador é que, por ser aprendizagem de máquina, é uma caixa preta até para os programadores.
>
> A ré, na condição de concessionária de serviço público, incumbe arcar com o risco das atividades econômicas que explora, especialmente por envolver os direitos fundamentais à intimidade, à privacidade, à imagem e à honra dos usuários consumidores, o que não ocorreu, pois utilizada as imagens dos usuários coletadas durante a prestação do serviço público para fins comerciais.

No caso, foi relevante constatar que a exploração de dados biométricos dos consumidores para tratamento de dados operacionalizados pela IA suscitou questões a respeito

da natureza de receita acessória no contrato de concessão e prestação do serviço público. Nota-se que a irregularidade dessa atividade, diante das circunstâncias analisadas, também encontrou fundamento na violação da "adequação entre meios e fins" prevista no art. 5º, IV, do CDC, o qual impõe essa determinação como diretriz a ser observada pelos agentes públicos e prestadores de serviços públicos.

Cabe a reflexão sobre a utilização desse mesmo propósito comercial, com o emprego da Inteligência Artificial, em um shopping center, por exemplo. A conclusão seria a mesma? É difícil prever deslindes *a priori* sem a consideração das características circunstanciais que serão levadas em conta nas decisões pelos tribunais. A abordagem da Inteligência Artificial ainda é tímida na jurisprudência e, em geral, não aprofunda um acordo terminológico ou do conteúdo que esse termo abrange.

Quanto aos conceitos e instrumentos correlatos à inteligência artificial, demonstrada que a funcionalidade dessa tecnologia recai sobre a qualidade dos dados processados, bem como do algoritmo que utiliza, é importante esclarecer a compreensão de termos utilizados para descrever uma opacidade (ou caixa preta) da IA. Os temores suscitados por essas terminologias, ainda que tomadas como características intrínsecas dessa tecnologia, não retiram seu caráter instrumental. Em outras palavras, é preciso enfatizar que os resultados de seu processamento (*output*) atende aos interesses de quem a emprega (como a empresa concessionária). Esse fator é relevante para demonstrar que os resultados da IA dependem da curadoria do dataset utilizado como *input*. Em maior ou menor medida, essa incumbência recai sobre aquele que se beneficia de seu processamento.

12.2 Dataset e Big Data: opacidade da IA.

Big data é conceituado como um acervo de dados de grande volume, coletados com alta velocidade e em grande variedade de bases ou tipos de informações. Conhecidos pelos três V's (volume, velocidade e variedade), o *big data* pode ser definido como uma grande base de dados, gerados em tempo real, caracteristicamente desorganizados e formado pelos mais diversos tipos de formatos (como imagens, texto e números). Da mesma forma como na IA, o termo ainda é utilizado como guarda-chuva para descrever diversas tecnologias e perspectivas (KITCHIN; MCARDLE, 2016).

A busca por mitigar a subjetividade do conceito atraiu a tentativa de combinar os três V's com outros termos abstratos, tais como: versatilidade, volatilidade, virtuosidade, vitalidade, visionariedade, vigor, viabilidade, vitalidade e até mesmo virilidade (UPCHARD, 2013 e

JOSE, 2014). Ocorre que a utilização desses e de outros termos abstratos sugerem mais ao propósito de tentar a manter a tradição de utilizar a letra "V" para descrever o *big data* do que para atender ao objetivo de oferecer uma base epistemológica mais concreta para sua compreensão. Essa variedade de termos e nuances, ao invés de fornecer um padrão referencial, demonstra (assim como no campo da IA) uma ausência de consenso na comunidade científica, ainda mais quando se considera que tais atributos não estão presentes em todas as bases de dados (KITCHIN; MCARDLE, 2016).

Por esse motivo, a MIT sugere a consideração do *big data* para além do volume, velocidade e variedade e apresenta a proposta de uma perspectiva pela qual o *big data* representa uma *abordagem diferenciada* para obter achados e descobrir informações a partir de uma base de dados (BALAZKA; RODIGHIERO, 2020). É o que Mayer-Schönberger e Cukier (2013) descrevem como a mudança de uma abordagem casual na descoberta de conhecimento para uma que seja baseada na razão indutiva e em correlações. Essa perspectiva é interessante pois muda o foco de atenção às características intrínsecas do *Big data* e o direciona para as relações estabelecidas entre diversos temas que empregam esse instrumento. Assim, o *big data* é termo que mais caracteriza uma nova dinâmica de aquisição de conhecimento do que uma sintetização estanque e não suficiente formada por substantivos e adjetivos iniciados pela letra "v".

O que importa evidenciar é a correlação do *big data* com a Inteligência Artificial – bem como a ligação de ambos com o emprego de dados pessoais. O aprendizado da máquina é caracteristicamente referencial, ou seja, o processamento da IA depende de dados – usados como um conjunto de treinamento para ajustar parâmetros de algum modelo ou algoritmo. A esse conjunto de dados utilizados para fins de treinamento do algoritmo da IA, atribui-se a denominação *dataset*. O *dataset* "*é o principal insumo para a geração de um resultado satisfatório para a IA*. *É uma definição mais estrita de conjunto de dados, em formatos adequados para a realização dos treinamentos e testes de aferição de desempenho.*" (PEIXOTO, 2020, pág 26).

Para afastar dúvidas terminológicas, compreende-se que, se o treinamento ou a avaliação do desempenho da IA recai sobre um conjunto de dados essencialmente diversificados e volumosos para a realização de análises preditivas que excedem a capacidade de processamento de um software tradicional (como definir nichos de consumo, prevenir doenças e combater crimes), pode-se compreender que o *dataset* corresponde à utilização do *big data* como campo da análise de dados. Em outras palavras, se o *big data* for utilizado na fase de treinamento ou de avaliação, se caracterizará como o *dataset*. Por outro lado, superada

a fase de treinamento, o *big data* também abrange a base de dados utilizada como *input* do processamento da IA.

As conceituações apresentadas auxiliam na compreensão de que os receios ligados à IA em muito se relacionam com o conjunto de dados utilizados para o treinamento da máquina (*dataset*). Conforme sintetiza Fabiano Hartmann (2020, p. 26):

> normalmente associado ao conceito de opacidade algorítmica, os enviesamentos, na realidade, têm forte ligação com um dataset inadequado. [Isso porque] em um conjunto de dados, há tendências hábitos, representações das mais diversas atividades humanas e, entre elas, os desvios e preconceitos tão característicos do ser humano. Se não observados e metodologicamente cuidados, o conjunto de dados pode gerar enviesamentos que comprometem o uso de IA.

As preocupações que emergem da utilização do *big data* e da IA se relacionam com a crítica à vigilância (por instituições públicas e grandes corporações empresariais), e à violação de direitos correlatos à privacidade.[94] O maior risco genérico de um sistema de IA é produzir um resultado que apresente problemas marcados pela "*opacidade, arbitrariedade de critérios e conclusões, associada à discricionariedade, à discrepância com direitos fundamentais e outros princípios jurídicos*" o que conduz à associação do emprego desse sistema com o agravamento da desigualdade e imprevisibilidade do impacto de suas correlações e inferências automatizadas (PEIXOTO, 2020, pág. 28).

A denominada opacidade da IA gera receios pela falta de compreensão da forma de seu processamento, especialmente quanto ao *deep learning*, cuja dificuldade de explicar o processamento de camadas ocultas fomentou o uso do termo *black box*[95]. Aliado à ideia de autonomia da máquina, muitos medos suscitados quanto à utilização dessa tecnologia dizem respeito aos possíveis erros de julgamento por máquinas e o fomento à discriminação (também conhecidos como preconceitos ou *bias*).

---

[94] Fabiano Hartmann bem sintetiza que o maior risco genérico de sistema de IA "*é produzir um resultado que apresente problemas marcados pela opacidade, arbitrariedade de critérios e conclusões, associada à discricionariedade, à discrepância com direitos fundamentais e outros princípios jurídicos, associando o sistema ao aprofundamento da desigualdade e imprevisibilidade do impacto da sua aplicação de correlações e inferência automatizadas*." (PEIXOTO, 2020, p. 28).

[95] Conforme explica Adadi e Berrada cuida-se de termo amplo que faz referência aos mais diversos níveis de fechamento interno de um sistema, restringindo sua exposição de explicação sobre o design interno, estrutura e implementação ao usuário externo. *in* ADADI, Amina; MOHAMMED Berrada. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, vol. 6, 2018, pp. 52138–60. DOI.org (Crossref), https://doi.org/10.1109/ACCESS.2018.2870052.

Todos os conceitos apresentados, além da função de estabelecer um acordo terminológico, ressaltam que a utilização do termo "autonomia" para descrever a IA refere-se ao seu processamento, mas não a uma cognição plena ou similar à humana. Os avanços proporcionados pela inovação tecnológica demonstram que o melhor resultado da tecnologia recai sobre a clareza da definição e detalhamento da descrição da tarefa a ser desempenhada. A autonomia da máquina refere-se ao *meio* para alcançar esse *fim*. Trata-se de um instrumento que, se bem empregado, pode otimizar uma tarefa, desde que bem definida e "alimentada" com *inputs* de qualidade.

A autonomia não é emancipação ou soberania da máquina e, portanto, não retira o seu caráter instrumental. Conforme explica Fabiano Hartmann (2020, p. 29):

> O resultado consistente de um sistema de IA segue um fluxo de inserção de dados provenientes de um *dataset*, a internalização algorítmica e o resultado entregue. Embora exista a característica da caixa preta algorítmica, os riscos de desvios estão fortemente associados à deficiência na curadoria do *dataset* (alimentado com dados desviados e outras falhas) e pela falta de sistemas de controle e transparência no resultado, que possam detectar erros e apontar para soluções.

A partir da noção da dependência da IA sobre os dados é possível deduzir que há um grande controle pelos humanos sobre o seu funcionamento e, consequentemente, sobre os seus riscos.[96] Em outras palavras: "*se há uma diferença entre o comportamento artificial e o humano é que o resultado da atividade cognitiva artificial pode ser mais facilmente corrigido que os desvios e preconceitos do próprio ser humano*." (PEIXOTO, 2020, p. 28). Fabiano Hartmann prossegue no raciocínio, do qual extrai duas relevantes observações:

> 1º) todos os riscos são controláveis em um sistema de IA robusto (eticamente estruturado);
> 2º) a IA é conceitualmente a reprodução de padrões humanos e, portanto, o próprio comportamento humano também possui esses riscos.[97]

[96] Quando a máquina apresenta um resultado não desejado, por vezes preconceituoso, o receio sobre o black box é agravado. Ao que se denomina "machine bias", ou "algorithm bias", ou simplesmente "bias", cuida-se de termos utilizados para se referir às situações quando uma IA apresenta um resultado ou processamento enviesado ou preconceituoso. Como afirma Fernanda Lage, "uma das advertências feitas ao uso da IA é que esta, como se vale da análise de dados pretéritos, pode perpetuar ou mesmo acentuar os preconceitos que já existem na sociedade, em especial, o racismo que a estrutura." P. 117

[97] Em uma divisão de IA fraca, forte e superinteligência, estamos muito distantes de uma IA que se equipare à inteligência orgânica dos humanos (IA forte). Sequer podemos considerar, em um futuro próximo, a ideia de Ias que sobressaiam à capacidade cognitiva humana.

A denominada “opacidade” da IA não é, portanto, um desafio intransponível, mas é característica que revela que a atividade mais crítica no desenvolvimento dessa tecnologia é a “curadoria de datasets”. Essa curadoria, por sua vez, deve ser compreendida como o conhecimento prévio do processamento e das técnicas de IA para além de recortes conceituais ou técnicas de amostragem tradicionais. O propósito da curadoria é voltado à otimização de desempenho de forma conjugada ao objetivo de identificar parâmetros para evitar a perpetração de preconceitos, violações a direitos. Esse exercício é realizado para que o resultado final da IA (*outputs*) de fato reflita em benefícios, como o fortalecimento de valores democráticos e a garantia à proteção a direitos da personalidade – como a privacidade, imagem, integridade psicofísica, honra e dados pessoais (PEIXOTO, 2020).

Em outras palavras, a “autonomia” e a “inteligência” da IA se referem ao seu processamento, mas não retiram seu caráter eminentemente instrumental. Não se olvida, com essa afirmação, dos riscos e prejuízos que podem advir do seu emprego. O que se demonstra é que o efeito “*black box*” pode indicar a opacidade de seu processamento, mas não retira a responsabilidade pelos resultados danosos por quem as emprega. O dever de realizar uma “curadoria dos datasets” com atenção à qualidade dos dados de treinamento e de *input*, bem como dos algoritmos iniciais, é de incumbência de quem busca otimizar uma atividade com o emprego da IA.

12.3 Machine Learning (ML)

Machine learning (ML), ou aprendizado de máquina, é um conjunto métodos de instrução de IA que permite a detecção de padrões e a realização de previsões a partir da análise de dados históricos. (LAGE, 2021, pág. 70; PEIXOTO, 2020, pág. 18).

O aprendizado da máquina é referencial. Isso quer dizer que o processamento depende de dados, usados como um conjunto de treinamento (*dataset*), para ajustar os parâmetros de algum modelo ou algoritmo. A forma de aprendizado engloba diversas técnicas, as quais são divididas em supervisionado, não supervisionado e por reforço. No aprendizado supervisionado, o ser humano realiza uma rotulação prévia dos dados, ou seja, atribui uma categoria ou valor ao dado de treinamento. No aprendizado não supervisionado, a atividade de rotulagem é transferida para a própria máquinaNo aprendizado por reforço, a máquina é instruída com um mecanismo de recompensa para o alcance de um resultado informado como

correto e/ou uma desaprovação quando o resultado não for o almejado (HILDEBRANDT, 2022).

Os limites de usos do ML recaem sobre a criatividade de sua utilização. A infinidade de possíveis aplicações, por outro lado, não retira seu caráter instrumental. Os problemas que podem ser solucionados pelo ML são amplos, mas específicos, os quais podem ser exemplificados pelos seguintes propósitos:

1. **Segmentação de mercado**: também chamada de "*customer profiling*", é uma estratégia de marketing que envolve a divisão de um amplo mercado-alvo em subconjuntos de consumidores, empresas ou mesmo países que têm ou são catalogados como tendo prioridades e interesses comuns para, a partir da identificação desse padrão, implementar estratégias para alcançá-los com um produto ou serviço. As estratégias de segmentação de mercado normalmente são utilizadas para identificar e definir melhor o público-alvo e fornecer dados de suporte para tópicos de um plano de marketing, como posicionamento da empresa para atingir certo propósito ou objetivo. A partir do emprego do ML para esse propósito, as empresas podem desenvolver estratégias de diferenciação de produtos ou uma abordagem singular envolvendo produtos ou linhas de produtos específicos a depender da demanda específica e dos atributos do segmento alvo.

2. **Sistemas de recomendação**: sistemas é aqui referido como sinônimo de plataforma digital. Cuida-se de uma subclasse de sistema de filtragem de informações que busca prever a classificação ou preferência que um usuário daria a um item.

3. **Aprendizagem por regras de associação**: é método para descobrir correlações entre variáveis de grandes bancos de dados como, por exemplo, a regra {cebolas, batatas} => {hambúrguer}, muito comum em dados de vendas de supermercados para indicar que, se um cliente comprar cebolas e batatas ao mesmo tempo, é provável que também compre outros componentes ou complementos de um hambúrguer (como queijo e *ketchup*). Na detecção de ilícitos, essa técnica também é utilizada para detectar padrões associados a fraudes com cartões de crédito, como a análise e bloqueio de compras ou saques em frequência, volume ou valores destoantes dos padrões de consumo de um cliente.

4. ***Scoring***: o modelo de *scoring* (pontuação) é um tipo especial de modelo preditivo muito comum em Bancos de Dados de Proteção ao Crédito. Busca-se, com essa técnica, prever a inadimplência nos pagamentos de empréstimos, risco de acidente, perda de um cliente ou a probabilidade de adquirir um bem. Os modelos de pontuação normalmente usam uma escala logarítmica (a cada 50 pontos adicionais na pontuação reduz o risco de inadimplência em 50%, por exemplo) e são baseados em uma lógica de regressão e árvores de decisão ou uma combinação de vários algoritmos. A tecnologia de pontuação é normalmente aplicada a dados transacionais, às vezes em tempo real (como na detecção de fraude de cartão de crédito ou fraude de cliques).[98]

Em acréscimo aos exemplos citados, cabe abordar que uma das mais complexas atividades da política de vigilância sanitária no enfrentamento da pandemia da COVID-19 é o monitoramento e diagnóstico de novos casos de contaminação. Para desenvolver um sistema que age racionalmente a partir do aprendizado com os dados, é possível adotar uma abordagem de lógica formal – ou seja, de estatística descritiva – (*se uma pessoa tem febre e perda de olfato, é possível que esteja contaminada com o vírus*); uma abordagem bayesiana – espécie de estatística inferencial (*a Covid-19 causa febre em determinado percentual de pessoas; ajustada à probabilidade de ter ou não perdido o olfato e ao percentual de uma amostragem populacional ser contaminada com o vírus, é possível gerar um diagnóstico sobre o desenvolvimento da doença de algum paciente*); e uma abordagem com base no desenvolvimento de redes neurais artificiais, caracterizada por camadas inter-relacionadas que visam mimetizar um raciocínio complexo (*como realizar diagnósticos a partir da amostragem de imagens de raio-x de pacientes contaminados*) (SILVA, *et al*. 2020).

Conforme esclarece Fabiano Hartmann (2020, pág. 19), "*os problemas podem ser simples ou complexos, mas necessariamente específicos. A capacidade de aprender regras de um jogo de tabuleiro sofisticado (problema complexo) não torna a máquina 'inteligente' para sugerir diagnósticos médicos, por exemplo – são problemas específicos distintos*". Esses exemplos são utilizados para demonstrar que o bom desempenho do aprendizado do ML depende diretamente da qualidade e quantidade de dados, da identificação do meio de

[98] Esses e outros exemplos podem ser verificados em <https://www.datasciencecentral.com/profiles/blogs/top-20-uses-of-statistical-modeling Acesso em 03/04/2021>

aprendizagem e da definição do problema, o qual deve ser o mais específico possível. Reitera-se, nesse sentido, o elemento humano como fator essencial para descrever uma finalidade específica para garantir o funcionamento ou o atendimento de resultados pretendidos com o emprego de tecnologias da IA, como o *machine learning*.

12.4 Deep learning (DL) e redes neurais.

As redes neurais artificiais se situam dentro do propósito de reproduzir ações cognitivas humanas. Foram assim denominadas em razão dos arranjos de funcionamento buscarem ser elaborados de forma similar aos dos neurônios cerebrais orgânicos – o sistema nervoso humano é composto por neurônios que se comunicam por meio de sinapses e funcionam em redes de processamento de estímulos entre suas conexões estabelecidas por axônios e dendritos (PEIXOTO, 2020, pág. 20).

As redes neurais artificiais buscam mimetizar essa estrutura cerebral. São conectadas entre si por meio da atribuição de pesos (valores) e enfrentam a solução de um problema específico a partir de exemplos inseridos como treinamento. O termo aprendizado é utilizado para descrever o reconhecimento de padrões ou regras. A inferência de regras são extraídas a partir da análise dos exemplos e de acordo com os pesos delineados pelo algoritmo inicial. A entrada (*input*) "*é dimensionada por um peso que reflete na função e na saída* [*output*]. *A modulação dos pesos seguirá sendo feita pelos testes de resultados e o aprendizado é estimulado pelos dados de treinamento*." (PEIXOTO, 2020, pág. 20).

O *deep learning* é uma abordagem algorítmica baseada no noção de redes neurais. O conceito surgiu em 2006 com o objetivo de alcançar, por meio de modelos matemáticos, a capacidade de aprender com a experiência (tal como ocorreria com redes neurais biológicas). (LAGE, 2021). O DL é um subconjunto do ML. Para mitigar a confusão entre ambos, Fernanda Lage (2021, pág. 84) observa que:

> a distinção existente é que o começo do fluxo de trabalho de aprendizado de máquina se dá com os recursos (ou dados) relevantes sendo extraídos de forma manual das imagens ou do texto. E, esses recursos são usados para criar um modelo que categorize os objetos na imagem. Já no fluxo de trabalho de aprendizado profundo esses recursos relevantes são extraídos automaticamente das imagens. Além disso, o *deep learning* realiza o chamado 'aprendizado de ponta a ponta' – em que uma rede recebe dados brutos e uma tarefa a ser executada, como a da classificação, e aprende como fazer isso automaticamente.

Aprendizado de máquina, portanto, é um conjunto de algoritmos que "treinam" em um conjunto de dados para fazer previsões ou realizar ações com o propósito de otimizar algum sistema. O *deep learning,* subseção do ML, trata da hipótese de tornar os robôs inteligentes com técnicas diversas como as de reconhecimento facial ou de visão computacional para pilotar automaticamente um avião ou um carro. Quando os algoritmos são automatizados, como no caso de carros autônomos, fala-se em aprendizado profundo. Se os dados coletados vêm de sensores e são transmitidos pela Internet, fala-se em ML ou DL aplicado à IoT (GRANVILLE, 2016).

Muitos algoritmos de aprendizagem profunda (como *clustering*, reconhecimento de padrões, lances automáticos, mecanismo de recomendação e assim por diante), mesmo que apareçam em novos contextos como IoT ou comunicação de máquina para máquina, ainda dependem de técnicas relativamente antiquadas, como logística regressão, SVM, árvores de decisão, K-NN, *Bayes* ingênuo, modelagem Bayesiana, conjuntos, florestas aleatórias, processamento de sinal, filtragem, teoria dos gráficos, teoria dos jogos e muitos outros. Por isso se fala em IA específica, forte e superinteligência. Mesmo no contexto de resultados avançados com o emprego do *deep learning*, o modelo de inteligência artificial utilizado ainda se enquadra no momento inicial da capacidade das máquinas, denominado como IA fraca ou específica.

A inteligência artificial não é um fenômeno novo, mas os contínuos avanços tecnológicos permitem a visualização de uma nova dimensão da tecnologia. No entanto, ainda nos encontramos na primeira fase da IA, denominada fraca, estreita ou específica (*narrow*) por seu foco ser limitado à execução de tarefas específicas. Ainda que a quantidade de dados e os tipos de informações permitam processamentos de resultados sofisticados, a IA ainda é concebida para cuidar de problemas individualizados. (PEIXOTO, SILVA, 2019)

Uma evolução da capacidade da IA para um nível superior corresponderia à concepção da IA geral ou forte, a qual, de fato carregaria capacidades de adaptação e resposta semelhantes à humana. Há, ainda, uma fase sucessora à essa denominada como superinteligência, que se caracteriza pela sucessão do desenvolvimento da IA com uma capacidade que ultrapassa a inteligência humana (RUSSEL, 2022). É nesse ponto que a visão apocalíptica ou *hollywoodiana* da IA se situa. Esse momento é também apontado como o ponto da "singularidade" dos computadores.

A previsão de quando esse momento se consolidará ainda é difícil. Sequer passamos pela fase da IA forte ou generalizada. As máquinas já ultrapassam a capacidade humana em várias atividades, mas se mostram incapazes de realizar tarefas simples desempenhadas até por crianças de pouca idade (como desviar de objetos na locomoção). Ademais, não há uma escala

linear de inteligência para avaliar esse momento singular (PEIXOTO, SILVA, 2019). De toda forma, o momento contemporâneo apenas permite especular capacidades extraordinárias e perigosas. Atualmente, na consideração da IA fraca, específica ou estreita, há ainda mais argumento para adequar suas características às qualidades de um instrumento a ser utilizado para executar ou otimizar tarefas específicas. A autonomia dessa tecnologia se refere à sua capacidade de processamento e de adaptação para solução de problemas específicos e bem delineados, mas não para sua consideração como um ser de vontade autônoma.

De fato, as premissas que sustentam a consideração da IA como um instrumento podem se modificar. Em outras palavras, o emprego da IA no cenário atual de "IA fraca" não permite defender a existência de uma vontade autônoma a ser manifestada pela máquina. Eventuais danos causados que envolvam a sua utilização – com ou sem o emprego de dados pessoais – devem ser atribuídos a quem a emprega. Por outro lado, essa consideração não esgota o debate que envolve os impactos que as características autônomas que podem desafiar as atuais estruturas institucionais do ordenamento jurídico.

Em termos simplificados, não se insere no escopo deste trabalho exaurir a discussão sobre a atribuição ou não de personalidade às máquinas que funcionam com Inteligência Artificial ou da necessidade de se criar enquadramentos jurídicos diferenciados para se adequarem a situações determinadas.[99] O que se pode evidenciar é que, nos casos cotidianos suscitados pela jurisprudência colacionada, em que a Inteligência Artificial é de alguma forma suscitada como um problema ou aspecto relevante, não cabe a sua consideração como agente autônomo, mas sim, como instrumento a serviço de quem a emprega.

13. DA INSTRUMENTALIDADE DA IA: ESTUDOS DE CASOS

Os conceitos especificados, como Inteligência Artificial, Machine Learning e Deep Learning, são representativos de tecnologias cujos impactos para o Direito são grandes, mas de delineações ainda imprecisas. A percepção hollywoodiana de sua capacidade não auxilia na aplicação de institutos jurídicos. Serviços que utilizam inteligência artificial cotidianamente desafiam tanto a criatividade como a ciência jurídica. Questões sobre a responsabilidade por danos causados por decisões automatizadas, robôs inteligentes, carros autônomos e outros serviços que fazem uso da inteligência artificial são apenas alguns temas que instigam o

[99] Trata-se de temática extremamente interessante e que requer estudo detalhado próprio. O aprofundamento dessas questões podem ser vislumbrados nos trabalhos de Fernanda Lage (2021 e 2023) bem como por Paweł Kiężak e Sylwia Wojtcazk (2023).

intérprete a questionar qual é o quadro normativo que deve incidir para que seja possível promover a efetiva reparação de uma potencial vítima de danos causados por uma situação que envolva o emprego de Inteligência Artificial.

Sistemas tecnológicos com ações e respostas cada vez mais autônomas são constantemente inaugurados e rapidamente incorporados no convívio social. Uma novidade tecnológica, no entanto, não implica na necessidade automática de uma inovação legal que a tutele. Em primeiro lugar, cabe notar que a informatização ou automação de um serviço não significa que houve o emprego de uma tecnologia autônoma. Em segundo lugar, ainda que efetivamente utilizada, não se pode abandonar a noção de que aplicações de tecnologias como a IA não abandonam o seu caráter instrumental. Por mais que se apresentem de forma cada vez mais avançadas, inteligência artificial e aplicação de tecnologias autônomas se aproximam muito mais da noção jurídica de um *instrumento* do que de um *sujeito* autônomo. Assim como um carro, uma faca ou um inseticida, a inteligência artificial pode causar graves danos, mas não deixa de ser um instrumento cujos limites, aplicações e consequências dependem de como (e por quem) será utilizada.

Ocorre que esse entendimento ainda não é pacificado e não foi replicado em caso concreto enfrentado pelo Tribunal de Justiça do Distrito Federal e Territórios (TJDFT).[100] Em 2019, o TJDFT não reconheceu o cabimento de repetição do indébito (art. 42, parágrafo único, do CDC) em caso em envolveu cobrança indevida por uma instituição bancária. O entendimento do tribunal recaiu no argumento de que a utilização da inteligência artificial, que marca a 4ª Revolução Industrial, exige a revisão de conceitos jurídicos tradicionais uma vez que estes seriam condizentes com o cenário do vendedor de balcão, que utilizada uma caderneta de apontamentos pessoais dos seus fregueses, em uma forma de operacionalização contemporânea à 1ª Revolução Industrial, na era da máquina movida a vapor.

Na ocasião, tomou-se como pressuposto para aplicar a sanção de repetição do indébito a comprovação do elemento volitivo do fornecedor em auferir vantagem pela cobrança indevida. O Relator designado sustentou que "*a má-fé, no caso, é a atitude de quem não disfarça a intenção de enriquecimento ilícito ao cobrar o que já foi pago, ao cobrar o que não era devido, sem qualquer erro justificável, e ao de receber o que foi cobrado*." Suscitou, ademais, que "*as instituições financeiras operam com inteligência artificial, a chamada 4ª*

[100] A seleção da jurisprudência indicada foi pautada pela busca do emprego da expressão "inteligência artificial" como elemento determinante na fundamentação de um julgado. Representativo dessa hipótese foi encontrada no âmbito do TJDFT (como no caso indicado). Demais casos escolhidos tangenciaram o tema, como no caso do TJ-SP (também mencionado no presente trabalho). A utilização das características da IA como elemento relevante da fundamentação de uma decisão ainda é incipiente na formação da jurisprudência brasileira.

revolução industrial, que é caracterizada pela fusão de tecnologias que estão pondo em xeque as esferas física, digital e biológica." Por esse raciocínio, concluiu que não haveria "*como se imputar má-fé às cobranças feitas por sistemas, por robôs eletrônicos*." Pela representatividade do tema, cabe citar o inteiro teor da ementa do acórdão:

> 1. "A aplicação do art. 42, parágrafo único, do Código de Defesa do Consumidor somente é justificável quando ficarem configuradas tanto a cobrança indevida quanto a má-fé do credor fornecedor do serviço. Precedentes do STJ" (AgRg no REsp 1200821/RJ, Relator Ministro João Otávio de Noronha, Terceira Turma, julgado em 10/02/2015, DJe 13/02/2015.).
> 2. Para que haja a devolução em dobro do indébito, é necessária a comprovação de **três requisitos**, conforme o parágrafo único do artigo 42 do CDC, a saber: 1) que a cobrança realizada tenha sido indevida; 2) que haja o pagamento indevido pelo consumidor; e 3) que haja engano injustificável ou má-fé. Mutatis mutandis, a mesma exigência impõe-se para a repetição ou para a indenização prevista no art. 940 do Código Civil.
> 3. A **má-fé é inerente à atitude humana de quem age com a intenção deliberada de enriquecimento ilícito** ao cobrar o que já foi pago, ao receber o que foi cobrado e ao cobrar o que não era devido, sem qualquer engano ou erro justificável.
> 4. Para a devolução em dobro, não basta a cobrança indevida. **As instituições financeiras,** conceito que compreende bancos e, também, companhias que administram operações de cartões de crédito, conhecidas como bandeiras, **operam com inteligência artificial, a chamada 4ª Revolução Industrial, que é caracterizada pela fusão de tecnologias que puseram em xeque as esferas física, digital e biológica. Não há como se imputar má-fé às cobranças feitas por sistemas computacionais, por robôs eletrônicos**.
> 5. Há que se repensar conceitos que não poderão receber dos juristas as antigas soluções impostas pelo Direito Romano ao vendedor de balcão, com caderneta de apontamentos pessoais dos seus fregueses, contemporânea da 1ª Revolução Industrial, a era da máquina movida a vapor.
> 6. **As inconsistências do emprego de inteligência artificial não podem ser punidas com o rótulo da má-fé, atributo exclusivamente humano, ínsito a quem anota, naquela mencionada caderneta, uma compra que não foi feita ou uma dívida que já foi paga, para dobrar, fraudulentamente, o lucro no fim do mês.**
> 7. Sem os requisitos legais, a devolução do indébito deve ocorrer de forma simples.
> (Acórdão 1157854, 07150148120188070001, Relator: Eustáquio de Castro, Relator Designado: Diaulas Costa Ribeiro 8ª Turma Cível, data de julgamento: 14/3/2019, publicado no DJE: 6/5/2019.) - grifos da autora.

Há três apontamentos que devem ser abordados para a análise desse julgado. Em primeiro lugar, é preciso analisar os requisitos necessários para a devolução em dobro (art. 42, parágrafo único, do CDC) nos termos do posicionamento do STJ indicado no acórdão (AgRg no REsp 1200821/RJ, julgado em 10/02/2015) em face da tese posteriormente fixada pela Corte

Superior (Tema 929), publicada em 30 de março de 2021. Nota-se que a má-fé é exigida como pressuposto no primeiro posicionamento, mas é elemento dispensável no segundo.

Como segundo apontamento, diferente do que afirmado no tópico 2 da ementa do acórdão, consoante os termos do posicionamento adotado pelo STJ no Tema 929, cabe esclarecer que a repetição do indébito nos moldes do art. 42, parágrafo único, do CDC, não se confunde com a disciplina do art. 940 do Código Civil. Cabe especificar que esses dispositivos possuem pressupostos de aplicação diferentes e incidem em hipóteses circunstanciais distintas. Ocorre que a influência do direito civil provocou um mosaico de posições nem sempre convergentes a respeito da relevância ou não do elemento volitivo da conduta (dolo ou culpa) para aplicação dessa sanção civil. Cabe pontuar que as diferenças de pressupostos e de circunstâncias distintas não afasta a incidência subsidiária do Código Civil nas relações de consumo.

Em terceiro lugar, uma vez constatado que o entendimento proferido no acórdão pelo TJDFT, em 2019, destoa da tese fixada pelo STJ (Tema 929), e 2021, cabe analisar os efeitos da decisão pela Corte Superior sobre a análise desse caso bem como sobre situações supervenientes. O Superior Tribunal de Justiça determinou a adoção da concepção objetiva do abuso de direito adotada no art. 42, parágrafo único do CDC (com dispensa, portanto, da comprovação de elemento volitivo na cobrança indevida). Ocorre que os efeitos dessa decisão foram modulados para que somente fossem aplicados às cobranças realizadas após a publicação do acórdão paradigma (o que ocorreu em 30 de março de 2021, após, portanto, a decisão proferida pelo tribunal de justiça do Distrito Federal). Esses fatores devem ser levados em consideração, especialmente para apontar os motivos e justificativas para resultados tão distintos.

13.1 Premissa para o caso prático: Tema 929/STJ e aplicação da sanção civil de repetição do indébito (art. 42, parágrafo único, do CDC, e art. 940, do CC).

A devolução em dobro – nos moldes do art. 42, parágrafo único, do CDC, e do art. 940, do CC – constitui sanção civil específica em favor do consumidor ou do particular. A devolução do valor pago de forma indevida, denominada como devolução simples, decorre de outra lógica, pautada pela vedação do enriquecimento ilícito prevista no art. 884, do Código Civil, o qual estipula que "*aquele que, sem justa causa, se enriquecer à custa de outrem, será obrigado a restituir o indevidamente auferido, feita a atualização dos valores monetário*s". A devolução

simples, portanto, não constitui sanção civil e se justifica pelo reconhecimento de obrigação de restituir o que foi indevidamente obtido (ao que se denomina como locupletamento).

Nas demandas privadas, a repetição do indébito prevista no art. 940, do CC, exige que a cobrança indevida seja realizada no meio judicial: "*aquele que demandar por dívida já paga, no todo ou em parte, sem ressalvar as quantias recebidas ou pedir mais do que for devido, ficará obrigado a pagar ao devedor, no primeiro caso, o dobro do que houver cobrado e, no segundo, o equivalente do que dele exigir, salvo se houver prescrição*.". A doutrina exige a demonstração de má-fé do credor (ROSENVALD, NETTO, 2022). Portanto, são requisitos para a devolução em dobro, exigidos esse dispositivo do Código Civil, a cobrança indevida por meio judicial e a demonstração de má-fé do credor.

A descrição dos pressupostos do art. 42, do CDC, sofreu oscilações no âmbito do STJ e ainda enfrenta posicionamentos distintos na doutrina – possivelmente em decorrência de uma indevida influência do direito civil (BESSA, 2022). Fato é que, ao menos desde o julgamento do Tema 929/STJ[101], foi estabelecida a tese no sentido de que "*a repetição em dobro, prevista no parágrafo único do art. 42, do CDC, é cabível quando a cobrança indevida consubstanciar conduta contrária à boa-fé objetiva, ou seja, deve ocorrer independentemente da natureza do elemento volitivo*".

Afasta-se, portanto, a necessidade da má-fé como pressuposto dessa sanção civil no âmbito da legislação de consumo. A devolução em dobro, nos termos do art. 42, parágrafo único, do CDC, dispensa a necessidade de demonstrar o elemento volitivo (má-fé) e estabelece que a cobrança indevida pode ocorrer independentemente do meio (ou seja, não exige que a cobrança ocorra em meio judicial, admitindo-se a circunstância da dívida ser cobrada indevidamente pela via administrativa).

O parágrafo único do art. 42, do CDC, estabelece que "*o consumidor cobrado em quantia indevida tem direito à repetição do indébito, por valor igual ao dobro do que pagou em excesso, acrescido de correção monetária e juros legais, salvo hipótese de engano justificável*." A expressão "salvo engano justificável" não se confunde com a exigência de demonstração de um elemento volitivo do fornecedor que realiza uma cobrança indevida. Trata-se de um parâmetro excludente da repetição dobrada que admite que o fornecedor comprove a boa-fé objetiva que justifique o engano da cobrança. Trata-se de um ônus da defesa (e não do autor).

---

[101] Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&cod_tema_inicial=929&cod_tema_final=929 Acesso em 30 de maio de 2023.

Os requisitos legais para a repetição em dobro na relação de consumo são a cobrança indevida, o pagamento em excesso e a inexistência de engano justificável do fornecedor. Grande diferença perante a disciplina do direito civil, portanto, se refere à dispensa do aspecto circunstancial de que a cobrança indevida ocorra em meio judicial (exigida pelo art. 940, do CC, mas não pelo CDC) bem como sobre a dispensa da comprovação de elemento volitivo (culpa ou dolo) para seu reconhecimento.

Nota-se que a má-fé, como requisito para a devolução em dobro pelo art. 940 (CC), é elemento constitutivo de direito, de modo que deve ser alegada e demonstrada pelo particular que visa a aplicação dessa sanção civil. De modo diverso, além de não exigir a má-fé, a disciplina do parágrafo único do art. 42, do CDC, não demanda, do consumidor, prova da injustificabilidade da cobrança realizada. O engano justificável, reitere-se, é matéria de defesa, de incumbência do fornecedor que busca se evadir da aplicação da sanção cível.

Como outra diferença, cabe notar que, pelo regime do Código Civil (art. 42, parágrafo único), além da comprovação da má-fé, basta que ocorra a cobrança *judicial* indevida da dívida. Por outro lado, o CDC (art. 42, parágrafo único) exige que o consumidor realize efetivamente o pagamento dessa dívida, cobrada de forma indevida (mas independentemente se pela via judicial ou extrajudicial).

Nota-se que o entendimento fixado no Acórdão 1157854 (TJDFT, 2019) destoa do firmado no âmbito do Tema 929 (STJ, 2021), tanto quanto aos requisitos que precisam ser comprovados para que haja a possibilidade de imputar a devolução em dobro do indébito, quanto pela equiparação, *mutatis mutandis*, das exigências impostas para a repetição prevista no art. 940, do Código Civil. Os dispositivos (art. 42, parágrafo único, do CDC, e art. 940, do CC) apresentam pressupostos de aplicações diferentes e hipóteses de incidência distintas.

Por outro lado, já reconheceu o STJ a possibilidade de aplicar o art. 940, do CC, em relação de consumo na qual, embora não preenchidos os requisitos do art. 42, parágrafo único, do CDC (uma vez ausente a efetivação do pagamento pelo consumidor, no caso concreto), restava comprovada a má-fé do demandante que realizou cobrança em meio judicial:

> RELAÇÃO DE CONSUMO. COBRANÇA JUDICIAL. INDEVIDA. DÍVIDA PAGA. INSTITUIÇÃO BANCÁRIA. MÁ-FÉ. DEMONSTRAÇÃO. ART. 42 DO CÓDIGO DE DEFESA DO CONSUMIDOR. INAPLICABILIDADE. ARTIGO 940 DO CÓDIGO CIVIL. REPETIÇÃO DE INDÉBITO EM DOBRO. PRESSUPOSTOS PREENCHIDOS. COEXISTÊNCIA DE NORMAS. CONVERGÊNCIA. MANDAMENTOS CONSTITUCIONAIS.
> [...]

> 4. Os artigos 940 do Código Civil e 42, parágrafo único, do Código de Defesa do Consumidor possuem pressupostos de aplicação diferentes e incidem em hipóteses distintas.
> 5. A aplicação da pena prevista no parágrafo único do art. 42 do CDC apenas é possível diante da presença de engano justificável do credor em proceder com a cobrança, da cobrança extrajudicial de dívida de consumo e de pagamento de quantia indevida pelo consumidor.
> 6. O artigo 940 do CC somente pode ser aplicado quando a cobrança se dá por meio judicial e fica comprovada a má-fé do demandante, independentemente de prova do prejuízo.
> 7. **No caso, embora não estejam preenchidos os requisitos para a aplicação do art. 42, parágrafo único, do CDC**, **visto que a cobrança não ensejou novo pagamento da dívida, todos os pressupostos para a aplicação do art. 940 do CC estão presentes.**
> 8. Mesmo diante de uma relação de consumo, se inexistentes os pressupostos de aplicação do art. 42, parágrafo único, do CDC, deve ser aplicado o sistema geral do Código Civil, no que couber.
> 9. **O art. 940 do CC é norma complementar ao art. 42, parágrafo único, do CDC e, no caso, sua aplicação está alinhada ao cumprimento do mandamento constitucional de proteção do consumidor**.
> (STJ - REsp: 1645589 MS 2016/0186599-2, Relator: Ministro RICARDO VILLAS BÔAS CUEVA, Data de Julgamento: 04/02/2020, T3 - TERCEIRA TURMA, Data de Publicação: DJe 06/02/2020) – grifos da autora.

Cabe notar que o STJ manifestou preocupação quanto à superação da compreensão previamente estabelecida pela jurisprudência da Segunda Seção (a qual exigia o critério volitivo doloso da cobrança indevida) – composta pela Terceira e Quarta Turmas do STJ. Nesse sentido, a Corte Superior optou por modular os efeitos de sua decisão para que o entendimento fixado fosse aplicado aos indébitos de natureza contratual não pública cobrados após a data da publicação do acórdão (em 21 de março de 2021).

Nesses termos, para cobranças posteriores à data de publicação do Tema 929 (21 de março de 2021), restou superada a decisão de que a aplicação do art. 42, parágrafo único, do CDC, somente seria justificável quando configuradas tanto a cobrança indevida quanto a má-fé do credor fornecedor do serviço – conforme precedente adotado pelo TJDFT, em 2019, externalizado pela Terceira Turma do STJ, no AgRg no REsp 1200821/RJ julgado em 10/02/2015.

13.2 Considerações sobre o caso prático: clonagem e cartão e cobrança indevida.

No caso enfrentado pelo Tribunal de Justiça do Distrito Federal e Territórios, em 2019, o cartão de um consumidor foi clonado e, mesmo com a rápida efetivação para o bloqueio do cartão e comunicação imediata da fraude à instituição financeira, o banco insistiu em incluir valores de operações fraudulentas sucessivas na fatura da vítima, a qual optou por realizar o

pagamento do débito e pleitear judicialmente a repetição de tais valores. O TJDFT reformou a sentença de piso, favorável ao consumidor, que reconheceu o preenchimento dos requisitos necessários para configurar o direito à repetição do indébito.

No acórdão, o Tribunal reconheceu o pagamento do débito cobrado indevidamente o que, segundo sua visão, motivava a devolução simples, mas não a má-fé necessária para determinar a devolução em dobro pela instituição bancária. O argumento utilizado suscitou a impossibilidade de imputar má-fé às cobranças feitas por sistemas computacionais, por robôs eletrônicos, tendo em vista que a má-fé é atributo exclusivo do ser humano. O Relator Designado sustentou que:

> Não houve má-fé nem engano injustificável que autorizasse a restituição em dobro. [...]
> Não basta, data vênia, a cobrança indevida. Inclusive porque todos esses bancos e as companhias que administram as operações com cartões de crédito, conhecidas como bandeiras, operam com inteligência artificial, a chamada 4ª revolução industrial, que é caracterizada pela fusão de tecnologias que estão pondo em xeque as esferas física, digital e biológica.
> **Não há como se imputar má-fé às cobranças feitas por sistemas, por robôs eletrônicos**.
> Há que se repensar, inclusive, conceitos que não poderão receber dos juristas as antigas soluções imposta ao vendedor de balcão, com caderneta de apontamentos pessoais dos seus fregueses, no tempo da primeira revolução industrial (máquina a vapor).
> Apenas para registro, a segunda revolução industrial foi caracterizada pelo uso da eletricidade e a terceira pelo uso das tecnologias eletrônicas. **As inconsistências da inteligência artificial não podem ser punidas como quem anota, naquela mesma caderneta, uma compra que não foi feita, para dobrar o seu lucro no final do mês, ao cobrar a conta.**
> O Banco do Brasil é um gigante do sistema financeiro nacional e não se pode presumir que tenha cobrado, de propósito, escondendo-se na surpresa ao devedor, para obter lucro. Não se pode avançar para a conclusão de que houve má-fé. **A má-fé deve ser equivalente ao dolus malus,e não se contenta com o mero erro de fato.** Não se pode confundir erro de fato com má-fé.

No mérito, a instituição financeira baseou sua defesa com fundamento na obrigação do correntista de usar e guardar o cartão, a senha e o código de acesso. Desse modo, sustentou inexistir fraude, pois ausente comprovação de ato ou de omissão no sentido de vinculá-la ao evento narrado. Ocorre que, como reconhecido pelo relator inicial (cujo voto restou vencido), a situação dos autos é distinta justamente por não ter sido sequer comprovado o meio utilizado para realização da compra realizada por terceiros que ocorreu, inclusive, no exterior. Situação diversa se daria caso se tratasse de saques em caixa eletrônico, operação na qual a senha é imprescindível.

Ainda que não suscitada como defesa pela parte requerida, o acórdão baseou-se na consideração de que a inteligência artificial empregada pelo banco possui natureza de serviço com atuação autônoma – e não instrumental – na formação e execução do contrato de prestação de serviços ao consumidor. O argumento, no entanto, não é consistente.

De fato, o emprego da inteligência artificial é condizente com muitas atividades bancárias, pois é ideal para atividades repetitivas, com propósitos específicos, que exijam alto grau de atenção e memória – como no caso de cobranças e formação de faturas de clientes. No entanto, apesar de ter sido desenvolvida com o objetivo de mimetizar a inteligência humana (fato que contribui para a descontextualização conceitual da tecnologia) a IA mais se aproxima da capacidade de identificar padrões do que do desenvolvimento de sensibilidade, emoções e raciocínios complexos que de fato se aproximam da característica de autonomia humana.

Ademais, cabe considerar que a formação de faturas de cada cliente é atividade que mais representa uma *informatização* de um serviço do que uma tomada de decisão autônoma. A tecnologia empregada confere celeridade pela automatização de um serviço, mas não muda a titularidade de quem a utiliza. A cobrança indevida é instrumentalizada pela tecnologia, mas não deixa de compor um serviço prestado pela instituição financeira.

Nota-se que o TJDFT considerou, à época, o precedente fixado pelo STJ que restou superado, pelo Tema 929, em 2021.

Sanção civil do art. 42, parágrafo único, do CDC: requisitos para repetição do indébito.	
Antes da publicação da decisão no EResp 1.4.13.542/RS (Tema 929)	**Após** publicação da decisão do EResp 1.4.13.542/RS (Tema 929)
1) cobrança indevida;	1) cobrança indevida;
2) Efetivo pagamento indevido pelo consumidor;	2) Efetivo pagamento indevido pelo consumidor;
3) engano injustificável ou má-fé.	3) Engano injustificável (matéria de defesa) – independente do elemento volitivo.

Condizente com o atual posicionamento do STJ, condizente seria o posicionamento adotado pelo juiz, que sentenciou em 1º grau, e o adotado no voto vencido do relator inicial do caso em análise. Como bem ponderou, sem apelo ao elemento volitivo e pelo prisma da boa-fé objetiva, não haveria erro justificável no caso analisado uma vez que, com o bloqueio do cartão pelo consumidor, oportunidade em que não reconheceu a realização de compra fraudulenta, não

haveria justificativa para o banco insistir em incluir, na fatura do novo cartão, a quantia regularmente contestada.

A importância que pode ser extraída desse caso, além da representativa mudança de entendimento pelo STJ, é que não haveria motivo para acrescentar complexidade ao caso sob o argumento de que o dano envoldou o emprego de inteligência artificial.

Conceitos e capacidades de tecnologias são constantemente renovados e difíceis de delinear, mas nem sempre representam um desafio jurídico, especialmente quanto à identificação de autores de eventual dano decorrente de sua utilização. A tecnologia é um instrumento e (*ao menos, ainda,*) não um sujeito de direito autônomo. A maior dificuldade pode recair, em realidade, sobre qual o quadro normativo deve incidir caso a caso. No exemplo apresentado, verifica-se tanto a formação de uma relação de consumo entre a instituição financeira e seu cliente quanto a utilização de dados pessoais do consumidor. A incidência concomitante de diversos diplomas legais, como o CDC e a LGPD, representa uma complexidade ao intérprete, mas não uma impossibilidade de tutela de danos causados por tecnologias pelo Poder Judiciário.

A tutela de dados pessoais disciplina um regime de responsabilidade civil próprio, mas não exclusivo (art. 45, da LGPD). Se considerada, a incidência da LGPD não se daria de forma subsidiária, com prevalência ao CDC, mas de modo complementar – em uma "simbiose protetiva", conforme suscita Cláudia Lima Marques e Bruno Miragem (2023). Como relevante para o caso, a tutela da expectativa de segurança do titular (art. 44, parágrafo único) também poderia ser utilizada para impor o dever de reparar os danos sofridos pelo titular. Não há, por outro lado, a imposição de sanção civil similar à prevista no art. 42, parágrafo único do CDC.

A relevância do caso recai mais na análise da sanção civil do que no quadro normativo de responsabilidade civil disciplinado por ambos os quadros normativos. A repetição do indébito não seria afastada por eventual aplicação da LGPD.

Cabe ressalvar que o complexo de normas legais incidentes sobre um mesmo caso não conduz, contudo, a uma tutela integral de todo e qualquer dano sofrido em meio tecnológico. Um posicionamento nesse sentido vai de encontro aos próprios pressupostos na LGPD que visa amparar o titular de dados pessoais que seja vítima de um tratamento irregular, mas, também, fomentar o desenvolvimento tecnológico. A responsabilidade civil pressupõe o preenchimento de requisitos expressamente previsto na norma. Não pode se transformar em um meio para reprimir o emprego de tecnologias ou formar uma barreira à inovação.

14. RESPONSABILIDADE CIVIL POR DANOS CAUSADOS PELA IA.

Para o Código de Defesa do Consumidor, o produto ou serviço possui qualidade quando funciona adequadamente – ou seja, atende à finalidade que lhe é inerente – e, ao mesmo tempo, não oferece risco à saúde e segurança do consumidor. Os pressupostos que ensejam o dever de indenizar são: 1) produto ou serviço com vício e/ou defeito; 2) dano moral e/ou material; 3) relação de causalidade. A culpa não é elemento necessário para a caracterização da responsabilidade do fornecedor, salvo quanto aos profissionais liberais, cuja responsabilidade pessoal é apurada mediante a verificação de culpa, conforme exigência constante do art. 14, §º, do CDC (BENJAMIN, 2020).

Para a Lei Geral de Proteção de Dados Pessoais, o tratamento será regular quando atender à legislação *lato sensu* bem como à legítima expectativa de segurança do titular. Os elementos que ensejam o dever de indenizar são: 1) violação à legislação (*lato sensu*) e/ou à legítima expectativa de segurança do titular; 2) dano moral e/ou material; 3) relação de causalidade.

É inerente à Sociedade da Informação (LASTRES, 1999) a realização de atividades tratamentos de dados pessoais voltadas para a efetivação de fins comerciais que envolvem o consumidor ou têm a pretensão de estabelecer uma relação de consumo. O art. 45 e 64 da LGPD, bem como o art. 7º, *caput*, do CDC, amparam a aplicação concomitante de ambos os regimes dos respectivos diplomas normativos, em uma relação de complementariedade e não de revogação ou de subsidiariedade.

A incorporação de tecnologias cada vez mais avançadas nas atividades e relações cotidianas ressalta o benefício dessa aplicação sinérgica de diplomas normativos, em especial diante de potenciais danos causados pela Inteligência Artificial. O caráter instrumental dessa tecnologia permite apontar o responsável por eventual dever de indenizar nos termos descritos pelo CDC e/ou LGPD. É possível afirmar, com uma relativa certeza, que os danos porventura causados com o emprego da Inteligência Artificial no âmbito comercial potencialmente envolverão uma relação de consumo e/ou a utilização de dados pessoais de modo a sujeitar o caso à disciplina de um ou de ambos os diplomas.

Não se pode olvidar, por outro lado, que o uso da Inteligência Artificial possa causar danos em circunstâncias distintas das delineadas, ou seja, que não atraiam a incidência do CDC ou da LGPD. Na ação coletiva promovida, em 2015, pelo promotor Marc Stanley contra a empresa Toyota Motor Corporation, em 2015, buscou-se demonstrar preocupação com ameaças à segurança e privacidade dos consumidores tendo em vista uma falha de segurança que

permitia que sistemas de inteligência artificial dos veículos fossem invadidos por *hackers* de modo a possibilitar a aceleração, mobilização dos freios e controle da direção dos automóveis à distância. Nenhum veículo havia sido efetivamente *hackeado*. Diante desse fato, por considerar ausente a comprovação de defeito ou dano efetivo, o magistrado Willian Orrick reconheceu a improcedência da ação (*Cahen et al. v. Toyota Motor Corporation et al., Case* nº. 3:15-cv-01104, in the U.S. *District Court for the Northern District of California*).

Para a hipótese em que mesmo caso fosse submetido à análise pelo ordenamento jurídico brasileiro, seria preciso examinar se os dados utilizados para realizar o acesso à distância do veículo seriam passíveis ou não de identificar os condutores para se enquadrar como dado pessoal. Em caso positivo, seria possível verificar se houve violação da legislação por omissão a alguma medida imposta pela legislação. Por outro lado, a constatação da violação a uma legítima expectativa do titular de dados seria uma tarefa difícil. Isso porque as circunstâncias do caso envolvem a consideração da exposição do titular em risco como a efetivação de dano ao titular, uma vez que não houve um efetivo ataque hacker ou danos concretos no caso aventado.

Pelo mesmo motivo, a ausência de dano efetivo (não potencial) afastaria a incidência da disciplina do fato do produto uma vez que a responsabilidade civil decorrente do disposto no art. 12, do CDC, recai exclusivamente aos casos em que o evento danoso (acidente de consumo) tenha ocorrido. Conforme alerta Leonardo Bessa (2022, pág. 125), ainda que diante de uma alta potencialidade lesiva à integridade do consumidor e de seu patrimônio, não há cabimento que habilite a invocação desse dispositivo. A resolução do caso, por outro lado, poderia recair na disciplina constante do art. 18, do CDC (vício do produto), ou seja, o argumento recairia na afetação da funcionalidade ou utilidade do veículo. Afastada a hipótese de mau funcionamento do veículo, há ainda, o respaldo do art. 6º, VI, do CDC, que estabelece uma cláusula geral de responsabilidade civil no âmbito da legislação de consumo. O desafio para este caso também recai na ponderação quanto à possibilidade de danos potenciais consubstanciarem elemento suficiente para imputação de responsabilidade ao fornecedor.

Ainda que afastada a incidência da disciplina de responsabilidade civil pela LGPD ou pelo CDC, há a possibilidade de aplicação das cláusulas gerais de responsabilidade civil pelo Código Civil, consubstanciadas nas disposições do artigo 927 c/c os artigos 186 e 187. Eventual dificuldade, para esse caso, envolve a já existente divergência doutrinária do que se conceitua como ato ilícito. Essa questão é superável, conforme argumentação apresentada neste trabalho.

O que importa destacar, pela presente exposição, é que o exemplo apresentado representa um dos maiores problemas de importar dificuldades e soluções jurídicas experimentadas por ordenamentos estrangeiros, em especial, o da *Common Law* americana. A lógica da responsabilidade civil pautada pelo risco ou por cláusulas gerais do *Civil Law* aponta soluções que não encontram eco no contexto americano. Não há um sistema de responsabilidade civil extracontratual objetiva nos Estados Unidos como o previsto no Brasil. As denominadas "*torts*" são utilizadas para descrever delitos específicos e, pela norma consuetudinária, demandam um procedimento rigoroso com vários obstáculos jurisprudenciais a serem superados para então estabelecer uma obrigação de reparar àquele eventualmente considerado responsável (AVGOUTI, 2015). A lógica definida no ordenamento jurídico brasileiro é outra, pautada por complexidades próprias que muitas vezes não se confundem com os problemas enfrentados no exterior. Não há justificativas para importação dessas dificuldades

A inteligência artificial não promove óbices de aplicação normativa no Brasil nos mesmos moldes como no âmbito do direito consuetudinário. A complexidade de questões pode envolver o detalhamento do quadro normativo, mas não implica necessariamente no reconhecimento de um vácuo legislativo.

Aliás, o "fetichismo da lei", compreendido como uma miragem da codificação pautada pela noção de completude de "uma regra para cada caso", reflete uma lógica do individualismo oitocentista que foi superada em um processo que se iniciou no século XX, na Europa, e na década de 1930, no Brasil. O processo de descodificação do direito civil promoveu o deslocamento do centro de gravidade do direito privado no Código Civil (monossistema) para abrir espaço à constituição de direitos especiais anunciado uma era dos estatutos. Mesmo essa transformação não foi suficiente para fazer frente à evolução do cenário econômico e social que, em uma realidade cada vez mais complexa, estimulou uma proliferação desmesurada da produção legislativa para atender ao anseio de regulamentação de cada aspecto da vida social (TEPEDINO, 1998).

A "era dos estatutos" substitui um problema (o monossistema) por outro (polissistema) justamente por seguir a mesma lógica da completude normativa. As transformações sociais, estimuladas pelas inovações tecnológicas, demonstrou ser infrutífera a tentativa de tipificar a totalidade das situações jurídicas que, assim como os bens jurídicos objeto do direito, multiplicam-se a todo momento. Cabe notar que essa observação foi realizada por Gustavo Tepedino em 1998. Nota-se que a preocupação com a regulação normativa da tecnologia não é inaugurada com o crescente emprego da inteligência artificial. Antecede a entrada do novo milênio.

O cenário de multiplicação de leis especiais gerou uma crise de fontes normativas caracterizadas por um conjunto crescente de leis tidas como centros autônomos de gravidade. Surge o termo "microssistema" para descrever uma realidade fragmentada pela pluralidade de estatutos autônomos, com centros de gravidade próprios, para os quais o Código Civil perdeu qualquer capacidade de influência normativa (IRTI, 1999). Nesse ponto, cabe pontuar que o termo microssistema surge nesse contexto e não é compatível, em sua origem, com a metodologia interpretativa atual.

A crise de fontes normativas exigiu a superação de uma "era da segurança", própria do milênio passado, na qual o legislador atua como um "tabelião da história" limitado a chancelar as transformações sociais sem protagonizá-las. Exsurge um "direito pós-moderno", a exigir novas posturas do legislador e do intérprete. O legislador é instado a compor de maneira harmônica o complexo de fontes normativas formais e informais, nacionais e supranacionais, codificadas e extracodificadas. Exemplo dessa postura é refletida nos artigos 45 e 64, da LGPD, por exemplo. Do aplicador do direito exige-se a utilização de novos critérios interpretativos, com valores a serem preservados, a realização enquadramentos axiológicos que atribui teor normativo aos princípios fundamentais de modo a respeitar *todas* as regras do sistema, de diversos patamares hierárquicos, de modo homogêneo e conteúdo objetivamente definido (TEPEDINO, 1998, pág. 11).

Assim, no contexto contemporâneo, o "direito pós-moderno" sucede à era dos microssistemas. Nas palavras de Cláudia Lima Marques (2012, pág. 33): "*efetivamente, essa solução sistemática pós-moderna chega em um momento posterior à codificação, à tópica e à microrrecodificação, e procura uma eficiência não só hierárquica, mas funcional do sistema plural e complexo de nosso direito contemporâneo; [...] A chave aqui é o campo de aplicação da lei*."

O pluralismo de fontes normativas e de sujeitos a proteger (como consumidor e titular), por vezes indeterminados (como nos interesses difusos), bem como dos agentes ativos a quem imputar a responsabilidade (como fornecedores e agentes de tratamento) em relações múltiplas e multifacetadas (de consumo e de tratamento de dados pessoais) reforça a aplicação da teoria do "diálogo das fontes", conceito desenvolvido por Erik Jayme, no Curso Geral de 1995, ministrado na Academia de Direito Internacional de Haia, sob o título "*Identité Culturelle et Intégration: Le Droit International Privé Postmoderne"* e introduzido no Brasil pelas lições significativas de Cláudia Lima Marques (2012). A autora (2012, pág. 19) conceitua diálogo das fontes como a:

> aplicação simultânea coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o Código de Defesa do Consumidor e a lei de planos de saúde) e leis gerais (como o Código Civil de 2002), de origem internacional (como a Convenção de Varsóvia e Montreal) e nacional (como o Código Aeronáutico e as mudanças do Código de Defesa do Consumidor), que, como afirmar o mestre de Heidelberg, tem campos de aplicação convergentes, mas não mais totalmente coincidentes ou iguais.

Trata-se de uma superação da solução de conflito de leis ou de ordens jurídicas pela prevalência de uma e a consequente exclusão (ab-rogação, derrogação, revogação) da outra ou outras do sistema. Essa metodologia afasta a própria premissa de conflito normativo. Ao contrário da concepção de microssistema, o diálogo das fontes defende influências recíprocas de normas, em aplicação conjunta, ao mesmo tempo e ao mesmo caso, complementarmente ou subsidiariamente, coordenada por valores constitucionais e direitos fundamentais.

Nota-se a incompatibilidade conceitual do termo "microssistema", por Natalino Irti, e de "diálogo das fontes", conforme lição de Erik Jayme defendida por Cláudia Lima Marques. Por outro lado, é comum a utilização do termo para descrever normas que regulam determinado nixo, como o do processo coletivo (microssistema do processo coletivo) ou das relações de consumo (microssistema de defesa do consumidor). Não há problema em descrever um conjunto de normas por essa terminologia. O que se deve levar em conta é que não é condizente defender uma interpretação pautada por princípios e regras próprios, não sinérgicos com regulamentos gerais e demais normas do ordenamento jurídico.

Ademais, é preciso atentar-se que a descrição de um "microssistema de defesa do consumidor" ou um "microssistema de proteção de dados pessoais" assume um contexto didático que não pode se confundir com a exigência de um correspondente "microssistema" para regular a Inteligência Artificial. Essa lógica encontra-se superada pelo desenvolvimento e mudanças no papel do legislador e do intérprete que remontam à época da descodificação, no século passado.

Não há óbice para aplicação dos regimes de responsabilidade civil previsto no CDC, na LGPD e no Código Civil àqueles que empregam inteligência artificial em suas atividades.

14.1– IA e responsabilidade civil pelo ato ilícito: a desvinculação da culpa.

Para tratar da aplicabilidade das cláusulas de responsabilidade civil previstas no Código Civil de 2002 aos danos causados pelo emprego da IA, cabe apontar, como premissa, que esse

diploma adota uma sistematização relativa aos Fatos Jurídicos, ou seja, aqueles fatos que geram ou apresentam alguma repercussão jurídica. Além de disciplinar o *negócio jurídico*, o Código Civil dedica disposições relativas aos atos lícitos e ilícitos. As disposições sobre dos atos ilícitos (arts. 186 a 188) são complementadas pelas relativas à responsabilidade civil (arts. 927 a 954, do CC). Essa sistematização revela uma complexidade do tema na forma organizada pelo Código Civil. Os artigos 186 e 187, do CC, apresentam o conceito de ato ilícito. Sua leitura combinada com o art. 927, do mesmo diploma, revelam duas cláusulas gerais de responsabilidade civil pelo ato ilícito.

Para San Tiago Dantas, "*o ilícito é a transgressão de um dever jurídico. Não há definição mais satisfatória para o ilícito civil*." (*apud* CAVALIERI, 2007, p. 9.) A simplificação de San Tiago Dantas não esconde a discórdia que representa a conceituação do ato ilícito, ainda presente na doutrina brasileira. A inauguração do conceito – atribuída ao Código Civil alemão (famoso BGB), de 1897 – representou um avanço do Direito moderno por marcar o abandono da tradicional classificação romana dicotômica de delito e quase delito para erigir o conceito único do ato ilícito (DIREITO, CAVALIERI, 2011). Desde os séculos XVIII e XIX, no entanto, a construção dogmática do conceito de ato ilícito se mostra complexa e controvertida.

A dualidade dos dispositivos que descrevem o ato ilícito no Código Civil (art. 186 e 187) agrava a divergência de seu conceito e o estudo dos seus elementos na doutrina brasileira. O primeiro questionamento sobre o tema se refere à inclusão ou não do elemento culpa em sua definição. A diversificação das noções de dolo e culpa e a gradação da culpa leve, grave e levíssima se inserem no que De Paige categoriza como *diferenciações sem utilidade prática*. Apesar de reconhecer que a culpa compõe o esquema legal do ato ilícito, o autor adverte que o termo traz um sentido amplo de modo a abranger toda espécie de comportamento contrário ao Direito, seja intencional ou não, porém imputável, por qualquer razão, ao causador do dano. (*apud* DIREITO; CAVALIERI, 2011, p. 52).

Aos partidários da culpa como elemento integrante do conceito de ato ilícito (ao que aqui é refererido como uma postura clássica), o ato ilícito pode ser decomposto em três elementos: 1) conduta dolosa ou culposa contrária à norma jurídica; 2) dano; e 3) nexo de causalidade entre ambos (TEPEDINO, BARBOZA, MORAES; 2014). Por esse viés, a verificação de dolo ou culpa por parte do agente é um dos elementos dogmáticos do ato ilícito. Partindo-se dessa mesma perspectiva, Orlando Gomes (2019) extrai a seguinte conclusão: se a responsabilidade é determinada sem culpa, o ato não poderia, a rigor, ser considerado ilícito.

Aduzir que a responsabilidade subjetiva estaria relacionada a um ilícito enquanto a responsabilidade objetiva estaria ligada a uma conduta lícita foi visto como um problema para os doutrinadores que adotaram perspectiva diversa. Por esse outro ponto de vista, a fronteira da ilicitude é determinada pela violação de um dever jurídico (DIREITO; CAVALIERI, 2011, p. 54). Para essa perspectiva, o ato ilícito apresenta duplo aspecto (objeto e subjetivo) e, tomado como violação de um dever jurídico, permite a formulação de dois juízos de valor a seu respeito: o juízo de valor sobre caráter nocivo do ato ou de seu resultado (aspecto objetivo) e um juízo de valor sobre a conduta de seu agente (aspecto subjetivo). (*idem*, p. 55).[102]

Essa perspectiva abraça o conceito "flutuante" (ou dúplice) do ato ilícito que ora é definido pela conduta (culposa – art. 186, do CC), ora é definido pelo dano (injusto – art. 187, do CC). Nesse sentido, Judith Martins Costa (2018, pág. 667):

> O Ordenamento acolhe não apenas a ilicitude subjetiva, isto é, a lesão derivada de ato (doloso ou culposo, voluntário, negligente ou imprudente; comissivo ou omissivo) que viola direito e causa dano a outrem (art. 186), mas igualmente a lesão proveniente da chamada «ilicitude objetiva» – porque independente do elemento subjetivo (culpa ou dolo) –, normalmente configurada no momento do exercício de posições jurídico--subjetivas, quando tido, este, como inadmissível ou disfuncional, segundo certas balizas que o enunciado legal pontua.

Por essa perspectiva, o Código Civil apresenta não um, mas dois conceitos de ato ilícito: um previsto no art. 186 e outro no art. 187. Caso o legislador almejasse unificar tais conceitos, não bastaria expandir a noção de culpa, mas abandonar o juízo de valor da conduta do agente na sua definição. Isso é reforçado pelo fato de que, no art. 187, a culpa não constitui elemento integrante do ato ilícito, mas sim o abuso de direito, configurado quando ultrapassados os limites impostos pela boa-fé, bons costumes e o fim econômico ou social do direito (conceitos que, apesar de indeterminados, não se confundem com a avaliação culpa).

---

[102] De modo diverso, Anderson Schreiber afirma que *ilicitude* somente pode ser utilizada para indicar o ilícito subjetivo, ao passo que a expressão *antijuridicidade* se refere ao ilícito objetivo. O autor valoriza a distinção semântica para caracterizar se a análise de uma conduta leva em conta a vontade do humano que a pratica: "Então, quem viola um dever jurídico ou o direito de outrem, pratica um ato antijurídico – contrário ao direito – mas nem por isso, comete ato ilícito. A ilicitude depende da configuração desta possibilidade de agir de maneira diversa, sem a qual a responsabilidade subjetiva não se impõe. [...] De qualquer modo, é certo que a antijuridicidade, como componente objetivo da ilicitude, corresponde à violação de um dever de conduta, não se confundindo com a ilicitude em si, que exige, além disso, um componente vinculado visceralmente à conduta do sujeito: o da culpabilidade, essencial à responsabilidade subjetiva" (2015, pág. 153-154). Ainda sobre distinções terminológicas, enquanto Sérgio Cavalieri designa ilícito subjetivo o juízo de valor de uma conduta, Orlando Gomes considera esse aspecto como antijuridicidade subjetiva.

Além disso, o amparo à responsabilidade objetiva, conforme expresso no parágrafo único, do art. 927, do Código Civil demonstra que há duas cláusulas gerais de responsabilidade civil (uma objetiva e outra subjetiva) que convivem, mas não se excluem. Daí a justificativa para defender que, fundamentalmente, não há que se confundir o conceito de ilicitude e a culpa.

A análise desses dois posicionamentos antagônicos, no que diz respeito à avalição da culpa ser elemento constitutivo ou não do conceito do ato ilícito, deve exercida com cautela. Melhor do que tomar a conceituação como um fim em si mesmo, deve-se avaliar o que se pretende atingir e o que efetivamente é alcançado com a defesa de um posicionamento ou de uma distinção de conceitos.

Gustavo Tepedino, Maria Celina Bodin e Heloísa Barboza (2014, pág. 337) afirmam que a tese da desvinculação da culpa do conceito de ato ilícito vai de encontro à segurança jurídica:

> Mostra-se equivocada a tentativa de ampliar a noção de ato ilícito, a despeito de seus elementos essenciais, em detrimento da segurança jurídica. A tese, desprovida de base doutrinária, revela-se falsamente progressista, como se propalasse um desprendimento da noção de culpa. Ao contrário, contudo, acaba por ampliar a noção do ilícito, recrudescendo a visão do direito como instrumento não de promoção, mas de repressão, voltado exclusivamente para o momento patológico das relações sociais. Afinal, o ato ilícito constitui-se em fonte das obrigações e sua ampliação desmesurada nenhum proveito traz às relações privadas.

Com base na Teoria Geral do Direito, o raciocínio tem sentido. Isso porque não é qualquer fato social que produz consequências jurídicas. Para o âmbito jurídico, interessa somente os fatos que geram repercussão jurídica, ou seja, os denominado fatos jurídicos. Os fatos jurídicos voluntários, por sua vez, podem ser distinguidos por ato jurídico (que podem ser lícitos ou ilícitos) e negócios jurídicos. A distinção entre ambos é apresentada por Caio Mário (2022, pág. 406): "*os negócios jurídicos são declarações de vontade destinadas à produção de efeitos jurídicos queridos pelo agente; os atos jurídicos em sentido estrito são manifestações de vontade obedientes à lei, porém geradores de efeitos que nascem da própria lei.*"

Por essa perspectiva, a própria definição do ato (seja lícito ou ilícito) exige a manifestação de uma vontade como elemento constitutivo e, por isso, define-se a culpa como elemento que integra o perfil legal de ato ilícito, o que, em princípio, seria respaldo na base normativa constante do art. 186, do Código Civil: "*aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito*."

Com relação ao art. 187, os doutrinadores dessa vertente clássica afirmam que a redação do dispositivo não foi feliz. Definir o abuso de direito como ato ilícito somente faz sentido em uma ampla visão do termo (ilicitude *lato sensu*). Defendem, no entanto, que a etiologia do ato ilícito e do ato abusivo são essencialmente distintas. Nesse sentido (TEPEDINO, MORAES, BARBOSA, 2014, pág. 346):

> A opção legislativa [do art. 187] contraria a doutrina mais moderna do abuso de direito, que procura conferir-lhe papel autônomo na ciência jurídica. A ultrapassada concepção do abuso de direito como forma de ato ilícito, na prática, condicionava sua repressão à prova de culpa, noção quase inerente ao conceito tradicional de ilicitude.
> No direito civil contemporâneo, ao contrário, a aferição de abusividade no exercício de um direito deve ser exclusivamente objetiva, ou seja, deve depender tão-somente da verificação de desconformidade concreta entre o exercício da situação jurídica e os valores tutelados pelo ordenamento civil-constitucional. Além disso, a associação do abuso com o ilícito restringe as hipóteses de controle do ato abusivo à caracterização do ato ilícito, deixando escapar um sem-número de situações jurídicas em que, justamente por serem lícitas, exigem uma valoração funcional quanto ao seu exercício.
> Assim sendo, o art. 187 do CC, que define o abuso de direito como ato ilícito, deve ser interpretado como uma referência a uma ilicitude lato sensu, no sentido de contrariedade ao direito como um todo, e não como uma identificação entre a etiologia do ato ilícito e a do ato abusivo, que são claramente diversas.

Essa perspectiva é fiel à concepção do ato ilícito como fonte de obrigações. Esse posicionamento é um dos motivos que incitou uma postura doutrinária contraposta à clássica. Afinal, se não o ato ilícito, qual seria o fato gerador da responsabilidade objetiva? Para a posição doutrinária diversa da apresentada, vincular culpa ao ato ilícito tem como propósito tecer discussões e retomar debates antigos, que, em síntese visam atacar a existência da responsabilidade objetiva, sob o argumento de que, sem culpa, não há ato ilícito e, sem ato ilícito, não há responsabilidade. Sérgio Cavalieri (2021, pág. 43), em crítica à distinção da responsabilidade objetiva ou subjetiva com foco na licitude ou ilicitude de uma conduta (respectivamente), assim aduz:

> Não há que se falar em *ato lícito* se em todos os casos de responsabilidade objetiva – do transportador, do Estado, do fornecedor etc. – há sempre a violação de um dever jurídico preexistente, o que configura a ilicitude. Ora será o dever de incolumidade, ora o dever de segurança – mas, como veremos, haverá sempre o descumprimento de uma obrigação originária. Ademais, os casos de indenização por *ato lícito* são excepcionalíssimos, só tendo lugar nas hipóteses expressamente previstas em lei, como no caso de dano causado em estado de necessidade e outras situações específicas (Código Civil, arts. 188, II, c/c arts. 929 e 930, 1.285, 1.289, 1.293, 1.385, § 3º etc.). Nesses e em outros

> casos não há responsabilidade em sentido técnico, por inexistir violação de dever jurídico, mas mera obrigação legal de reparação por ato lícito.

Por outro lado, ao se analisar as demais considerações dos doutrinadores tomados como referência para representar a doutrina clássica ou tradicional do ato ilícito, verifica-se que não há uma negação da responsabilidade objetiva. Ao contrário, defendem que se trata de uma evolução da responsabilidade civil, pautada em uma distinção de foco (voltada para a vítima – e não para o agente) e de origem (no risco e não na culpa), conforme se verifica (TEPEDINO et al, 2012. p. 806 e 807):

> A propagação da responsabilidade objetiva no século XX, através da adoção da teoria do risco, comprova a decadência das concepções do individualismo jurídico para regular os problemas sociais. A multiplicação de acidentes, ditos anônimos, que deixavam a vítima completamente desassistida, fez com que, progressivamente, passasse a se atribuir responsabilidade não apenas em razão de manifestação culposa ou dolosa, mas também em decorrência da atividade exercida (e dos benefícios dela obtidos), através das noções de risco-proveito e risco-criado. [...] Com o intuito ele não deixar desamparada a vítima, desenvolveram paulatinamente o novo sistema de responsabilização com base na teoria elo risco, segundo a qual quem exerce determinadas atividades eleve ser responsável também pelos seus riscos, independentemente ele quaisquer considerações em torno do seu comportamento pessoal. [...] Ao contrário da responsabilidade subjetiva, fundada na noção de culpa, a responsabilidade objetiva não se volta para o agente, mas para a vítima, buscando reparar o prejuízo experimentado por determinada pessoa.

Nenhuma das posições negam a convivência da responsabilidade subjetiva e objetiva. Pela doutrina tradicional, a culpa e o risco consistem em duas fontes de responsabilidade distintas, mas que convivem em harmonia (TEPEDINO *et al*, 2012). Pelo posicionamento doutrinário oposto (ou progressista), o ato ilícito continua alçado como o (único) fato gerador da responsabilidade civil e é configurado pela violação de um dever jurídico preexistente, seja o dever de incolumidade (para a responsabilidade subjetiva) seja o dever de segurança (para a responsabilidade objetiva). (Cavalieri, 2021).

Para assumir um posicionamento quanto às teorias, cabe notar que o ponto comum de todas as controvérsias que envolvem a responsabilidade civil – que vão desde a sua conceituação à definição de suas funções – é a tentativa de formular uma teoria ampla o suficiente que ofereça coerência em todas as circunstâncias que o instituto seja aplicado. A constante superveniência de casos "novos", no entanto, revela a insuficiência dos elementos e conceitos de institutos da responsabilidade civil estruturados com essa ambição. Ainda que se busque atualizar conceitos (doutrina progressista) ou acrescentar visões da responsabilidade

(doutrina clássica), a superveniência de inconsistências teóricas revela inseguranças e demonstra que o Direito sempre está um passo atrás na tentativa de regular fatos sociais que se renovam de forma mais rápida do que as teorias jurídicas.

Assim, antes de buscar um posicionamento entre as teorias apresentadas, cabe perguntar: qual seria o propósito de discutir o conceito de ato ilícito? De certa forma, ao analisar os argumentos de ambas as posições, a discussão sobre o conceito de ato ilícito revela um face de "conflito em si mesmo", sem efeito que abale a existência da responsabilidade objetiva ou subjetiva.

Fundamentalmente, reitere-se, não se nota uma consequência que abale a convivência da responsabilidade objetiva e subjetiva a partir das noções de ato ilícito propostas. Os doutrinadores de ambos os lados defendem a existência de duas cláusulas de responsabilidade civil no Código Civil: uma subjetiva (prevista no *caput* do ar. 927) e outra objetiva (disposta no parágrafo único do art. 927).

Para fins de prosseguimento na análise da responsabilidade pelo ato ilícito, defende-se que, a partir da opção pautada pela norma, o Código Civil optou por não confundir ilicitude e culpa. Nesse sentido, acompanha-se a linha de raciocínio no sentido de que, enquanto ilicitude corresponde à contrariedade a direito, a culpa em sentido *lato* consiste no juízo de reprovabilidade da conduta negligente – seja por imprudência, negligência ou imperícia (culpa em sentido estrito) seja por intenção de causar o dano (dolo) (Cavalieri, 2021).

Superada a questão de a ilicitude não conter a culpa como seu elemento constitutivo, cabe anotar que o art. 927 prevê três condições de imputação de responsabilidade civil: uma em seu *caput,* baseada no ato ilícito, e duas em seu parágrafo único. Além da responsabilidade civil pelo ato ilícito (art. 927, *caput*), a obrigação de indenizar pode decorrer de dano causado por atividade de risco normalmente desenvolvida pelo autor do dano bem como nos casos especificados em lei (art. 927, parágrafo único).

O dispositivo é importante para demonstrar que a opção legislativa da origem da responsabilidade civil não se restringe à discussão dos fatores de imputação baseados no ato ilícito ou na atividade de risco, mas também abrange hipóteses legais distintas, tais como danos ambientais (art. 14, §1º, da Lei 6.938/1981), acidentes de consumo (arts. 12 e 18, do CDC) e em razão de tratamento de dados pessoais (art. 44, da LGPD). Para que o conceito de ato ilícito abarque todas essas hipóteses é preciso considerar que a noção legalmente estabelecida de ilicitude civil recobre, conforme especifica Judith Martins Costa (2018), a contrariedade ao Direito em qualquer de suas formas.

A visão de Judith Martins e Sérgio Cavalieri não são fundamentalmente diversas. Inclusive, a autora expressamente concorda com o autor. Mas a tênue diferença da conceituação de ato ilícito entre os doutrinadores não se mostra tão sutil no contexto da Inteligência Artificial. Isso porque Sérgio Cavalieri alude, na qualificação da ilicitude, in verbis: "à conduta humana, contrária ao Direito, sem qualquer referência ao elemento subjetivo ou psicológico" (2021, pág. 45). Ocorre que a "conduta humana contrária ao Direito" indica a valorização de um comportamento que o ordenamento jurídico almeja atingir. A expressão pode sugerir que a responsabilidade civil exige a identificação de uma "possibilidade de agir de modo diverso" (SCHREIBER, 2015), o que nem sempre se verifica em todas as hipóteses que geram o dever de indenizar uma vítima.

Aliás, esse é um dos argumentos utilizados para afirmar que danos decorrentes do emprego da IA não poderiam imputáveis a outrem tendo em vista que a natureza autônoma dessa tecnologia não poderia corresponder a uma ação ou omissão atribuível a alguém. Conforme argumentação apresentada, a vinculação do ato ilícito a uma conduta humana não se confunde com a verificação de seu aspecto volitivo. Além disso, a autonomia da IA se refere à capacidade de processamento para atingir o fim determinado para a qual foi criada, e não uma autonomia de pensar, de ser ou de existir. Em outras palavras, conforme reiteradamente sustentado, a alta capacidade de processamento não retira o caráter instrumental dessa tecnologia.

De toda forma, a par de evitar confusões ou debates meramente conceituais, prefere-se a definição de Judith, para quem "*ilicitude é a lesão a interesse juridicamente protegido*" e não *conduta* contrária ao direito, ainda que independentemente de uma avaliação subjetiva do agente. Seja pela visão da conduta, seja pela visão do dano, "*a noção legalmente estabelecida de ilicitude civil recobre, portanto, a contrariedade ao Direito em qualquer de suas formas*" (MARTINS-COSTA; p. 667).

Diante do exposto, na hipótese de elaboração de uma Inteligência Artificial, seus eventuais resultados danosos podem ser objeto de tutela pelas cláusulas de responsabilidade civil previstas no Código Civil (tais como as elencadas em seu artigo 927). Tomando-se como exemplo a avaliação da responsabilidade civil por ato ilícito diante de consequências discriminatórias do emprego dessa tecnologia, a contrariedade ao Direito pode ser verificada tão somente pelos seus resultados danosos (e não necessariamente pela possibilidade de conduta diversa por aquele que a emprega).

Não se pode afirmar, portanto, que há algum óbice que, a priori, proíba a aplicação de alguma das cláusulas de responsabilidade civil por ato ilícito, previstas no Código Civil. Há,

nesse sentido, uma convivência de regimes de responsabilidade civil extracontratual pelos danos causados por tecnologias autônomas, ainda que com o emprego da inteligência artificial.

14.2– Autonomia da IA e o quadro de responsabilidade civil da LGPD e do CDC.

O caráter instrumental da instrumental da inteligência artificial é o principal argumento a dirimir eventuais conflitos argumentativos sobre a imputação de responsabilidade civil a quem as emprega. Para fins de incidência da LGPD, as circunstâncias de um caso concreto podem ensejar a responsabilidade civil pelo tratamento irregular na modalidade tratamento ilícito (art. 42, *caput*) ou tratamento indevido (art. 44, parágrafo único) bem como pelo tratamento irregular por violar a legítima expectativa de segurança do titular de dados (art. 44, *caput*, segunda parte).

Reitera-se que o caráter autônomo da IA se refere aos meios que pode utilizar (ou adaptar) para atingir o fim para o qual foi desenhada. O bom funcionamento dessa tecnologia depende da qualidade dos dados que servem como *input* para seu processamento e da especificidade dos algoritmos que servem como partida para a atividade (lembrando-se que a qualidade autônoma da IA implica no reconhecimento de sua capacidade de formular e adapte algoritmos para otimizar seu funcionamento). No entanto, a otimização de uma atividade proporcionada pela IA beneficia àquele que a emprega. A autonomia relativa à adaptação de seus códigos de funcionamento ainda atende àquele que a implementou.

No caso de um tratamento de dados pessoais com o emprego da IA, os danos eventualmente causados aos titulares devem ser imputados àqueles que implementaram a tecnologia para a atividade que se pretenda realizar. Ainda que da IA não sucedam benefícios ou resultados adversos (não pretendidos), ao controlador ou operador que a utilizaram como ferramenta para sua atividade de tratamento de dados incumbe a responsabilidade de responder pelos danos causados.

A título de exemplo, em um tratamento de dados pessoais com o emprego da IA para avaliação de candidatos a vaga de trabalho que culmine em resultados discriminatórios (como sexistas, racistas, xenófobos ou etaristas) não há como se desincumbir do dever de responder pelos danos causados sob o argumento da autonomia da tecnologia. Esta está à serviço de quem a emprega.

Nesse exemplo, se o caso envolve o tratamento de dados que identifiquem pessoas ou as tornem identificáveis, o tratamento discriminatório atrairá a incidência do quadro normativo disciplinado pela LGPD. Seria possível, em tese, enquadrar o resultado da atividade em uma violação à segurança esperada pelos titulares de dados, vítimas do preconceito da atividade de

tratamento de dados, a incidir a responsabilidade civil pelo tratamento que viola à expectativa de segurança dos titulares, nos termos do art. 44, *caput*, segunda parte. É mais provável, por outro lado, que o resultado discriminatório envolva a utilização de dados pessoais sensíveis (art. 5º, II) em violação à legislação de proteção de dados, a incidir, portanto, o tratamento ilícito disciplinado no art. 42, *caput*, da LGPD.

Além de identificar ou tornar identificável uma pessoa, se o caso também envolver uma relação de consumo, também atrairá a disciplina do CDC. A título exemplificativo, se a avaliação de um seguro de vida considerar um atributo sensível como orientação sexual ou gênero para avaliar o grau de exposição ao risco de uma pessoa, há nítido emprego da IA que deturpa um tratamento legítimo de dados pessoais, em violação ao art. 6º, IX, que estabelece um princípio geral de não discriminação, pelo qual torna vedado "*o tratamento para fins ilícitos ou abusivos*"[103]. Ademais, essa hipótese pode se sujeitar à disciplina responsabilidade civil pelo fato do serviço, conforme regulamentado pelo CDC.

Sobre a incidência do CDC, cabe notar que o conceito de produto ou serviço completa o entendimento a respeito da figura do fornecedor (art. 3º, *caput*, do CDC), o qual é designado como qualquer pessoa física ou jurídica, pública ou privada, nacional ou estrangeira que desenvolva atividade de produção ou comercialização de produtos ou prestação de serviços. Em outras palavras, fornecedor é aquele que atua profissionalmente no mercado de consumo, recebendo remuneração direta *ou indireta* pela produção, distribuição e comercialização de bens e serviços (BESSA, 2022). Essas qualidades traduzem o conceito genérico ou padrão de fornecedor (apresentado no *caput* do art. 3º).

Ocorre que o CDC também detalha *atividades* que estão subordinadas à sua disciplina, com sujeição à deveres específicos, como no caso das relativas aos bancos de dados de consumo (arts. 43 e 44) e à publicidade (arts. 36 a 38). Sobreleva, nesses casos, a preponderância da *atividade* para concluir pela incidência da disciplina própria do CDC, independentemente da atividade ser remunerada (direta ou indiretamente) ou pela colaboração do autor na criação e veiculação em atuação profissional no mercado de consumo. Trata-se da figura do fornecedor equiparado. Quanto à publicidade, por exemplo, todos que a promovem são considerados fornecedores equiparados (BESSA, 2022, pág. 18).

A figura do fornecedor aparente complementa a abrangência da disciplina do CDC. Trata-se de conceito doutrinário, acolhido pela jurisprudência (STJ, REsp 1.580.432/SP),

[103] Para aprofundar espécies de tratamento de dados pessoais discriminatórios, também referenciados como "discriminação algorítmica", ver MENDES, MATTIUZZO e FUJIMOTO (2023).

utilizado para abranger a pessoa que, de algum modo, se beneficia da marca ou nome consagrado no mercado de consumo de forma a gerar expectativas legítimas nos consumidores quanto à qualidade dos produtos e serviços que divulga e promove (BESSA, 2022). Nesse sentido, o CDC também abrange a figura do fornecedor aparente, de modo a sujeitar sua disciplina àquele que, embora não tenha participado diretamente do processo de fabricação, apresenta-se como tal ao ostentar nome, marca ou sinal de identificação comum com o bem desenvolvido por terceiro. Leonardo Bessa (2022, pág. 20) anota que o conceito de fornecedor aparente também é utilizado em outro sentido, para referir-se à disciplina do fato do produto ou serviço, a incidir ao comerciante quando este não identifica o fabricante do produto ou quando a identificação não é clara (art. 13, do CDC).

A compreensão da figura do fornecedor aparente também ganha relevância na análise da responsabilidade do *influencer* que divulga um produto ou serviço que opera com Inteligência Artificial e que, como em muitos casos, o respectivo fornecedor não tem sede no Brasil. A jurisprudência já tem condenado, a título exemplo, *influencers* que promoveram e/ou divulgaram aplicativos de aposta *Blaze,* reconhecida por polêmicas que envolvem fraudes e favorecimentos a determinados usuários, em prejuízo aos demais apostadores.[104]

Todo esse quadro conceitual demonstra que a abrangência de incidência do CDC compreende a figura do fornecedor padrão, a do fornecedor assim considerado pela atividade que exerce (exemplo: publicidade) – fornecedor equiparado –, bem como a do fornecedor que se ostenta determinada marca ou sinal consagrado no mercado como forma de promover seu produto ou serviço.

Ao retomar o exemplo da avaliação do seguro de vida com o emprego da IA, os consumidores não precisam adquirir o serviço para atrair a disciplina do CDC. Tampouco poderia aquele que fez uso da IA alegar não ser responsável pelas consequências danosas dos resultados (*outputs*) apresentados por essa ferramenta, sob o argumento de suposta autonomia do programa ou por não ser o responsável por elaborar, desenvolver ou comercializar a tecnologia empregada.

Em primeiro lugar, a IA é um instrumento utilizado pelo fornecedor, de modo que não se apresenta como óbice que impossibilite seu enquadramento pelo conceito padrão previsto no art. 3º, *caput*, do CDC. Em segundo lugar, aquele que emprega a tecnologia pode se enquadrar como fornecedor equiparado tendo em vista que a *atividade* de publicidade que utilizou para

[104] O tema merece aprofundamento, tendo em vista as peculiaridades de cada caso. Ver mais em: https://www.jusbrasil.com.br/artigos/influencer-e-responsavel-por-suas-publicacoes-uma-perspectiva-do-caso-blaze/1865283930 Acesso em 12/07/2023.

promover seus produtos ou serviços o torna sujeito à disciplina do CDC. Em terceiro lugar, como fornecedor aparente, ainda que não tenha participado diretamente de um processo de fabricação ou fornecimento, aquele que utiliza a IA também se encontra sujeito às disposições do CDC ante a proibição de se exigir do consumidor que conheça pormenorizadamente a organização interna dos instrumentos empregados, fazendo-se incidir a teoria da aparência e da causalidade adequada caso o fornecedor ostente determinada marca ou sinal que gere expectativa de qualidade ao consumidor.

Por diversas perspectivas, portanto, reforça-se que o emprego da IA não se apresenta como óbice à identificação do agente de tratamento (LGPD) ou do fornecedor (CDC) que será responsabilizado pelos resultados danosos que se apresentam como *output* do emprego dessa tecnologia. O quadro normativo a incidir e disciplinar a responsabilidade civil varia de acordo com as circunstâncias que a atividade é realizada.

14.3– IA e cláusulas gerais de responsabilidade civil do Código Civil.

Um dos mais suscitados argumentos para afastar a responsabilidade civil disciplinada pelo Código Civil se refere à impossibilidade de ser aplicar os preceitos da responsabilidade subjetiva ao tratar de aplicação de sistemas com alto nível de autonomia, como a inteligência artificial. Considera-se, por essa perspectiva, que se determinada ação (ou tomada de decisão) não estava sob a esfera de influência de um ser humano, não seria possível atribuir culpa a essa pessoa em específico pelo dano causado pela máquina. O nexo causal estaria afastado ante a desvinculação da vontade do usuário (como a do motorista ou dos desenvolvedores de um veículo autônomo) pelos danos causados em virtude das decisões de tecnologias guiadas por sistemas de autoaprendizagem (FRULLANI, 2022).

A despeito das diversas ponderações pertinentes aos elementos culpa e nexo de causalidade, que já ensejam debates sobre a responsabilidade civil subjetiva, a instrumentalidade da IA afasta a alegação de que a autonomia de seu processamento seria argumento suficiente, por si só, a afastar a incidência de eventual responsabilidade civil subjetiva disciplinada pelo Código Civil (art. 186, c/c art. 927, *caput*). Cite-se, por exemplo, o desenvolvimento de um carro autônomo cuja programação foi realizada de forma relapsa, em negligência a aspectos relevantes para evitar acidentes. Em que pese a eventual dificuldade inerente à caracterização do elemento volitivo e do nexo causal da responsabilidade civil subjetiva, uma vez demonstrada a negligência (*culpa lato sensu*), a autonomia da máquina não poderia ser utilizada como argumento por seus desenvolvedores.

Por outro lado, no caso de um acidente carreado em fase de testes na elaboração de um carro autônomo inteligente (ou *self-driven cars*) que causa a morte de um pedestre, a definição da responsabilidade civil pelo emprego da IA pode envolver circunstâncias distintas de forma a direcionar a um quadro normativo distinto. Antes de ponderar sobre eventual cláusula de responsabilidade civil do Código Civil que seria incidente sobre o caso, há que se detalhar o funcionamento desse produto e a aplicabilidade dos regimes de tutela previstos no CDC e na LGPD.

Para tratar dos possíveis deslindes dessa hipótese, cabe esclarecer que o funcionamento de um carro de direção autônoma recai no emprego de sensores, algoritmos, sistemas de aprendizado de máquina e processadores de alta capacidade para executar softwares complexos. Para maiores detalhes sobre o funcionamento dos carros autônomos, colaciona-se a seguinte transcrição, em tradução livre, pela autora (ONDRUŠ; KOLLA; VERTAL; SARIĆ, 2020, pág. 229):

> O motorista define insere o destino em um software do carro o qual calcula uma rota e dá a partida. Um sensor LIDAR [*Light Detection And Raging*] giratório montado no teto monitora um alcance de 60 metros ao redor do carro e cria um mapa 3-D dinâmico do carro.
> [...] LIDAR é uma tecnologia de sensoriamento remoto que mede a distância de um alvo a partir do "retorno" do reflexo de luz que emite. É instalado no teto do veículo em um invólucro cilíndrico que gira 360º. LIDAR é o dispositivo mais importante de um veículo autônomo e consiste em um emissor (de luz – ultravioleta, visível ou infravermelha), o espelhamento, e o receptor (da luz refletida).
> [...]
> Um sensor [em geral] na roda traseira monitora o movimento lateral para detectar a posição do carro em relação ao mapa 3-D. Os sistemas de radar instalados [em geral] nos para-choques dianteiro e traseiro calculam as distâncias até os obstáculos.
> [...]
> O software de inteligência artificial no carro está conectado a todos os sensores que servem de *input* [entrada] para seu processamento. [A IA] também recebe *inputs* de Google Street View e de câmeras de vídeo instaladas nas vias.
> [...]
> A IA simula a percepção humana e os processos de tomada de decisão para controlar os sistemas de direção, como direção e freios. O software do carro consulta o Google Maps para aviso prévio de coisas como pontos de referência e sinais de trânsito e luzes

A despeito da enorme quantidade de dados que devem ser coletados e processados para o funcionamento desses veículos, nota-se que o emprego da IA, nesses casos, não envolve, necessariamente, o tratamento de dados pessoais. Por essa perspectiva, a responsabilidade civil

pelos danos decorrentes do acidente causado pelo carro de direção autônoma, ainda que com emprego da inteligência artificial, não seria disciplinado pela LGPD.

Quanto à eventual incidência do CDC, a análise do caso se mostra mais complexa. Com relação ao pedestre, vítima do acidente, não seria o caso enquadrá-lo no conceito de consumidor padrão (art. 2º, *caput*, do CDC) mas sim em uma das três definições de consumidor por equiparação (ou consumidor equiparado) previstas nos artigos 2º, parágrafo único, 17 e 29.

O artigo 17, do CDC, institui a figura do consumidor *bystander* para efeito de aplicação da disciplina de acidente de consumo (responsabilidade pelo fato do produto ou do serviço) equiparando-se as vítimas de um evento ao consumidor, em favor da aplicação do CDC, tanto nos aspectos materiais quanto processuais (BESSA, 2022). Nota-se, portanto, a possibilidade de tratar eventual vítima de atropelamento de um carro de direção autônoma em fase de testes na figura do consumidor equiparado (ou por equiparação). Por outro lado, a identificação da figura do fornecedor não segue a mesma facilidade.

No caso, por se tratar de produto em fase de testes, não haveria *atividade* de publicidade a atrair a figura do *fornecedor equiparado* (art. 36, do CDC). Tampouco haveria a possibilidade de reconhecimento da figura de um *fornecedor aparente* tendo em vista que não há utilização de marca ou sinal para gerar expectativa de qualidade no consumidor, uma vez que o produto sequer foi lançado no mercado. O reconhecimento de um *fornecedor padrão* (art. 3º, *caput*) também resta prejudicado. O fornecedor padrão é aquele que atua profissionalmente no mercado de consumo, recebendo remuneração direta ou indireta pela produção, distribuição e comercialização de bens e serviços. No exemplo, o veículo autônomo envolvido no acidente está em fase de testes e, portanto, nãos e trata de um produto comercializado.

Nota-se que, pelo exemplo, não há dificuldade quanto à equiparação da vítima de atropelamento à figura do consumidor. O responsável pelo desenvolvimento do veículo, por outro lado, não se encaixa na figura de fornecedor tendo em vista a ausência de promoção ou efetiva comercialização do veículo como um produto no mercado de consumo.

A solução do caso remete à disciplina da responsabilidade civil no Código Civil. Ainda que não seja possível identificar o elemento volitivo necessário para estabelecer o nexo causal do condutor ou dos desenvolvedores com o dano causado pelo veículo em fase de testes, a sujeitar o caso à responsabilidade civil subjetiva (art. 186 c/c art. 927, *caput*), cabe notar que o Código Civil também consagra três cláusulas gerais de responsabilidade objetiva: por abuso de direito (arts. 187 c/c art. 927); pelo exercício de atividade de risco (parágrafo único do art. 927); e pelos produtos colocados em circulação por empresários ou empresas (art. 931) (CAVALIERI, 2021).

No exemplo de acidente causado pelo veículo autônomo, não se vislumbra, a priori, abuso de direito apto a atrair a incidência da primeira cláusula de responsabilidade civil objetiva do Código Civil (art. 187 c/c art. 927, *caput*). Isso porque o abuso de direito envolve o exercício irregular de uma vantagem ou privilégio. Como exemplo de abuso de direito, cite-se que a imunidade profissional conferida ao advogado para o exercício de suas funções não abarca violações a direitos da personalidade, especialmente da honra e da imagem de outras pessoas.[105] A liberdade da advocacia, conquanto caracterize projeção do direito fundamental à ampla defesa, admite manifestações contundentes ou inflamadas que não devem ser cesuradas. O limite do exercício dessa liberdade é a sua afetação a direitos da personalidade de outra parte. Como exemplo, não é possível chancelar a prática de advocacia que realize acusações infundadas com o objetivo de macular a legitimidade da prestação jurisdicional à parte adversa. Tal exercício caracteriza exercício abusivo de direitos (art. 187, do Código Civil) do qual exsurge o dever de indenizar pelos danos causados a outrem.[106]

Por outro lado, quanto à segunda cláusula geral de responsabilidade civil, verifica-se que o parágrafo único do art. 927, do Código Civil aduz que "*haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem*". Assim, para além dos casos especificados em lei, o Código Civil também estabelece a responsabilidade objetiva (independente de culpa) para todos aqueles que, no exercício de habitual de atividade perigosa (de risco), causar dano a outrem.

De um lado, é possível verificar que a operação desempenhada pelos empresários, empenhados no desenvolvimento do veículo de direção autônoma, envolve riscos inerentes à própria atividade, especialmente quando o produto é submetido a testes em vias públicas. Por essa perspectiva, o risco é assumido pelo empresário, diante da exposição à segurança e à incolumidade de terceiros na fase de testes de produto cuja alta periculosidade já é reconhecida em seu tráfego comum (direção não autônoma). Em que pese a maior segurança que os veículos autônomos possam vir a proporcionar, não se pode afirmar que um produto em fase de testes carrega a mesma qualidade de segurança que um produto em sua versão final.

---

[105] "A imunidade conferida ao advogado para o pleno exercício de suas funções não possui caráter absoluto, devendo observar os parâmetros da legalidade e da razoabilidade, não abarcando violações de direitos da personalidade, notadamente da honra e da imagem de outras partes ou de profissionais que atuem no processo." STJ. Jurisprudência em Teses, edição nº 138 - Direitos da Personalidade – II. Tese nº 2. Disponibilizada em 29/11/2019. Disponível em: https://processo.stj.jus.br/SCON/jt/doc.jsp?livre=%27138%27.tit. Acesso em 16/03/2023

[106] REsp 1677957/PR, Rel. Ministro RICARDO VILLAS BÔAS CUEVA, TERCEIRA TURMA, julgado em 24/04/2018, DJe 30/04/2018

Quanto aos requisitos dessa responsabilidade civil (art. 927, *parágrafo* único) pode-se dizer que os riscos advindos da prática de testar o funcionamento do veículo autônomo é inerente à atividade desempenhada por aquele que a realiza. No entanto, o dispositivo também é expresso quanto à necessidade dessa atividade ser qualificada como aquela que é "normalmente desenvolvida pelo autor do dano". Por "normalmente desenvolvida" compreende-se aquela atividade exercida profissionalmente ou com habitualidade pelo autor do dano (CAVALIERI, 2021).

Se uma empresa tem por foco de sua atividade a realização de testes de segurança e da qualidade de produtos antes de serem colocados em circulação, é possível enquadrar o acidente causado na fase de testes de um veículo autônomo como risco concretizado pela atividade inerente e habitualmente exercida pela empresa, na forma disciplinada pelo art. 927, parágrafo único, do Código Civil.

Por outro lado, na hipótese em que a realização de testes no desenvolvimento de um carro autônomo integre um projeto, mas não a atividade habitualmente exercida por uma empresa, a situação não apresenta o mesmo enquadramento. Para esses casos, é pertinente a análise da responsabilidade civil nos termos da terceira cláusula geral apresentada pelo Código Civil, conforme a disciplina de seu art. 931: "*ressalvados outros casos previstos em lei especial, os empresários individuais e as empresas respondem independentemente de culpa pelos danos causados pelos produtos postos em circulação*."

Há total sintonia entre a disciplina do art. 931, do Código Civil, e a do art. 12, do Código de Defesa do Consumidor. Ambas estabelecem a responsabilidade objetiva pelo fato do produto (CAVALIERI, 2021). No entanto, uma vez afastada a disciplina do CDC, como no caso tomado como exemplo, incide o art. 931, do CC, cuja norma, mais abrangente, permite aplicar a responsabilidade objetiva a outros casos de acidentes causados por produtos. Nesse sentido, o Enunciado nº 42, da Jornada de Direito Civil I, aduz que "*o art. 931 amplia o conceito de fato do produto existente no art. 12 do Código de Defesa do Consumidor, imputando responsabilidade civil à empresa e aos empresários individuais vinculados à circulação dos produtos*."

O artigo 931, do Código Civil, não exige habitualidade da atividade, tampouco a remuneração ou propósito de lucro. O dispositivo estabelece a responsabilidade civil tão somente pelo empresário ter colocado o produto em circulação. Colocar o produto em circulação não implica na necessidade de comercialização do produto, ou seja, pela literalidade do texto, não se exige que o produto em circulação seja para finalidades de atendimento ao mercado de consumo.

Nesse sentido, na hipótese de atropelamento de pedestre por veículo conduzido de forma autônoma por aplicações de inteligência artificial, sem utilização da dados que identifiquem ou tornem identificável pessoa natural, afastada a incidência da legislação de consumo, para situação que se enquadre como projeto e não atividade habitualmente exercida pela empresa, é possível que o caso se encontre sob a tutela da disciplina da responsabilidade civil prevista no art. 931, do Código Civil

CONSIDERAÇÕES FINAIS

O presente trabalho tem por maior propósito apresentar duas contribuições. A primeira, se refere à proposta de classificação do quadro normativo de responsabilidade civil regulada pela LGPD, composta pelo gênero tratamento irregular, organizada em duas espécies e integrada por duas modalidades por violação à legislação – caracterizadas como tratamento ilícito e tratamento indevido de dados pessoais. Trata-se de objeto desenvolvido na Parte II, do presente trabalho.

Como segunda contribuição, apresenta-se argumentação voltada a sustentar e defender o caráter instrumental da inteligência artificial para fins de apreciação do regime de responsabilidade civil por danos decorrentes de seu emprego. Trata-se de argumento essencial para definir a prescindibilidade de inovação normativa apta a formar um quadro normativo específico para a tutela de danos porventura causados com a utilização da IA. Nesse sentido, considera-se que o dano não decorre *da* inteligência artificial, como ser autônomo, mas sim do risco assumido *por quem a emprega* como instrumento para atingir determinado fim ou para realizar alguma atividade.

Nesse sentido, apresenta-se, de forma escalonada, hipóteses nas quais eventuais danos causados pelo emprego da IA se enquadram sob a tutela do quadro de responsabilidade civil da LGPD, do CDC e/ou do Código Civil. Aplica-se o regime de responsabilidade civil regulado pela LGPD (inclusive, na forma da classificação proposta na Parte II) quando houver a utilização de dados pessoais como *input* de seu processamento ou a externalização, como *output*, de informação que identifique ou torne identificável uma ou mais pessoas naturais.

Ademais, caso o emprego da IA se traduza em uma *atividade* submetida ao regime do CDC (como a publicidade) ou forme uma *relação de consumo* a atrair a incidência dessa legislação (ou seja, com a identificação de fornecedor, consumidor e produto ou serviço), eventuais danos se sujeitarão à tutela do regime de responsabilidade pelo fato ou acidente de consumo (para o caso de danos efetivos) ou pelo vício do produto ou serviço (para as

circunstâncias nas quais a sujeição de altos riscos da atividade implique em vício de qualidade por mau funcionamento ou resulte no não atendimento à finalidade pretendida).

Por outro lado, apresenta-se a solução para os casos nos quais eventuais danos causados com o emprego da IA não se sujeitam à incidência da LGPD ou do CDC. Trata-se do enfrentamento dos possíveis enquadramentos a respeito dos danos decorrentes de atividade que envolvam o emprego dessa tecnologia em cláusulas gerais de responsabilidade civil previstas no Código Civil. Demonstra-se a desvinculação da culpa como elemento integrante do ato ilícito para fins de incidência da responsabilidade civil regulada pelos artigos 186, 187 e 927, do Código Civil. Sempre em reforço ao caráter instrumental da IA, apresentou-se o enquadramento de circunstâncias concretas em face das três cláusulas de responsabilidade civil extracontratual objetiva previstas no Código Civil.

Ao exemplo de evento danoso causado pelo atropelamento de pedestre por um veículo de direção autônoma (*self driven cars*) em fase de testes, analisa-se a possibilidade de sujeição do caso à responsabilidade por abuso de direito (arts. 187 c/c art. 927, do Código Civil) e por danos decorrentes do exercício de atividade de risco (parágrafo único do art. 927, do Código Civil). Demonstra-se a relevância da disposição do art. 931, do Código Civil frente a essas circunstâncias (terceira cláusula geral de responsabilidade civil extracontratual objetiva prevista nesse diploma normativo).

Essa análise da responsabilidade civil, eventualmente imputável àqueles que empregaram a IA como instrumento para atingir o fim pretendido, demonstra a relevância da análise da circunstâncias concretas para efetivar a tutela de danos porventura causados, conforme o regime da LGPD, CDC ou pelas cláusulas de responsabilidade do Código Civil. Trata-se do conteúdo desenvolvido na parte III, do presente trabalho.

A parte I ocupa-se da apresentação do bem jurídico tutelado pelo quadro normativo de responsabilidade civil previsto na LGPD (cuja classificação é objeto da parte II) bem pelo complexo regime normativo de responsabilidade civil em face de danos causados pelo emprego da IA (cuja apresentação escalonada da incidência da LGPD, CDC e Código Civil é o objeto da parte III). Apresentam-se os principais aspectos que diferenciam a proteção de dados pessoais como categoria autônoma de direitos fundamentais e seu relacionamento com direitos correlatos (como privacidade e direito à imagem). Uma das principais contribuições dessa seção se refere à análise do tratamento jurisprudencial e doutrinário para a caracterização do dano moral bem como da tendência pelo (não) reconhecimento de dano *in re ipsa* para hipóteses de tratamento irregular de dados pessoais.

Cabe observar que o presente trabalho se volta a detalhar quadros normativos de responsabilidade civil incidentes sobre danos que envolvem a utilização de dados pessoais, com ou sem o emprego de tecnologias avançadas, como a inteligência artificial. O tema, por outro lado, não resta esgotado. Para além da definição do quadro normativo incidente – de acordo com as disposições da LGPD, do CDC e do Código Civil – há que se avaliar questões próprias que sucedem à identificação da normativa aplicável a casos concretos, tais como a inversão do ônus da prova, questões de solidariedade entre agentes e aprofundamento das hipóteses excludentes de responsabilidade civil.

Ademais, a efetiva tutela à vítima de danos causados pelas atividades cotidianas da sociedade da informação não implica o fim do percurso interpretativo da responsabilidade civil. Há que se enfrentar questões relativas aos interesses daqueles que tiveram que arcar com eventuais danos por força de obrigações estabelecidas pelo regime de solidariedade imposto pela LGPD, pelo CDC e/ou pelo Código Civil. Trata-se do detalhamento da disciplina que deve regular o regime do direito de regresso aplicável caso a caso. Esses temas merecem aprofundamento próprio.

A respeito da classificação proposta na parte II, sustenta-se que o foco da lei nacional de proteção de dados reside tanto na adequação normativa de um tratamento de dados (conformação normativa) quanto na proteção aos direitos do titular de dados (conformação à expectativa de segurança). Nesse sentido, identificam-se duas esferas de proteção distintas, mas não excludentes, previstas na LGPD: uma com foco na conformação da *conduta* dos agentes de tratamento – baseada em prescrições normativas – e outra com enfoque na efetiva *tutela de danos* eventualmente causados aos titulares de dados – em uma perspectiva de proteção e concretização da tutela à dignidade da pessoa humana (art. 1º, III, da CF/1988).

A primeira esfera de proteção da LGPD, prevista no art. 44, *caput*, primeira parte, tem como foco a regulação da conduta daqueles que realizam o tratamento de dados pessoais. O dispositivo exige não apenas que o dano decorra de uma conduta do controlador ou operador (nexo causal), mas que tal conduta expresse uma violação à LGPD ou a regulamento da ANPD. Do contrário, não se verifica o dever de reparar. Por outro lado, o tratamento irregular *"por não atender à expectativa de segurança que o titular dele pode esperar*" (art. 44, *caput*, segunda parte) é mais amplo pois tem como foco a expectativa da pessoa natural (o titular dos dados pessoais). O dever de reparar, por essa ótica, não decorre necessariamente de violação a um dever normativo, mas sim de um dano à expectativa de segurança que, por previsão legal, é tutelado e deverá ser ressarcido. Tal expectativa de segurança constitui a segunda esfera de proteção da LGPD (art. 44, *caput*, segunda parte).

Além de pressupostos distintos, as questões de solidariedade dos agentes de tratamento (art. 42, §1º, I) e de excludentes de responsabilidade (art. 43), conforme previstas na LGPD, merecem análise própria. A LGPD não é expressa quanto ao regime de solidariedade e de excludentes de responsabilidade para o que denominou como tratamento irregular por *violação à expectativa de segurança do titular*. Nesse ponto, ressalta-se a necessidade da análise conjunta dos diplomas legais incidentes sobre o tema, em especial, o Código Civil e o Código de Defesa do Consumidor, com vistas a oferecer respostas consistentes não apenas com as disposições da própria LGPD, mas coerentes com as demais ordenações do sistema jurídico.

A solução para identificar os requisitos dessa responsabilização é, em parte, encontrada no art. 45, da LGPD, que dispõe que "*as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente*." O dispositivo não é interpretado como uma hipótese que afasta a incidência da LGPD – ou seja, como hipótese adicional às dispostas em seu art. 4º – mas sim como mandamento de integração coordenado entre leis especiais.

Esse posicionamento é reforçado pelo art. 64, da LGPD, que expressamente consigna que "*os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte*." Trata-se de uma adoção expressa da interpretação sistemática segundo a técnica do diálogo das fontes.

Como consequência desse posicionamento tem-se que o tratamento de dados envolve a relação múltipla de fontes normativas. Os arts. 45 e 64 habilitam a aplicação sistemática não apenas da LGPD e do Código de Defesa do Consumidor (CDC), mas também destes com outras legislações especiais, como o Marco Civil da Internet (MCI) – Lei nº 12.965/2011 – e a Lei do Cadastro Positivo (LCP) – Lei nº 12.414/2011 –, bem como com as disposições da norma geral, ou seja, com o Código Civil. Ocorre que essa simbiose, ao mesmo tempo que amplia a tutela protetiva dos direitos existenciais do titular dos dados pessoais, torna mais complexa a análise e definição dos limites da responsabilidade do agente de tratamento.

O descumprimento de preceitos afetos à primeira esfera de proteção atrai a análise responsabilidade civil quando ocorre uma violação normativa *lato sensu* da proteção de dados. Tal hipótese configura o tratamento *irregular* por violação à legislação (art. 44, *caput*, primeira parte, da LGPD) a qual pode ser desdobrada em duas modalidades. A primeira denomina-se tratamento *ilícito*, que se configura quando o agente de tratamento, em uma violação de conduta, causa um dano ao titular de dados pela prática de um ato que configura transgressão de alguma exigência da Lei de Proteção de Dados Pessoais. Trata-se da hipótese de incidência

do art. 42, *caput*, da LGPD. A segunda modalidade é descrita como tratamento *inadequado*, o qual se verifica na circunstância em que o agente de tratamento, por omissão de conduta caracterizada pela ausência de adoção de medidas de segurança definidas pela ANPD, enseja que terceiro cause danos ao titular de dados. Cuida-se de modalidade de responsabilidade civil que atrai a incidência do art. 44, *parágrafo único*, da LGPD.

A violação que configura ofensa à segunda esfera de proteção de dados pessoais sujeita-se à tutela da responsabilidade civil pelo tratamento irregular que viola a expectativa de segurança do titular de dados pessoais (art. 44, *caput*, segunda parte). A expectativa em questão deve ser legítima (aspectos previstos nos incisos do art. 44) e *relevante*, ou seja, acarretar o comprometimento da confidencialidade ou da integridade dos dados pessoais.

A classificação do regime de responsabilidade sustentada na presente tese defende, em síntese, o tratamento *irregular* como gênero de duas espécies: aquela que deixa de atender a legislação *lato sensu* e a que não fornece a segurança que o titular possa esperar. A primeira espécie pode, ainda, desdobrar-se em duas modalidades: o tratamento ilícito (violação à legislação *stricto sensu* de proteção de dados pessoais) e o tratamento inadequado (por inobservância aos regulamentos da ANPD).

A classificação apresentada é visualmente estruturada da seguinte forma:

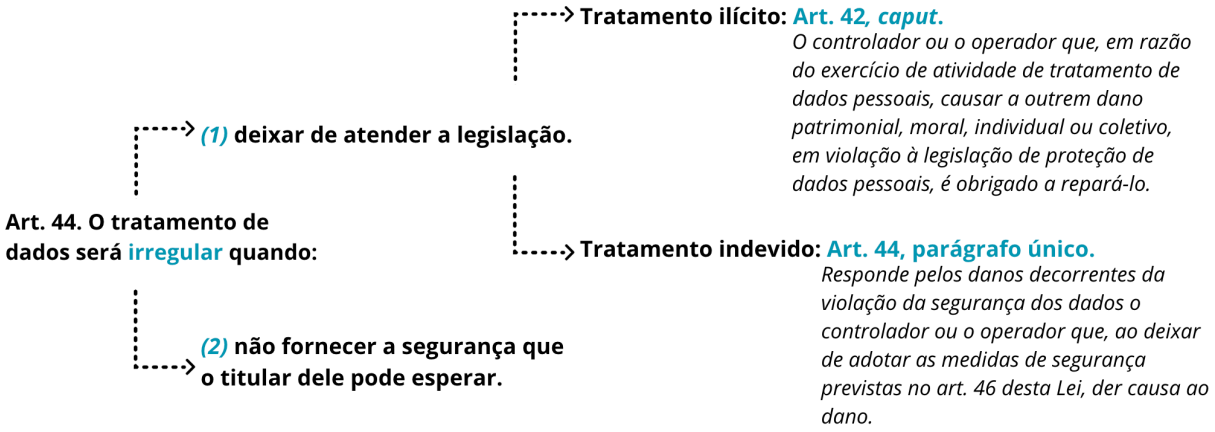

Figura 24 - Espécies de tratamento irregular e modalidades de tratamento irregular por violação à legislação. Distinção de tratamento irregular, ilícito e indevido.

A distinção das modalidades de responsabilidade pelo tratamento irregular em violação à legislação é defensável, pois há avaliação distinta tanto da conduta (por ação ou omissão) quanto da incidência das excludentes de responsabilidade. Defende-se que a alternativa conferida pelo art. 44, *caput*, não se apresenta no sentido de sinonímia (pois o texto seria

redundante) mas sim no sentido aditivo. O intérprete, desse modo, não pode olvidar da ambivalência do tratamento irregular de dados prevista no *caput* do art. 44, da LGPD. Nesse sentido, utilizando-se dos dispositivos constantes da própria LGPD, a classificação apresentada ampara o exercício interpretativo de modo integrado e com coerência não apenas interna – em especial quanto aos seus artigos 42 a 46 – como também com legislações incidentes sobre o mesmo suporte fático (em diálogo das fontes).

Cabe reiterar a ressalva quanto à responsabilidade civil pela violação à expectativa de segurança que, ainda que mais abrangente do que a primeira espécie de tratamento irregular, não pode ser tomada como uma *ditatura do titular dos dados*, a sujeitar todo e qualquer dano a cargo do agente de tratamento, sob pena de subverter os próprios propósitos da responsabilidade civil prevista na LGPD: garantir proteção ao titular de dados sem que isso implique obstáculo ao desenvolvimento tecnológico e à circulação de informações que pautam as relações da sociedade moderna (fundamentos do art. 2º, da LGPD).

O presente trabalho demonstra que a complexidade do sistema brasileiro de responsabilidade civil é apenas reflexo da complexidade da sociedade moderna. Mudanças provocadas por inovações tecnológicas incorporadas no cotidiano da sociedade da informação podem agravar desafios, mas não necessariamente inauguram novos problemas. Nesse sentido, o trabalho apresenta um caráter inovador em contribuição à análise de casos concretos diante da construção de uma classificação da responsabilidade civil da LGPD e por fundamentar a natureza instrumental da Inteligência Artificial – apresentada como premissa essencial para o enfrentamento de danos causados por eventos que envolvam o seu emprego.

A centralização do papel do intérprete se torna mais evidente diante de complexidades de litígios, o que não implica, todavia, na necessidade de inovação normativa para fazer face a toda e qualquer mudança de contexto fático. O quadro normativo de responsabilidade civil, desenvolvido neste trabalho, aplicado a casos que envolvam o emprego da Inteligência Artificial busca apontar soluções e direções para a efetiva tutela aos direitos do titular de dados pessoais e, ao mesmo tempo, criar um ambiente favorável ao desenvolvimento tecnológico o qual, em última análise, beneficia toda sociedade.

REFERÊNCIAS

ACKOFF, Russel. From data to wisdom. *Journal of Applied Systems Analysi*s. vol. 16, pág. 3-9. Lancaster University. 1989. *Internet Archive*. Disponível em: http://faculty.ung.edu/kmelton/documents/datawisdom.pdf

ADADI, Amina; MOHAMMED Berrada. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, vol. 6, 2018, pp. 52138–60. DOI.org (Crossref), https://doi.org/10.1109/ACCESS.2018.2870052.

AGRE, Philip; ROTENBERG, Marc. Technology and Privacy: The New Landscape. *MIT Press*. 1997. Disponível em: https://pages.gseis.ucla.edu/faculty/agre/landscape.html. Acesso em 18 de abril de 2023.

ALCÓN, Alejandro Platero. Análisis de la normativa europea y española de protección de datos personales: régimen de responsabilidad civil derivado de un incorrecto tratamento de datos personales. *Universidad de Extremadura*. Tesis doctoral. R015 programa de doctorado em desarrolho territorial sostenible. 2020. Disponível em: https://dehesa.unex.es:8443/bitstream/10662/11847/1/TDUEX_2020_Platero_Alcon.pdf Acesso em 05 de janeiro de 2023.

ARTIGO 29, Grupo de Trabalho de Proteção de Dados da Comissão Europeia. Parecer 4/2007 sobre o conceito de dados pessoais. Documento 01248/07/PT. WP 136. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf Acesso em 18 de maio de 2023.

AUGUSTINE, Cármen e RODRIGUES, Eduardo Alves. O conceito de língua em Benveniste. *Línguas e instrumentos linguísticos*. n.º 41. 2018.

AVGOUSTI, Cristina. Le droit anglais em matière de responsabilité civile délictuelle. *Le petit juriste*. 2015. Disponível online: https://www.lepetitjuriste.fr/le-droit-anglais-en-matiere-de-responsabilite-civile-delictuelle/#:~:text=En%20Common%20law%2C%20la%20responsabilit%C3%A9,dommage%20subi%20par%20la%20victime. Acesso em 2 de maio de 2023.

BALAZKA, Dominik; RODIGHIERO, Dario. Big Data and the Little Big Bang: An Epistemological (R)evolution. in MIT Open Access Articles. Frontiers in Big Data 3 (September 2020): 31. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/128865/fdata-03-00031.pdf?sequence=1&isAllowed=y Acesso em 14/11/2021.

BARCAROLLO, Felipe. *Inteligência artificial:* aspectos ético-jurídicos. São Paulo: Almedina, 2021.

BASTOS, Aurélio Wander. O habeas data e a proteção da privacidade individual. *Revista Universidade Estácio de Sá*. V. 1, n2, p. 63-85, out/dez, 1999.

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima; BESSA; Leonardo Roscoe. *Manual de Direito do Consumidor*. 9ª edição. São Paulo: Revista dos Tribunais, 2020.

BESSA, Leonardo Roscoe. *Código de defesa do consumidor comentado*. 2º ed. Rio de Janeiro: Forense, 2022.

BESSA, Leonardo Roscoe. *Cadastro positivo:* comentários à Lei 12.414. de 09 de junho de 2011, 1ª ed., São Paulo: Revista dos Tribunais, 2011.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*. Ano 21, nº 53, pág. 191-201, janeiro/março, 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimiza%C3%A7%C3%A3o_e_dado.pdf Acesso em 11 de abril de 2023.

BIONI, Bruno; MARTINS, Pedro. *Devido processo informacional: um salto teórico-dogmático necessário?* Online. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf Acesso em 17 de abril de 2023.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 3º ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistiva.com*. ano 9, nº 3, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506 Acesso em: 02 de maio de 2023.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Gen, 2019.

BIZWIT, Research. Global Artificial Intelligence (AI) in Retail Market Size study, by Offering (Solution, Services), by Function (Operation-Focused, Customer-Focusing), by Technology (Computer Vision, Machine Learning, Natural Language Processing (NLP), Others) and Regional Forecasts 2020-2027. Research Report ID: MSR3357874. *Market Study Report*. Bizwit Research. Publicado em 15 de fevereiro de 2021.

BLUM, Rita. Distinção entre privacidade e proteção de dados pessoais. *Revista de direito privado*, v. 22, n. 110, p. 29-57, out./dez. 2021.

BRITTO, Hágatta. O uso e a proteção de dados pessoais na economia do compartilhamento. *Revista de direito do consumidor*, v. 30, n. 137, p. 113-144, set./out. 2021.

CARDOSO, Oscar Valente. Responsabilidade civil na Lei geral de proteção de dados pessoais. *Revista de direito privado*, v. 23, n. 111, p. 109-123, jan./mar. 2022.

CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil*. 15ª ed. Barueri: Atlas, 2021.

CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil*. 7ª ed. Barueri: Atlas, 2007.

DHAR, Tripti. The California Consumer Privacy Act: The ethos, similarities, and differences vis-a-vis the General Data Protection Regulation and the road ahead in light of California Privacy Rights Act. *Jounal os Fata Protection & Privacy*. Vol. 4, 2. Pág. 179-192. London: Henry Stewart Publications. 2021.

DIREITO, Carlos Alberto Menezes.; CAVALIERI FILHO, Sérgio. Comentários ao novo código civil. 3ª. ed. Rio de Janeiro: Forense, 2011.

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

DONEDA, Danilo. *Da privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3º ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais, *in*: MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

FACCHINI NETO, Eugênio. Da responsabilidade civil no novo código. *Revista TST*. vol. 76, nº 1, jan/mar, Brasília, 2010. Disponível em: https://www.dpd.ufv.br/wp-content/uploads/2020/05/Bibiografia-DIR-313.pdf Acesso em 2 de junho de 2023.

FACHIN, Luiz Edson; BANHOZ, Rodrigo Pelais. Crítica ao legalismo jurídico e ao historicismo positivista: ensaio para um exercício de diálogo entre história e direito, na perspectiva do direito civil contemporâneo. *in*: RAMOS, Carmen Lucia Silveira [et al.] (Org.). *Diálogos sobre direito civil*: construindo uma racionalidade contemporânea. Rio de Janeiro: Renovar, vol. 1, 2002.

FARIAS, Cristiano Chaves de; ROSELVALD, Nelson; NETTO, Felipe Peixoto Braga. *Curso de direito civil*: responsabilidade civil. vol. 3. 10. ed. São Paulo: Juspodivm, 2023.

FEBRABAN; *Engenharia Social*. Grupo de Trabalho de Conscientização da Comissão Executiva de Prevenção a Fraudes da FEBRABAN. São Paulo, 2020.

FRULLANI, Marcelo. Quando um carro autônomo atropela alguém, quem responde? *Publicações*, 08 de março de 2022. Disponível online em: https://frullanilopes.adv.br/quando-um-carro-autonomo-atropela-alguem-quem-responde/#:~:text=Simplificando%3A%20em%20regra%2C%20n%C3%A3o%20%C3%A9,culpa%20a%20um%20indiv%C3%ADduo%20espec%C3%ADfico. Acesso em 4 de junho de 2023.

GARNETT, Simon. Informational self-determination and the semantics of personality in the jurisprudence of the Federal Constitucional Court 1949-1983. *in* KÄMPER, Heidrun; WARNKE Ingo; SCHMIDT-BRÜCKEN, Daniel (orgs.). *Textuelle historizität*: interdisziplinäre perspektiven auf das historische apriori. Berlin: Walter de Gruyter GmbH, 2016. – *online.* Disponível em: https://learning.oreilly.com/library/view/textuelle-historizitat/9783110436723/xhtml/Kapitel12.xhtml Acesso em 12 de abril de 2023. Acesso em: 14 de abril de 2023.

GOMES, Orlando; BRITO, Edvaldo e BRITO, Reginalda Paranhos de (atualizadores). *Obrigações*. 19ª ed. Rio de Janeiro: Forense. 2019.

GONÇALVES, Carlos Roberto. 2014. *Responsabilidade civil.* 10ª ed. São Paulo: Saraiva. 2014.

GRANVILLE, Vincent. Deep Learning: definition, resources, comparison with Machine Learning. *Data Science Central.* 2016. Disponível em: https://www.datasciencecentral.com/deep-learning-definition-resources-comparison-with-machine-learni/ Acesso em.17 de outubro de 2022.

GUERRA, Alexandre Dartanhan de Mello; BENACCHIO, Marcelo (coordenadores). *Responsabilidade Civil*. São Paulo: Escola Paulista da Magistratura. 2014. Disponível online: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Responsabilidade_civil.pdf Acesso em 28 de maio de 2023.

GUILHERME, Luiz Fernando do Vale de Almeida. *Manual de proteção de dados:* LGPD comentada. 1ª ed. São Paulo: Almedina, 2021.

HILDEBRANDT, Mireille. Law for Computer Scientists and Other Folk. *Oxford University Press*. 1st ed. Oxford, 2020. DOI.org (Crossref), https://doi.org/10.1093/oso/9780198860877.001.0001. Acesso em: 7 de abril de 2023.

HILDEBRANDT, Mireille. The issue of proxies and choice architectures. Why EU Law Matters for Recommender Systems. *Frontiers in Artificial Intelligence*. April. Vol. 5. 2022.

IRTI, Natalino. L'età della decodificazione, Giuffrè, 4ª edic., Milano, 1999 *in* TALCIANI, Hernán Corral. La Descodificación del Derecho Civil em Chile*. El Código Civil de Chile (1855-2005). Trabajos expuestos en el Congreso Internacional celebrado para conmemorar su promulgación* (Santiago, 3-6 de octubre de 2005), LexisNexis, Santiago, 2007.

ISMAIL, Kaya. AI vs. Algorithms: What's the difference? *CMSwire*. October, 26, 2018. Disponível em: <https://www.cmswire.com/information-management/ai-vs-algorithms> Acesso em: 18 de abril de 2023.

JOSE, Can Dijck. Datafication, Dataism and Dataveillance: big data between scientific paradigm and ideology. Surveillance & Society, vol. 12, nº 2, May 2014, págs. 197–208. DOI.org (Crossref), https://doi.org/10.24908/ss.v12i2.4776. Acesso em: 22 de abril de 2023.

JÚNIOZ, José Luiz de Moura Faleiros; BASAN, Arthur Pinheiro. Algoritmos, perfilização e contratos de consumo. *Revista Direitos Culturais. Santo Ângelo*. V. 17, n. 43, pág. 41-70, set./dez./ 2022. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/915/476 Acesso em 29 de maio de 2023.

KITCHIN, Rob; MCARDLE, Gavin. What makes big data, big data? Exploring the ontological characteristics of 26 datasets. Big Data & Society, vol. 3, no. 1, June 2016, p. 205395171663113. DOI.org (Crossref), https://doi.org/10.1177/2053951716631130. Acesso em 01 de maio de 2023.

KIĘŻAK, Paweł; Wojtcazk Sylwia. *Toward a conceptual network for the private law of Artificial Intelligence*. Cham: Springer, 2023.

KUEMPEL, Ashley. The Invisible Middleman: a critique and call for reform of the data broker industry. *Northwesterm Journal of International Law & Business*. vol. 36. Issue 1. Winter. 2016. Disponível em: http://scholarlycommons.law.northwestern.edu/njilb/vol36/iss1/4. Acesso em: 3 de abril de 2023.

LACROIX, Marieve. Os fundamentos epistemológicos da responsabilidade civil. *Os cadernos de Direito*, v. 50, nº 2, junho de 2009, págs. 415-433. Disponível online: Acesso em 01 de maio de 2023

LAGE, Fernanda de Carvalho. *Manual de Inteligência Artificial no direito brasileiro*. Salvador: Editora JusPodivm, 2021.

LAGO, José Manuel Busto. La responsabilidad civil y su función de tutela del derecho a la protección de los datos personales: una visión desde el derecho de la unión europea. *REJUR – Revista Jurídica da UFERSA*. Mossoró, v. 5, n. 10, jul/dez., pág. 1-60, 2021. Disponível em: file:///Users/anatarter/Downloads/mlauar,+1+busto.pdf Acesso em: 18 de novembro de 2022.

LASTRES, Helena. Informação e conhecimento na nova ordem mundial. *Revista Ciência da Informação.* v. 28, n 1. DOI: 10.18225/ci.inf.v28i1.862. Disponível em: https://revista.ibict.br/ciinf/article/view/862. Acesso em: 8 de abril de 2023.

LEME, Luciano Gonçalves Paes. Os riscos do desenvolvimento à luz da Responsabilidade do Fornecedor pelo Fato do Produto. *In:* LOPEZ, Teresa Ancona; LEMOS, Patrícia Faga Iglecias, RODRIGUES JÚNIOR, Otavio Luiz (orgs.). *Sociedade de risco e direito privado:* desafios normativos, consumeristas e ambientais. São Paulo: Atlas, 2013.

LEMOS, Ronaldo. *Direito, Tecnologia e Cultura*. FGV: Rio de Janeiro. 2015.

LEONARDI, Marcel. *Fundamentos de direito digital*. São Paulo: Revista dos Tribunais, 2019.

LEONARDI, Marcel. Legítimo Interesse. *Revista do Advogado*, vol. 39, nº 144, pág. 67-73, nov. 2019.

LIMA, Cíntia Rosa Pereira de (coord). *ANPD e LGPD*: desafios e perspectivas. 1ª ed. São Paulo: Almedina, 2021.

LINOWES, David F. (*chairman*). Privacy Protection Study Commission. *Personal Privacy in a Information Society*. The Report of The Privacy Protection Study Commission. Washington: Government Printing Office. July, 1977. Disponível em: https://www.justice.gov/media/1093996/dl?inline= Acesso em: 15 de abril de 2023.

LOBO, Paulo. Danos morais e direitos da personalidade. *Jus Navigandi*, Teresina, Ano 8, n. 119, 31 out. 2003. Disponível em: http://jus.com.br/revista/texto/4445. Acesso em: 18 de maio de 2023.

LONG, Clarissa; Privacy and Pandemics In PISTOR, Katharina. Law in the time of COVID-19. *Columbia Law School Books*, 2020.

LUI, Alison; LAMB, George William. Artificial intelligence and augmented intelligence collaboration: Regaining trust and confidence in the financial sector. *Information and Communications Technology Law*. Liverpool: LJMU Research Online. 2018.

MAIMONE, Flávio Henrique Caetano de. *Responsabilidade civil na LGPD:* efetividade na proteção de dados pessoais. Indaiatuba: Foco. 2022.

MARQUES, Cláudia Lima; MIRAGEM, Bruno. O necessário diálogo entre a LGPD e o Código de Defesa do Consumidor-titular dos dados, *in*: MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

MARQUES, Cláudia Lima. Diálogo das Fontes. *In*: BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. *Manual de Direito do Consumidor*. 9ª ed. São Paulo: Thomson Reuters, 2020.

MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo a Erik Jayme. *in* MARQUES, Cláudia Lima (coord). *Diálogo das Fontes*: do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012, págs. 12 a 79. Disponível https://edisciplinas.usp.br/pluginfile.php/5104368/mod_resource/content/1/10%20aula%20-%20Direito%20e%20fontes%20do%20direito%20em%20esp%C3%A9cie.pdf em: Acesso em 1 de junho de 2023.

MARTINS-COSTA, Judith. *A Boa-Fé No Direito Privado*: Critérios Para a Sua Aplicação. 2ª ed., São. Paulo: Saraiva Jur, 2018.

MAXIMILIANO, Carlos. *Hermenêutica e Aplicação do Direito*. Apresentação de Alysson Leandro. 23º ed. Rio de Janeiro: Forense, 2022.

MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. *Big Data*: a Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013.

MAYOR, Adrienne. *Gods and Robots: myths, machines, and Ancient Dreams of Technology*. Princeton: Princeton University Press. 2018

MCCARTHY, John; MINSKY, M.L.; ROCHESTER, Nathaniel; SHANNON, C.E (org.). *A proposal for the Darthmouth summer research Project on Artificial Intelligence*. Stanford. August. 31, 1955. Disponível em: http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html Acesso em 29 de maio de 2023.

MCCULLOCH, Warren S., PITTS, Walter. A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, 1943. p. 115–133 Disponível em <https://doi.org/10.1007/BF02478259> Acesso em 12 de março de 2023.

MENDES, Gilmar Ferreira. *Estado de Direito e Jurisdição Constitucional*. 2ª ed. Série IDP. São Paulo: Saraiva Educação, 2018.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito , Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020).

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de Dados para além do consentimento: tendências de materialização, *in*: MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *in*: MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da Informação e vazamento de dados. *in* MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

MIRAGEM, Bruno. *Responsabilidade civil*. 2ª ed. Rio de Janeiro: Forense, 2021.

NILSSON, Nils. Artificial Intelligence Prepares for 2001. *The AI Maganize*. 1983. Disponível em <http://ai.stanford.edu/~nilsson/OnlinePubs-Nils/General%20Essays/AIMag04-04-002.pdf>. Acesso em 14 de abril de 2021.

OECD. Organisation for Economic Co-operation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. September 23, 1980. Disponível em:
<http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.
Acesso em 29 de março de 2023.

OECD. Emerging privacy-enhancing technologies: Current regulatory and policy approaches. *OECD Digital Economy Papers*, nº 351, Paris: OECD Publishing, 2023. Disponível em: https://doi.org/10.1787/bf121be4-en. Acesso em 28 de maio de 2023.

OLIVEIRA, Ricardo. Vazamento de dados pessoais pós-LGDP. *Revista dos tribunais*, v. 110, n. 1025, p. 365-370, mar. 2021.

ONDRUŠ, Ján; KOLLA, Eduard; VERTAL; SARIĆ, Željko. How do autonomous cars work? *Transportation Research Procedia.* 44. LOGI 2019 – Horizons of Autonomous Mobility in Europe. Pág. 226-233, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S2352146520300995 Acesso em 2 de junho de 2023.

PAGANELLA, Victoria Dickow. *O nexo de imputação da responsabilidade civil na proteção de dados pessoais*. Londrina: Thoth, 2022.

PECK, Patrícia Pinheiro. *Proteção de dados pessoais*: comentários à lei nº 13.709/2018. 3ª ed. São Paulo: Saraiva Jur, 2021.

PEIXOTO, Fabiano Hartmann Peixoto. Direito e Inteligência Artificial. Coleção Inteligência Artificial e Jurisdição. Volume 2. Dr. IA: Brasília. 2020.

PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. Revista Brasileira de Inteligência Artificial e Direito. Volume 1. RBDI. AID-IA. **2020**. Disponível em: <https://rbiad.com.br/index.php/rbiad>. Acesso em 02/05/2021.

PEIXOTO, Fabiano Hartmann. SILVA, Roberta Zumblick Martins da. Inteligência Artificial e Direito. *Coleção Inteligência Artificial e Jurisdição*. Volume 1. Dr. IA. Curitiba: Alteridade. 2019.

PEREIRA, Caio Mário da Silva. *Instituições de direito civil*: introdução ao direito civil: teoria geral de direito civil. MORAES, Maria Celina Bodin de (atualizadora). Vol. 1. 34ª ed. 2ª reimpr. Rio de Janeiro: Forense, 2022.

RIBEIRO, Anna Carolina Mendonça Lemos; SANTOS, Carlos Denner dos. Isso não é uma pirâmide: revisando o modelo clássico de dado, informação, conhecimento e sabedoria. *Ciência da Informação*. Vol. 49, nº 2, pág. 67-87, maio/agosto. Brasília, 2020.

ROSENVALD, Nelson. NETTO, Felipe Braga. *Código Civil Comentado*. 3ª ed. São Paulo: Juspodivm, 2022.

ROSENVALD, Nelson. NETTO, Felipe Braga. *Leis civis comentadas*. São Paulo: Juspodivm, 2022.

ROSENVALD, Nelson. *As funções da responsabilidade civil*: reparação e a pena civil. 4ª ed. São Paulo: SaraivaJur, 2022.

ROZA, Rodrigo Hipólito. O papel das tecnologias da informação e comunicação na atual sociedade. *Revista Ciência da Informação*. v. 49, n1, p. 67-75, jan./abr., 2020.

RUSSEL, Stuart, NORVIG, Peter. *Inteligência Artificial*: uma abordagem moderna. Tradução: Daniel Vieira; Flávio Soares Corrêa da Silva. 4ª ed. Rio de Janeiro: Gen, 2022.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Sales; BITTAR, Eduardo. *Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital.* São Paulo: Expressa Jur, 2022.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *in* MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 1. ed. Rio de Janeiro: Forense, 2021.

SARTOR, Giovanni. The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Study. European Parliament, Brussels: European Union, 2020.

SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil*: da erosão dos filtros da reparação à diluição dos danos. 6ª ed. São Paulo: Atlas, 2015.

SCHREIBER, Anderson. *Direitos da Personalidade*. 3ª ed. São Paulo: Atlas, 2014.

SCHWABE, Jügen; MARTINS, Leonardo. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Konrad-Adenauer-Stiftung, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf Acesso em 18 de abril de 2023.

SERRANO, Pedro Estevam Alves Pinto. Autoritarismo líquido e as novas modalidades de prática de exceção no século XXI. *Revista Themis*. Vol. 18, nº 1, p. 197-223, jan/julho. Fortaleza. 2020. Disponível online em: file:///Users/anatarter/Downloads/admin,+Gerente+da+revista,+8.+Autoritarismo+l%C3%ADquido.pdf Acesso em 28 de maio de 2023.

SILVA, Fernando Rodrigues. A LGPD e o tratamento de dados pessoais como mecanismo de publicidade no ambiente das redes sociais. *Revista brasileira de direito comercial*, v. 9, n. 50, p. 36-57, dez./jan. 2022/2023.

SILVA, Luan; FERREIRA, Victor; ARAÚJO, Leandro; SANTOS, Adam. Aplicação de Deep Learning no pré-diagnóstico da COVID-19 através de imagens de raio-x. *UNIFES SPA contra a COVID-19*. 13 de maio de 2020. Disponível em: https://acoescovid19.unifesspa.edu.br/images/conteudo/Aplica%C3%A7%C3%A3o_de_Deep_Learning_no_pr%C3%A9-diagn%C3%B3stico_da_COVID-19.pdf Acesso em 29 de maio de 2023.

SIMÃO, Lucas Pinto; COSTA, Priscilla Martins de Freitas. Regimes de responsabilidade civil no Código de Defesa do Consumidor (CDC) e na Lei Geral de Proteção de Dados (LGPD). *Revista Forense*. São Paulo. vol. 431, janeiro-junho de 2020, set/2020. Disponível em: http://genjuridico.com.br/2020/09/09/regimes-de-responsabilidade-civil-cdc-lgpd/ Acesso em 20 de abril de 2023.

SOARES, Guido Fernando Silva. Estudos de Direito Comparado (I) - O que é a "Common Law", em particular, a dos EUA. *Revista Da Faculdade De Direito, Universidade de São Paulo*, 92, 163-198. Disponível em Acesso em: https://www.revistas.usp.br/rfdusp/article/view/67360. 2 de maio de 2023.

SOLOVE, Daniel J. Nothing to hide: The false tradeoff between privacy and security. *Yale University Press*, 2011. Disponível em: file:///Users/anatarter/Downloads/SSRN-id3976770.pdf Acesso em 11 de abril de 2023.

STRÖMHOLM, Stig. Right of privacy and rights of the personality. *Instituti upsaliensis iurisprudentiae comparativae.* ACTA VIII. Stocklm: Boktryckeri AB Thule, 1967. – *online*. Disponível em: https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf Acesso em 12 de abril de 2023.

TAKASHI, Tadao (org.). *Sociedade da informação no Brasil*: livro. Brasília: Ministério da Ciência e Tecnologia, 2000. Online. Disponível em: https://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf Acesso em 08/04/2023.

TARTER NUNES, Ana Luisa. PEIXOTO, Fabiano Hartmann. Inteligência Artificial (IA), inovação e os parâmetros na relativização da proteção de dados pessoais: a execução de políticas governamentais por meio da IA no combate ao coronavírus e outros impactos do julgamento da ADIN nº 6.387. LUNARDI, Fabrício, CLEMENTINO, Marco Bruno Miranda (Coord). *Inovação judicial:* fundamentos e práticas para uma jurisdição de alto impacto. pág. 261 a 189. Brasília: Enfam. 2021 Disponível em: https://www.enfam.jus.br/wp-content/uploads/2021/12/Livro-Inovacao-judicial.pdf

TARTUCE, Flávio. *Responsabilidade civil*. 3ª ed. Rio de Janeiro: Forense; 2021.

TEFFÉ, Chiara Spadaccini; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça. *Revista IBERC*, v. 1, n. 1, pág. 01-28, nov-fev, 2019. *Online*. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/6/5 Acesso em20 de abril de 2023.

TEIXEIRA, Tarcísio. GUERREIRO, Ruth. *Lei Geral de Proteção de Dados*. 4ª ed. São Paulo: Saraiva Jur, 2022.

TEPETINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do direito civil, volume 4*: responsabilidade civil. 4ª. Ed. Rio de Janeiro: Forense, 2023.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde. A evolução da responsabilidade civil por fato de terceiro na experiência brasileira. *Revista de Direito da Responsabilidade*. Ano 1, 2019. Disponível em: https://www.academia.edu/40331264/A_EVOLU%C3%87%C3%83O_DA_RESPONSABILIDADE_CIVIL_POR_FATO_DE_TERCEIRO_NA_EXPERI%C3%8ANCIA_BRASILEIRA?email_work_card=title Acesso em 28 de maio de 2023.

TEPEDINO, Gustavo; MORAES; Maria Celina Bodin de; BARBOSA, Heloísa Helena. *Código Civil interpretado*: conforme a Constituição da República. 3ª. Ed. Rio de Janeiro: Renovar; 2014.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. 1999. Disponível em: https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil_constitucional_brasileiro Acesso em 18 de abril de 2023.

TEPEDINO, Gustavo. Código Civil, os chamados microssistemas e a Constituição. *Revista da Faculdade de Direito da Universidade do Estado do Rio de Janeiro*. Rio de Janeiro: Imprenta UERJ, n. 6/7, pág. 13-25, 1998.

TOMUSCHAT, Christian; CURRIE, David; KOMMERS, Donald; KERR, Raymond. (tradutores). *Basic Law for the Federal Republic of Germany* in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 28 June 2022 (Federal Law Gazette I p. 968). *Online*: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html Acesso em 12 de abril de 2023.

TUMELERO, Naíra Ariana Souza. Perfilização e coleta de dados comportamentais: as políticas de privacidade da Google pela ótima consumerista no capitalismo da vigilância. *Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo.* v. 7, n. 1, p. 55-74, Jan/Jul. 2021.

TURING, Alan M. Computing Machinery and Intelligence. *Mind*. New Series, v. 59, n. 236, 1950, p. 433-460. Disponível em https://phil415.pbworks.com/f/TuringComputing.pdf Acesso em 02 de maio de 2021.

TURKINGTON, Richard. Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy. *Northern Illinois University Law Review*. Vol. 10: Issue 3, Article 3. Págs 479-520. Publication date: 07/01/1990. Disponível em: https://huskiecommons.lib.niu.edu/cgi/viewcontent.cgi?article=1666&context=niulr

UPRICHARD, Emma. Focus: Big Data, Little Questions?. *Discover Society,* issue 1, October 2013, disponível em https://archive.discoversociety.org/2013/10/01/focus-big-data-little-questions/

VERBICARO, Dennis. A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (Lei geral de proteção de dados pessoais). *Revista de direito do consumidor*, v. 31, n. 139, p. 73-99, jan./fev. 2022.

VERGNOLLE, Suzanne. *L'effectivité de la protection des personnes par le droit des données à caractère personnel*. Thèse pour le doctorat en droit. Orientador: Jérome Passa. Université Paris II. École Doctorale de Droit Privé. 2020.

VIGLIAR, José Marcelo Menezes (coord.). *LGPD e a proteção de dados pessoais na sociedade em rede*: dados de crianças e adolescentes na internet, tratamento de proteção de dados no comércio eletrônico, proteção dedados de falecidos, violação de direitos da personalidade e responsabilidade civil. São Paulo: Almedina, 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadaccine de. *in* MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord.). *Tratado de proteção de dados pessoais*. 1. ed. Rio de Janeiro: Forense, 2023.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, Dec. 1890.

ZANATTA, Rafael. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. *ResearchGate*. 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais#:~:text=tratamento%20de%20dados%20que%20objetiva,de%20consumo%20e%20de%20cr%C3%A9dito. Acesso em 18 de março de 2023.

ZAPATA, Ângela María Londoño; VALENCIA, Daniela López. La responsabilidad civil del manejo de datos em la era digital desde la perspectiva de la normativa jurídica colombiana y del marco normativo europeo. *Repositório UniLibre.* Universidad Libre. Colômbia. 2020. Disponível em: https://repository.unilibre.edu.co/bitstream/handle/10901/20671/LA%20RESPONSABILIDA

D%20CIVIL%20DEL%20MANJEO%20DE%20DATOS%20EN%20LA%20ERA%20DIGITAL.pdf?sequence=1 Acesso em 14 de setembro de 2022.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. Tradução. Antonio Holzmeister Oswaldo Cruz e Bruno Cardoso. *in* BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; MELGAÇO, Lucas (orgs.). *Tecnopolíticas da vigilân*cia: perspectivas da margem. 1 ed. São Paulo: Boitempo, 2018. P'GA. 17-68. Disponível em: https://medialabufrj.net/wp-content/uploads/2020/10/Tecnopoliticas-da-vigilancia_miolo_download.pdf Acesso em 13 de maio de 2023.

ZWITTER, Andrej; GSTREIN, Oskar. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of Internacional Humanitarian Action.* Springer. 2020. Disponível em: https://jhumanitarianaction.springeropen.com/track/pdf/10.1186/s41018-020-00072-6.pdf. Acesso em 11 de março de 2023.