BOCA
BOLETIM DE CONJUNTURA

A VULNERABILIDADE DIGITAL E A TUTELA DOS DIREITOS DA PERSONALIDADE: A VULNERABILIDADE DIGITAL E O ACESSO A JUSTIÇA NO PROCESSO CIVIL COLETIVO SOB A ÉGIDE DA LGPD

DIGITAL VULNERABILITY AND THE PROTECTION OF PERSONALITY RIGHTS: DIGITAL VULNERABILITY AND ACCESS TO JUSTICE IN COLLECTIVE CIVIL PROCEEDINGS UNDER THE LGPD (BRAZILIAN GENERAL DATA PROTECTION LAW)

VULNERABILIDAD DIGITAL Y PROTECCIÓN DE LOS DERECHOS DE LA PERSONALIDAD: VULNERABILIDAD DIGITAL Y ACCESO A LA JUSTICIA EN EL PROCESO CIVIL COLECTIVO AL AMBIENTE DE LA LGPD

10.56238/bocav25n77-021

Uassi Mogone Neto
Mestrando em Ciências Jurídicas
Instituição: Universidade Cesumar (UNICESUMAR)

Daniela Cristina Arone Mogone
Especialista em Direito Público
Instituição: Faculdade de Direito

Joaquim Pedro de Oliveira Volante
Doutor em Direito no Programa de Pós-Graduação em Ciências Jurídicas (PPGCJ)
Instituição: Universidade Cesumar (UNICESUMAR)

Roberson Neri Costa
Doutorando em Direito no Programa de Pós-Graduação em Ciências Jurídicas (PPGCJ)
Instituição: Universidade Cesumar (UNICESUMAR)

Horácio Monteschio
Pós-doutor pela Universidade de Coimbra - Portugal; Pós-doutor pelo Centro Universitário Curitiba - UNICURITIBA, Paraná - Brasil; Pós-doutor pela Mediterranea International Centre for Human Rights Research, MICHR, Regia Calábria – Itália
Bolsista Produtividade em Pesquisa do Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI), Maringá (PR)
Instituição: Universidade Cesumar (UNICESUMAR)

RESUMO
A expansão da sociedade da informação transformou os dados pessoais em extensões da personalidade humana, expondo os indivíduos a uma hipervulnerabilidade estrutural perante a economia de vigilância. O objetivo deste estudo é analisar a viabilidade da tutela processual coletiva estruturante como mecanismo adequado de defesa contra a exploração massiva e algorítmica de dados, visando superar a insuficiência dogmática do modelo baseado exclusivamente no consentimento. A

metodologia adota a abordagem lógico-dedutiva, fundamentada em revisão bibliográfica especializada na dogmática civil e processual, aliada à análise documental da legislação e ao exame da evolução jurisprudencial nos tribunais superiores brasileiros. Os resultados indicam que a assimetria de poder tecnológico, agravada por interfaces manipuladoras e políticas de adesão compulsória, inviabiliza o controle genuíno das informações pelo titular, o que exige a transição material para a responsabilidade proativa dos agentes de tratamento. Conclui-se que o microssistema de processo coletivo desponta como a via democrática indispensável para impor limites sistêmicos às corporações de tecnologia, permitindo decisões estruturantes que garantam a readequação arquitetônica dos sistemas informacionais e a efetiva preservação da dignidade no ambiente digital.

Palavras-chave: Direitos da Personalidade. Hipervulnerabilidade Digital. Proteção de Dados. Processo Coletivo. Consentimento.

ABSTRACT

The expansion of the information society has transformed personal data into extensions of human personality, exposing individuals to a structural hypervulnerability in the face of the surveillance economy. The objective of this study is to analyze the viability of structural collective procedural protection as an adequate defense mechanism against the massive and algorithmic exploitation of data, aiming to overcome the dogmatic insufficiency of the model based exclusively on consent. The methodology adopts a logical-deductive approach, based on a specialized bibliographic review of civil and procedural dogmatics, combined with documentary analysis of legislation and the examination of jurisprudential evolution in Brazilian superior courts. The results indicate that the asymmetry of technological power, aggravated by manipulative interfaces and compulsory adhesion policies, makes genuine control of information by the data subject unfeasible, which requires a material transition to the proactive responsibility of processing agents. It is concluded that the collective process microsystem emerges as the indispensable democratic path to impose systemic limits on technology corporations, allowing structural decisions that guarantee the architectural readjustment of informational systems and the effective preservation of dignity in the digital environment.

Keywords: Personality Rights. Digital Hypervulnerability. Data Protection. Collective Process. Consent.

RESUMEN

La expansión de la sociedad de la información ha transformado los datos personales en extensiones de la personalidad humana, exponiendo a los individuos a una hipervulnerabilidad estructural frente a la economía de la vigilancia. El objetivo de este estudio es analizar la viabilidad de estructurar la tutela procesal colectiva como un adecuado mecanismo de defensa frente a la explotación masiva y algorítmica de datos, buscando superar la insuficiencia dogmática del modelo basado exclusivamente en el consentimiento. La metodología adopta un enfoque lógico-deductivo, basado en una revisión bibliográfica especializada en dogmática civil y procesal, combinada con el análisis documental de la legislación y el examen de la evolución jurisprudencial en los tribunales superiores brasileños. Los resultados indican que la asimetría del poder tecnológico, agravada por interfaces manipuladoras y políticas de adherencia obligatoria, hace inviable un control genuino de la información por parte del poseedor, lo que requiere una transición material hacia la responsabilidad proactiva de los agentes procesadores. Se concluye que el microsistema de procesos colectivos emerge como la forma democrática indispensable para imponer límites sistémicos a las corporaciones tecnológicas, permitiendo estructurar decisiones que garanticen el reajuste arquitectónico de los sistemas de información y la preservación efectiva de la dignidad en el entorno digital.

Palabras clave: Derechos de la Personalidad. Hipervulnerabilidad Digital. Protección de Datos. Proceso Colectivo. Consentir.

1 INTRODUÇÃO

A transição para a sociedade da informação reconfigurou profundamente as interações sociais e econômicas, o dado pessoal consolidou-se como um verdadeiro prolongamento da essência humana no ambiente digital.

Nesse cenário, o direito civil contemporâneo depara-se com o desafio de tutelar a pessoa perante a economia de vigilância, a privacidade deixou de ser apenas o direito de ser deixado em paz e passou a exigir um controle dinâmico dos fluxos informacionais, configurando uma nova dimensão de identidade territorial e jurídica projetada nas redes.

A evolução desse modelo econômico baseado em dados evidenciou a profunda falência do consentimento individual como ferramenta exclusiva de proteção.

Diante de políticas de privacidade obscuras e sistemas algorítmicos opacos, o usuário é submetido a uma hipervulnerabilidade estrutural. Emerge, portanto, o problema central desta pesquisa, questiona-se como o ordenamento jurídico pode superar a insuficiência da tutela individual e do consentimento viciado para garantir a proteção efetiva dos direitos da personalidade frente à exploração massiva de informações.

A relevância deste debate justifica-se pela urgência em conter práticas discriminatórias e a mercantilização indiscriminada da vida privada, pois torna-se imprescindível deslocar o eixo de proteção da mera anuência formal para a responsabilidade proativa dos agentes de tratamento, resguardando a integridade da pessoa humana em seus variados contextos sociais.

É exatamente nesse vácuo de efetividade material que o direito processual coletivo se apresenta como o mecanismo democrático indispensável para impor limites sistêmicos às grandes corporações de tecnologia.

Para responder a essa problemática, o estudo tem como objetivo geral analisar a viabilidade e a necessidade da tutela processual coletiva estruturante como o instrumento adequado de defesa contra a hipervulnerabilidade digital.

Como passos específicos, busca-se examinar a reconfiguração dos direitos da personalidade na economia informacional, demonstrar a crise dogmática do consentimento perante a assimetria de poder tecnológico e, por fim, investigar a aplicação do microssistema processual coletivo brasileiro na repressão de danos massivos.

Metodologicamente, a pesquisa adota a abordagem lógico dedutiva, o raciocínio desenvolve-se por meio de revisão bibliográfica especializada na dogmática civil e processual, aliada à análise documental da legislação vigente e ao exame cauteloso da evolução jurisprudencial nos tribunais superiores brasileiros.

A fim de alcançar os resultados pretendidos, o texto está estruturado em cinco seções fundamentais. A primeira aborda a hipervulnerabilidade digital e os direitos da personalidade. A

segunda explora a crise do consentimento e a responsabilidade proativa. A terceira seção analisa as respostas do acesso à justiça e da tutela coletiva no processo civil. A quarta apresenta a pesquisa jurisprudencial pertinente. A quinta e última seção propõe sugestões de melhoria processual e material para o aperfeiçoamento do sistema legislado em vigor.

2 A HIPERVULNERABILIDADE DIGITAL E OS DIREITOS DA PERSONALIDADE

Os direitos da personalidade, fundados no princípio da dignidade da pessoa humana, não constituem um rol taxativo, mas representam o epicentro finalístico/axiológico da ordem constitucional, irradiando efeitos sobre todo o ordenamento jurídico e balizando não apenas os atos estatais, mas toda a miríade de relações privadas

O jurista italiano Pietro Perlingieri (PERLINGIERI, 1999) ensina que a tutela da privacidade configura uma situação subjetiva complexa, voltada para o livre desenvolvimento da personalidade

Diferente da ótica proprietária clássica, o direito civil contemporâneo é funcionalizado à realização da dignidade humana, de modo que a pessoa humana qualificada e vulnerável torna-se a categoria central do direito privado (TEPEDINO, 2008)

No Brasil, autores como Danilo Doneda e Bruno Ricardo Bioni consolidaram o entendimento de que a proteção de dados pessoais é um direito fundamental autônomo, projetando a própria identidade do indivíduo no ambiente digital. Stefano Rodotà (RODOTÀ, 2008) foi pioneiro ao alertar que o direito à privacidade não mais se estrutura exclusivamente em torno do eixo "pessoa-informação-segredo", mas sim no eixo dinâmico de "pessoa-informação-circulação-controle"

Na "Sociedade da Informação", a utilização cada vez mais ampla de dados pessoais faz com que estas informações assumam o lugar da própria presença física da pessoa em diversas circunstâncias

O dado pessoal atrelado a um indivíduo converte-se, assim, em um verdadeiro prolongamento corpóreo e incorpóreo de sua ipseidade, exigindo que a ciência jurídica o proteja das agressões que afetem sua individualidade (BIONI, 2019)

Ao se reconhecer a informação como um atributo da personalidade, o controle sobre esses fluxos de dados transcende a mera expectativa de isolamento (“right to be let alone”) e passa a ser uma ferramenta essencial de cidadania e de autodeterminação informacional (DONEDA, 2011).

A pessoa passa a ser definida, perante corporações e o Estado, por sua "biografia digital", que a padroniza e a categoriza em estereótipos baseados em seus valores, estilo de vida e hábitos de consumo.

Nas relações digitais contemporâneas, o indivíduo encontra-se em situação de severa assimetria informacional e de poder. A economia digital engendrou um novo modelo de acumulação de capital no qual os dados pessoais dos cidadãos ditam a lógica de geração de riquezas, estabelecendo o que a doutrina convencionou chamar de "economia de vigilância" (BIONI, 2019).

Neste cenário, o indivíduo é constantemente monitorado, acumulando-se uma série de rastros comportamentais que são monetizados por meio da publicidade direcionada e da formação de perfis (“profiling”).

O mercado informacional caracteriza-se por uma ilusão de gratuidade (“zero-price advertisement business model”), em que o consumidor entrega seus dados em troca de acesso a plataformas, motores de busca e redes sociais. Ocorre que, dadas as limitações cognitivas humanas e a complexidade do ecossistema de atores que compartilham essas informações (como os data brokers), o titular dos dados é incapaz de prever os reais custos dessa transação (BIONI, 2019).

Ele "compra agora para pagar depois", em um quadro de incertezas no qual os possíveis danos decorrentes da perda do controle sobre seus dados só serão experimentados no futuro.

Diante desse cenário de opacidade, Bruno Miragem (MIRAGEM, 2014) destaca que o novo direito privado deve tutelar os vulneráveis, reconhecendo que a tecnologia instaura uma verdadeira "hipervulnerabilidade" do usuário/consumidor.

Essa hipervulnerabilidade não decorre apenas de condições subjetivas intrínsecas ao indivíduo (como idade, saúde ou grau de instrução), mas da inserção objetiva do sujeito em um mercado informacional opaco e predatório, no qual ele é transformado em mero objeto de vigilância e mercadoria (BIONI, 2019).

Essa nova camada de vulnerabilidade é agravada pelo mecanismo do consentimento forçado ou das políticas de "tudo ou nada" (“take-it-or-leave-it”). O usuário é submetido a longos e incompreensíveis “Termos de Uso”, sem qualquer poder de barganha para negociar suas preferências de privacidade.

O consentimento, em vez de ser um instrumento de emancipação, transmuda-se em uma "ficção legal" utilizada para legitimar a exploração contínua e massiva de dados por corporações.

Para Gustavo Tepedino, a tecnologia expande o alcance da memória humana de forma incalculável, registrando paradeiros, itinerários, origens e destinos, sendo estritamente necessário proteger as liberdades civis contra a ingerência abusiva (TEPEDINO, 2008).

O processamento desses dados em larga escala (“Big Data”) pode instituir uma "ditadura dos dados", onde os algoritmos passam a orquestrar as vidas das pessoas, retirando-lhes a autonomia de decidir como querem viver e balizando invisivelmente as suas oportunidades.

Essa arquitetura tecnológica não apenas extrai informações, mas as utiliza para classificar, prognosticar e julgar seres humanos, o que frequentemente culmina na chamada discriminação algorítmica (FRAZÃO, 2018).

Embora exista o mito de que os algoritmos matemáticos sejam neutros e objetivos, a doutrina demonstra que a neutralidade tecnológica é uma ilusão (GRAMINHO, 2024).

Os algoritmos são construções humanas e aprendem com bases de dados históricos que carregam preconceitos atávicos estruturais da sociedade. Na esfera das relações de trabalho, os impactos da inteligência artificial são profundos. Empresas delegam a sistemas automatizados poderes diretivos e disciplinares que antes cabiam ao empregador físico, utilizando softwares para selecionar currículos, recrutar candidatos, monitorar a produtividade em tempo real e até promover dispensas.

Contudo, se o modelo estatístico é treinado com dados enviesados — por exemplo, uma empresa cujo histórico de contratação foi predominantemente de homens brancos, a inteligência artificial (“machine learning”) replicará o viés, penalizando currículos de mulheres e minorias.

Trata-se da "discriminação por erro estatístico" ou "generalização injusta", que afeta diretamente o princípio constitucional da igualdade e cerceia o acesso democrático ao mercado de trabalho.

Situação semelhante ocorre no mercado de consumo e na concessão de crédito, em que a "discriminação por proxy" pune o indivíduo não por seus atos, mas por presunções baseadas na sua geolocalização, em seus hábitos de navegação ou em compras em determinadas lojas, alterando preços de produtos (“price discrimination”) ou negando financiamentos. Esses dados sensíveis, em especial, representam o "núcleo duro" dessa tutela da personalidade (TEFFÉ, 2020).

A LGPD (Lei nº 13.709/2018) classifica como sensíveis os dados referentes a origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde, à vida sexual, e dados genéticos ou biométricos

A proteção exacerbada a essa categoria justifica-se pelo seu alto potencial de gerar perfilamentos e exclusões ilícitas e abusivas de grupos historicamente vulneráveis.

Ocorre que a evolução do “Big Data” permite que mesmo dados inicialmente "triviais" ou anonimizados sejam cruzados e refinados até revelarem características íntimas do sujeito. Um histórico de compras ou simples cliques de navegação podem denunciar uma gravidez precoce, o estado de saúde mental ou a orientação sexual de um indivíduo (BIONI, 2019).

Por isso, o direito à proteção de dados atua como garantidor do princípio da não discriminação, vedando a utilização dessas inferências tecnológicas para fomentar práticas segregatórias nas relações civis, de consumo e laborais.

Para refrear esse quadro de hipervulnerabilidade, a LGPD impõe limites principiológicos intransponíveis à gestão algorítmica, destacando-se a transparência, a responsabilização e o direito à explicação (GRAMINHO, 2024).

A exigência legal de que o consentimento para o tratamento de dados sensíveis seja "específico e destacado" (art. 11, I, da LGPD) visa restituir ao cidadão a sua capacidade de autodeterminação informativa. Mais importante ainda, o art. 20 da LGPD consagra ao titular dos dados o direito de

solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses, incluindo a definição de seu perfil pessoal, profissional ou de crédito.

Esta garantia assegura que a autonomia privada e a dignidade humana não sejam substituídas pela frieza dos algoritmos e pelo determinismo matemático das big techs, resgatando a pessoa natural como o verdadeiro fim de todo o ordenamento jurídico.

3 A CRISE DO CONSENTIMENTO E A RESPONSABILIDADE PROATIVA

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) consagrou o consentimento como uma de suas bases legais (art. 7º, I), definido como a manifestação livre, informada e inequívoca do titular (art. 5º, XII).

Ocorre que essa premissa normativa, historicamente calcada no princípio da autodeterminação informacional (consolidado desde a decisão do Tribunal Constitucional Alemão de 1983), pressupõe um indivíduo plenamente racional e capaz de rastrear o fluxo de suas informações. Contudo, a evolução do "capitalismo de vigilância" demonstrou que essa expectativa constitui uma profunda ficção legal.

O fluxo informacional contemporâneo envolve uma rede “labiríntica” de atores, como os “data brokers” e as ferramentas de “cross-tracking”, que operam invisivelmente para agregar dados e formar perfis comportamentais precisos (BIONI, 2019).

Exigir que o titular exerça controle genuíno sobre essa engrenagem ignora as evidências da "racionalidade limitada", teoria que postula que as habilidades cognitivas do ser humano são restritas, impedindo-o de processar e memorizar a vastidão de variáveis contidas nas complexas políticas de privacidade. Soma-se a isso a "teoria prospectiva" e o modelo da utilidade subjetiva, que revelam uma idiossincrasia cognitiva fundamental, pois o indivíduo tende a supervalorizar o benefício imediato (como o acesso a um aplicativo ou serviço digital) e subestimar a perda mediata (a mitigação de sua privacidade a longo prazo) (BIONI, 2019).

É nesse cenário que surge o chamado "paradoxo da privacidade", onde embora as pessoas declarem valorizar intensamente a proteção de seus dados, suas condutas práticas no ambiente digital contradizem essa valoração, resultando em uma atitude de resignação diante do poder das plataformas (BIONI, 2019). A rigor, não há um paradoxo de escolhas livres, mas uma submissão inevitável à lógica predatória da economia de dados.

A tradicional vigilância estruturada em moldes panópticos e centralizados deu lugar, na atualidade, a uma "vigilância líquida" e distribuída. Os dados são continuamente absorvidos por múltiplos sensores e atores econômicos que transformam o comportamento humano em mercadoria.

Essa arquitetura instaura uma hipervulnerabilidade do usuário que transcende questões de hipossuficiência técnica ou etária, configurando-se como uma vulnerabilidade objetiva decorrente da própria inserção do sujeito no mercado informacional. A assimetria de poder não se dá apenas pela

disparidade econômica, mas pela opacidade dos algoritmos e pela impossibilidade de o titular prever os desdobramentos dos processos de "datificação".

Trata-se, portanto, de uma hipervulnerabilidade estrutural, na qual a exigência do consentimento atua muito mais como um mecanismo de legitimação (e exculpação) para a indústria de dados do que como uma ferramenta real de empoderamento cidadão.

Na prática, a autodeterminação informacional tem sido reduzida à contratualização da privacidade mediante a adesão massificada a Termos de Uso extensos. Instala-se a lógica coercitiva do "tudo ou nada", em que o usuário se vê diante da falsa escolha de aceitar integralmente a extração de seus dados ou ser sumariamente excluído da vida digital e do convívio social mediado pelas plataformas (BIONI, 2019).

Karine Mota defende que o aprofundamento dessa crise ocorre ao transpor os institutos do Código Civil para a esfera digital, demonstrando que a obtenção de dados pessoais frequentemente ocorre mediante a configuração de vícios de consentimento. O mercado utiliza interfaces enganosas, conhecidas como “dark patterns” (padrões escuros), cujo design é arquitetado para manipular o comportamento e induzir o usuário a fornecer consentimento de forma automatizada e acrítica (MOTA, 2025).

Sob a ótica civilista, a ocultação da real finalidade do tratamento configura dolo, ao passo que o uso de “paywalls”, nome dado a muros de pagamento que condicionam o acesso à entrega de dados, ou de “pop-ups” alarmistas que ameaçam a exclusão do usuário da rede podem consubstanciar formas modernas de coação moral (MOTA, 2025).

Sendo a manifestação de vontade eivada de erro, dolo ou coação, o consentimento torna-se viciado, ferindo frontalmente os preceitos de validade dos negócios jurídicos previstos no Código Civil e, por conseguinte, a própria essência da LGPD, que exige anuência livre e inequívoca.

Com isso, temos que a vulneração da liberdade do consentimento atinge seu grau máximo nos modelos de negócios baseados em privacidade como produto. Essa dinâmica ocorre quando o controlador condiciona a entrega de vantagens econômicas (brindes, descontos em farmácias, acesso a conteúdos) ao fornecimento de dados pessoais do titular.

Nesse contexto, o consentimento perde completamente a sua característica de "liberdade". A recusa em consentir passa a operar em desfavor econômico imediato do titular, que se vê obrigado a pagar valores superiores por produtos essenciais, como medicamentos, penalizando severamente, em especial, as classes de menor poder aquisitivo (MARTINS, 2020).

Além disso, aponta-se um entrave jurídico insuperável nessa modalidade que é a inviabilidade da revogação do consentimento. A LGPD (art. 8º, § 5º) assegura ao titular o direito irrenunciável de revogar sua anuência a qualquer tempo, de forma gratuita e facilitada

Contudo, nas relações em que a privacidade é o produto, após o titular ter recebido o desconto ou o brinde físico, o controlador perde o interesse em permitir a revogação, visto que a "troca" já se consumou no mercado. Isso demonstra que utilizar o consentimento para maquiar permutas de dados por vantagens comerciais fere o espírito da lei, exigindo que as corporações busquem outras bases legais, se houver adequação.

Diante do colapso do consentimento individual, a doutrina socorre-se da teoria da "Privacidade Contextual" (“Privacy in Context”), desenvolvida por Helen Nissenbaum. Nissenbaum rechaça a ideia de que a privacidade significa apenas isolamento ou controle subjetivo absoluto, postulando que a proteção se baseia na garantia de que a informação "flua apropriadamente". A integridade desse fluxo é governada pelas normas informacionais inerentes a cada contexto social específico, por exemplo, médico, educacional, comercial ou político. (NISSENBAUM, 2010).

Mesmo havendo um suposto consentimento, se os dados de saúde de um paciente forem cruzados e transferidos para uma seguradora ou agência de publicidade para a formação de um perfil de risco e discriminação de preços, haverá quebra intolerável da integridade contextual e violação da "legítima expectativa" do titular. Estabelece-se, aqui, o conceito de um "dirigismo informacional", semelhante ao dirigismo contratual do século XX, que limita a autonomia da vontade em prol da dignidade da pessoa humana, impedindo que o titular dos dados se coisifique ao assentir com a mercantilização total de sua biografia digital (BIONI, 2019).

A exigência de um "consentimento granular" e específico busca impedir o alargamento furtivo das finalidades iniciais de coleta. Reconhecendo as falhas profundas do consentimento, a LGPD desloca o eixo de gravidade da tutela jurídica do indivíduo hipervulnerável para o agente de tratamento.

Maria Celina Bodin de Moraes explica que a legislação inaugurou o regime especial de "responsabilização e prestação de contas" (“accountability”), previsto no art. 6º, inciso X, no qual "não descumprir a lei não é mais suficiente; é preciso proativamente prevenir a ocorrência de danos" (MORAES, 2019).

O sistema de responsabilidade civil da era digital abandona a lógica reativa de apenas compensar danos consumados, cujo nexo causal algorítmico é de dificílima comprovação para a vítima, passando a sancionar o próprio desrespeito aos deveres preventivos. As empresas são obrigadas a incorporar a privacidade desde a concepção na base de suas arquiteturas tecnológicas, devendo o ordenamento estimular a adoção de tecnologias de facilitação da privacidade (“PETs - Privacy Enhancing Technologies”), garantindo nativamente a minimização e a anonimização de dados como padrão normativo (BIONI, 2019).

Por fim, todo esse denso arcabouço sucumbe se não encontrar proteção em um sistema processual condizente. O processo individual é impotente contra “big techs” e práticas de

discriminação algorítmica disseminadas nas relações de massa (DIDIER JR., 2016). É imprescindível fortalecer o Direito Processual Coletivo para impor limites estruturais ao mercado de dados.

Decisões judiciais estruturantes requeridas por legitimados estruturados como o Ministério Público e a Defensoria Pública são o mecanismo necessário para obrigar corporações a modificarem seus sistemas opacos e algoritmos tendenciosos, garantindo um devido processo legal coletivo e a reparação integral dos direitos individuais homogêneos lesados em megavazamentos ou abusos de consentimento.

4 O ACESSO À JUSTIÇA E A TUTELA COLETIVA NO PROCESSO CIVIL

O processo civil clássico, forjado sob um viés puramente individualista e patrimonial, revela-se estruturalmente insuficiente para lidar com as lesões transindividuais características da sociedade da informação, como os vazamentos de dados ou a discriminação algorítmica em larga escala.

Fredie Didier Jr. leciona que a tutela de litígios de massa exige a adaptação de institutos processuais basilares como a legitimidade ativa, a competência e a coisa julgada para garantir a universalidade da jurisdição e o efetivo acesso à ordem jurídica justa. A tutela individual mostra-se incapaz de inibir as condutas ilícitas de megacorporações tecnológicas, uma vez que a microlesão sofrida individualmente muitas vezes não justifica o custo e o desgaste de uma demanda judicial solitária, favorecendo a impunidade do ofensor e a fragmentação das decisões (DIDIER JR, 2016).

Para superar essa barreira, o direito brasileiro desenvolveu um autêntico "microssistema de processo coletivo", cujo núcleo é formado pela Lei da Ação Civil Pública (LACP – Lei nº 7.347/1985) e pelo Título III do Código de Defesa do Consumidor (CDC – Lei nº 8.078/1990).

É a integração destes diplomas que fornece o arcabouço processual adequado para que as normas materiais da Lei Geral de Proteção de Dados (LGPD) saiam do papel. A própria LGPD prevê expressamente a tutela coletiva dos dados pessoais em seus arts. 22 e 42, §3º, permitindo o ajuizamento de ações para responsabilização por danos patrimoniais e morais, sejam eles de natureza individual ou coletiva.

O ordenamento jurídico brasileiro, desta forma, utiliza os conceitos estabelecidos no art. 81, parágrafo único, do CDC para classificar os direitos tuteláveis coletivamente em três espécies, quais sejam difusos, coletivos em sentido estrito e individuais homogêneos.

No contexto da proteção de dados pessoais, um mesmo vazamento ou tratamento inadequado de dados pode ofender simultaneamente as três categorias, dependendo da tutela jurisdicional pretendida (ROQUE, 2019).

Os direitos difusos são aqueles de natureza indivisível, titularizados por pessoas indeterminadas e ligadas por circunstâncias de fato. Na seara da LGPD, isso ocorre, por exemplo,

quando se postula uma obrigação de fazer ou não fazer contra uma autoridade pública ou rede social para cessar uma política geral de mineração obscura de dados que afeta toda a sociedade.

Os direitos coletivos em sentido estrito, por sua vez, também são indivisíveis, mas pertencem a um grupo, categoria ou classe ligada por uma relação jurídica base prévia. Seria o caso de um sindicato ajuizando ação contra uma empresa para que ela adeque os sistemas de inteligência artificial e proteção de dados referentes aos seus empregados (ROQUE, 2019).

Para além dos direitos essencialmente coletivos, a tutela dos dados pessoais ganha contornos de altíssima relevância no campo dos interesses individuais homogêneos. Para o jurista e ex-Ministro do Supremo Tribunal Federal Teori Albino Zavascki, os direitos individuais homogêneos são, na essência, direitos subjetivos individuais divisíveis que, por terem uma "origem comum", recebem tratamento processual molecular para otimizar a prestação jurisdicional e evitar decisões conflitantes (ZAVASCKI, 2017).

Segundo Zavascki, a tutela coletiva desses direitos estrutura-se em um modelo bifásico. Na primeira fase, consubstanciada no processo de conhecimento da ação coletiva, a atividade cognitiva do juiz limita-se ao "núcleo de homogeneidade" da lesão, ou seja, decide-se se há o dever de indenizar (“an debeatur”), o que é devido (“quid debeatur”) e quem é o responsável (“quis debeat”). O resultado, em caso de procedência, é uma sentença condenatória genérica, conforme possibilita o artigo 95 do CDC) (ZAVASCKI, 2017).

No caso de megavazamentos de dados, como exposição de CPFs, senhas e cartões de crédito, a sentença genérica atestará a falha de segurança da empresa. A segunda fase consiste na liquidação e execução individual, em que cada vítima demonstrará a sua "margem de heterogeneidade", provando ser titular do direito e a extensão do seu dano particular (ZAVASCKI, 2017).

Contudo, Fredie Didier Jr. alerta para uma terceira fase essencial ao processo coletivo que é a reparação fluida (“fluid recovery”). Caso as vítimas do vazamento de dados não se habilitem em número compatível com a gravidade do dano, o que é comum nas microlesões digitais, os legitimados coletivos deverão promover a execução do valor residual, que será revertido ao Fundo de Defesa dos Direitos Difusos, conforme comando do art. 100 do CDC (DIDIER JR, 2016).

Essa medida garante que o ofensor não retenha o lucro ilícito extraído do tratamento indevido de dados e concretiza o caráter repressivo e pedagógico da responsabilidade civil (NEVES, 2018).

Para que todo esse maquinário processe as violações à LGPD sem ferir preceitos constitucionais, o Ministério Público, a Defensoria Pública e as associações civis assumem forte protagonismo. Porém, deve-se assegurar um devido processo legal coletivo. Isso porque, o processo coletivo não pode significar a simples exclusão dos titulares do direito da lide sob o pretexto de conveniência processual. O devido processo legal coletivo exige a verificação rigorosa da "representatividade adequada" do ente legitimado (VITORELLI, 2020).

A doutrina propõe uma teoria unificada dos litígios coletivos, abandonando as abstrações teóricas tradicionais para focar no grau de conflituosidade e complexidade do caso concreto. Para ele, litígios envolvendo proteção de dados podem configurar litígios de "difusão irradiada", caracterizados por alta complexidade e pela existência de múltiplos subgrupos com interesses muitas vezes contrapostos.

Nesses litígios, a decisão judicial não pode ser pautada exclusivamente pela visão do legitimado extraordinário, por exemplo o Ministério Público ou uma associação. Exige-se que o juiz promova o contraditório participativo e assegure que a voz da coletividade afetada seja ouvida por meio de mecanismos democráticos, como as audiências públicas e a admissão de “amici curiae”.

Por fim, a simples condenação pecuniária frequentemente falha em resolver o problema crônico do "capitalismo de vigilância". A falta de aplicação contínua da LGPD pelas “big techs” e pela Administração Pública configura um problema sistêmico que clama por soluções que vão além da responsabilidade civil clássica.

André Roque destaca a utilidade das decisões estruturantes no processo civil contemporâneo. As ações coletivas fundadas na LGPD podem envolver pleitos para que os controladores de dados alterem integralmente a arquitetura de seus sistemas de segurança, promovam a anonimização massiva de bases de dados ou corrijam vieses algorítmicos discriminatórios (ROQUE, 2019).

Tais medidas exigem do Poder Judiciário uma postura voltada para o modelo de reparação, com decisões flexíveis, prospectivas e acompanhadas de planos de transição.

Desse modo, a tutela coletiva converte-se no instrumento mais poderoso e adequado para readequar o comportamento das organizações aos ditames de proteção da personalidade e autodeterminação informativa no ambiente virtual.

5 PESQUISA JURISPRUDENCIAL

O entendimento dos tribunais superiores tem acompanhado a evolução doutrinária sobre a personalidade, a proteção de dados e a tutela coletiva. A jurisprudência vem consolidando a tese de que as antigas categorias do processo civil clássico precisam ser redimensionadas para fazer frente aos desafios da sociedade informacional.

Após pesquisa, buscou-se trazer alguns precedentes históricos de destaque para comparação com decisões mais recentes sobre o tema, com o intuito de ilustrar esta evolução jurisprudencial.

No plano do direito comparado, o ponto fixo de referência e fonte da matéria é a decisão do Tribunal Constitucional Federal da Alemanha, proferida em 15 de dezembro de 1983. Na ocasião, a Corte suspendeu a execução de uma lei de recenseamento populacional sob o argumento de que a coleta estatal de dados cruzados, sem finalidade estatística rígida, ameaçava o livre desenvolvimento da personalidade.

O tribunal cunhou o termo "direito à autodeterminação informativa", estabelecendo que não existem "dados insignificantes" sob as condições modernas do processamento automático (DONEDA, 2019).

A decisão rompeu com a noção de que a privacidade seria apenas o sigilo, garantindo o direito do indivíduo de controlar, em princípio, a obtenção, o tratamento e a transmissão de informações relativas à sua pessoa, marco este que influenciou globalmente a jurisprudência e a criação da LGPD (BIONI, 2019).

No cenário nacional, o processo coletivo dependia da superação de um obstáculo hermenêutico, eu estava em como justificar a atuação do Ministério Público na defesa de dados pessoais, que são, em regra, direitos individuais e disponíveis. A resposta foi consolidada no Supremo Tribunal Federal no julgamento do RE 631.111/GO (Relator Min. Teori Zavascki, julgado em 07/08/2014, com Repercussão Geral) (ZAVASCKI, 2014).

Neste precedente, que originariamente tratava do seguro DPVAT, o STF entendeu que os direitos individuais homogêneos são direitos subjetivos divisíveis, de origem comum. Contudo, o Ministro Teori Zavascki destacou que, quando a ofensa a esses direitos ganha uma "dimensão ampliada" e atinge um número expressivo de titulares, o que é uma situação típica de falhas de segurança e vazamentos massivos de dados, a lesão transcende a esfera individual e passa a comprometer institutos e valores jurídicos superiores da comunidade.

Configura-se, assim, um "interesse social qualificado", o que atrai a legitimidade ativa do Ministério Público (art. 127 da CF) para propor ação civil coletiva buscando a condenação genérica do ofensor (ZAVASCKI, 2017). Esta tese jurídica ampara diretamente a judicialização contra megacorporações de tecnologia ou seja, as “big techs”.

De igual modo, a jurisprudência avançou para garantir o acesso à justiça aos chamados hipervulneráveis digitais por meio da Defensoria Pública. O STF, ao julgar a ADI 3.943 (Relatora Min. Cármen Lúcia, julgada em 07/05/2015), reconheceu a constitucionalidade da Lei nº 11.448/2007, fixando a legitimidade irrestrita da Defensoria para propor ações civis públicas (PINHO, 2020).

A consolidação se deu no julgamento do RE 733.433/MG (Relator Min. Dias Toffoli, DJe 07/04/2016, Repercussão Geral), no qual o STF determinou que a expressão "necessitados", prevista no art. 134 da Constituição Federal, não abrange apenas os carentes de recursos financeiros, mas inclui os hipervulneráveis e os necessitados organizacionais (LORDELO, 2018).

Nas relações digitais, em que o titular dos dados é submetido a algoritmos predatórios e a contratos de adesão inflexíveis, o usuário se encontra em estado de vulnerabilidade organizacional e informacional, legitimando a Defensoria Pública a atuar molecularmente na defesa de seus direitos de personalidade (PINHO, 2020).

Na esfera do Superior Tribunal de Justiça (STJ), a jurisprudência também já vinha balizando as práticas de formação de perfis, como observado no julgamento do REsp 1.419.697/RS (Relator Min. Paulo de Tarso Sanseverino) sobre os sistemas de "Credit Scoring" (BIONI, 2019).

A Corte reconheceu a licitude da avaliação de risco de crédito por algoritmos, contudo, impôs severos limites garantistas baseados no respeito à privacidade do consumidor e na necessidade de transparência e clareza dos critérios do algoritmo. Esta decisão dialoga umbilicalmente com o atual art. 20 da LGPD, que prevê o direito do titular à revisão de decisões unicamente automatizadas e à explicação sobre os métodos que formam o seu perfil, a fim de impedir a discriminação ilícita.

Com a vigência plena da LGPD, a jurisprudência passou a enfrentar incidentes reais de violação dos direitos da personalidade na rede. A doutrina e os veículos jurídicos catalogam as primeiras e mais emblemáticas condenações, e processos em trâmite, pelo uso indevido e vazamento de dados no Brasil, como sendo as do "Caso Cyrela", o "Caso das operadoras de telefonia", o megavazamento de dados de consumidores, e a Ação Civil Pública pelo "vazamento do SUS".

No "Caso Cyrela" a Construtora Cyrela foi a primeira empresa brasileira a ser condenada na Justiça por compartilhamento indevido de dados pessoais. O cliente que comprou um apartamento passou a ser assediado por instituições financeiras e de decoração sem o seu consentimento. A juíza determinou a condenação por danos morais no valor de R$ 10.000,00, além de multa cominatória em caso de novos repasses, sob o fundamento de que a conduta feriu a LGPD e violou a honra, a privacidade e a intimidade do consumidor (BEZERRA, 2023).

No "Caso das operadoras de telefonia", o Tribunal de Justiça do Distrito Federal e Territórios manteve a condenação de grandes operadoras de telefonia (Vivo e Claro) pelo vazamento massivo de informações de clientes, como CPFs e endereços. A decisão determinou que as empresas paguem pesada indenização por danos morais coletivos pela exposição vulnerabilizante dos consumidores (BEZERRA, 2023).

Sobre o megavazamento de dados de consumidores, estima-se que pelo menos 223 milhões de brasileiros tiveram seus dados vazados. Fato notório ocorrido em 2021, que expôs um banco de dados contendo CPFs, imagens faciais e dados de praticamente toda a população do país, inclusive de pessoas falecidas, demonstrando a extrema fragilidade da custódia das informações no país, evidenciando o perigo da sociedade da hipervigilância (BEZERRA, 2023).

Também é possível citar a condenação do INSS pela ANPD. Tanto na via administrativa como na processual, a própria Autoridade Nacional de Proteção de Dados (ANPD) iniciou a sua fase sancionatória. A Autarquia proferiu condenação contra o Instituto Nacional do Seguro Social (INSS) pelo vazamento de dados sensíveis de milhares de beneficiários, exigindo providências corretivas e comprovação de relatórios de impacto de proteção de dados.

Por fim, outro caso emblemático foi a Ação Civil Pública para indenização por vazamentos no SUS e Auxílio Brasil promovida pelo Ministério Público Federal. A Justiça, mediante ação civil, determinou o pagamento de indenização de R$ 15 mil de danos morais individuais a cidadãos que tiveram informações íntimas, dados de saúde (SUS) e renda vazados sob a custódia do Estado. A decisão ratificou a responsabilidade estatal pelas falhas gravíssimas na segurança da informação à luz da LGPD

6 SUGESTÕES DE MELHORIA DO SISTEMA LEGISLADO E PROJETOS EM TRÂMITE

Embora o Brasil conte com a Lei da Ação Civil Pública (LACP) e o CDC, o microssistema de processo coletivo encontra-se fragmentado. O presente estudo propõe algumas melhorias, sendo a primeira a aprovação de um Código de Processo Coletivo, explica-se: Existem propostas históricas e Projetos de Lei que visam unificar o processo coletivo. A principal sugestão é a incorporação do sistema de exclusão voluntária, típico das "class actions" norte-americanas, em contraposição ao modelo atual, que mitiga os efeitos secundários para quem propõe ação individual. Esse sistema vincularia todos os titulares afetados por um vazamento, garantindo economia processual.

Outra melhoria que se sugere é a institucionalização Processual das PETs ("Privacy Enhancing Technologies"). Nesses casos a legislação processual deve prever mecanismos coercitivos atípicos, conforme garante o artigo 139, IV, do CPC, que obriguem empresas infratoras a implementarem tecnologias de anonimização (BIONI, 2019).

Por fim, a ampliação dos danos morais coletivos, pode ser uma melhoria palpável, já que uma alteração legislativa na LACP para parametrizar de forma objetiva a reparação fluida em casos de infração à LGPD, destinando os recursos para o Fundo de Defesa dos Direitos Difusos com aplicação em letramento digital, está ao alcance de uma alteração de lei ordinária, mais acessível do que alterações constitucionais.

7 CONCLUSÃO

A presente pesquisa demonstrou que a tutela dos direitos da personalidade na era digital transcende as categorias clássicas do direito civil. A conversão dos dados pessoais em extensões da própria identidade humana inseriu o indivíduo em um mercado marcado pela opacidade algorítmica e pela exploração comercial contínua, consolidando um estado de hipervulnerabilidade estrutural perante a economia de vigilância.

Ficou evidenciado que o modelo de proteção alicerçado exclusivamente na figura do consentimento entrou em colapso dogmático e prático. Diante da severa assimetria informacional, do uso de interfaces manipuladoras e da imposição de políticas contratuais inflexíveis, a manifestação de vontade do titular transmudou-se em uma ficção legal. Para contornar essa falência, conclui-se que o

ordenamento jurídico deve efetivar a transição para o regime da responsabilidade proativa, exigindo que os agentes de tratamento incorporem a privacidade desde a concepção de suas arquiteturas tecnológicas.

Nesse cenário de microlesões disseminadas e danos massivos, o estudo constatou que a jurisdição civil individual revela-se materialmente impotente. A efetividade das garantias materiais consagradas na Lei Geral de Proteção de Dados pressupõe, inexoravelmente, a instrumentalização do microssistema de processo coletivo. As ações coletivas, quando manejadas pelos legitimados adequados, despontam como o único meio capaz de equalizar forças contra as grandes corporações de tecnologia. Mais do que a mera reparação pecuniária, o devido processo legal coletivo viabiliza a prolação de decisões estruturantes, capazes de impor readequações sistêmicas na forma como as empresas e o Estado tratam os dados dos cidadãos.

A análise da evolução jurisprudencial ratifica que os tribunais superiores brasileiros já caminham para o reconhecimento da dimensão molecular desses litígios informacionais. Contudo, para que o arcabouço processual alcance sua plenitude, apontou-se a necessidade de reformas legislativas pontuais, como a aprovação de um Código de Processo Coletivo unificado, a adoção do sistema de exclusão voluntária e a parametrização objetiva da reparação fluida, garantindo que o lucro ilícito extraído da exploração de dados seja revertido para a coletividade.

Em suma, a defesa da autodeterminação informativa no ambiente virtual não constitui um obstáculo à inovação tecnológica, mas o resgate da pessoa humana como o fim último do ordenamento jurídico. A afirmação do direito à proteção de dados depende de uma hermenêutica processual arrojada e coletivizada, apta a impedir que a autonomia privada e a dignidade humana sejam suplantadas pelo determinismo dos algoritmos.

REFERÊNCIAS

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

DIDIER JR., Fredie; ZANETI JR., Hermes. **Curso de direito processual civil**: processo coletivo. 9. ed. Salvador: Juspodivm, 2014.

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

FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade. **JOTA**, São Paulo, 2018. Disponível em: [inserir link da publicação]. Acesso em: 27 abr. 2026.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. 2. ed. São Paulo: Revista dos Tribunais, 2014.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc (ed.). **Technology and privacy**: the new landscape. Cambridge: MIT Press, 1997. p. 219-241.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito "proativo". **Civilistica.com**, Rio de Janeiro, a. 8, n. 3, p. 1-15, 2019.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

PERLINGIERI, Pietro. **Perfis de direito civil**: introdução ao direito civil constitucional. Tradução de Maria Cristina De Cicco. Rio de Janeiro: Renovar, 1999.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda. Rio de Janeiro: Renovar, 2008.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *In*: TEPEDINO, Gustavo. **Temas de direito civil**. 4. ed. Rio de Janeiro: Renovar, 2008. p. [inserir intervalo de páginas].

VITORELLI, Edilson. **O devido processo legal coletivo**: dos direitos aos litígios. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

WESTIN, Alan F. **Privacy and freedom**. New York: Atheneum, 1970.

ZAVASCKI, Teori Albino. **Processo coletivo**: tutela de direitos coletivos e tutela coletiva de direitos. 7. ed. São Paulo: Revista dos Tribunais, 2017.