Revista ARACÊ
ISSN: 2358-2472

CAPITALISMO DE VIGILÂNCIA, DIREITOS FUNDAMENTAIS E A TUTELA CONSTITUCIONAL DA PROTEÇÃO DE DADOS NO BRASIL

https://doi.org/10.56238/arev7n5-053

Data de submissão: 04/04/2025 **Data de publicação:** 04/05/2025

Vinícius Teixeira Bressan
Advogado e Procurador Municipal de Matinhos/PR. Graduado em direito pela Universidade Federal do Paraná (UFPR). Especialista em Direito Aplicado pela Escola da Magistratura do Estado do Paraná (EMAP-PR). Especialista em Licitações e Contratos Administrativos pela Pontifícia Universidade Católica do Paraná (PUC-PR). Mestrando em Direito pelo Centro Universitário Internacional (PPGD-UNINTER), sob orientação do Professor Doutor Daniel Ferreira.
E-mail: viniciustbressan@gmail.com

Jailson de Souza Araujo
Doutor em Direito Econômico e Socioambiental pela PUC/PR. Professor permanente do Mestrado em Direito do Centro Universitário Internacional – PPGD-UNINTER. Advogado.
E-mail: araujoadv@yahoo.com.br

RESUMO
O presente artigo é destinado a analisar, sob um viés abrangente, a tutela constitucional da proteção de dados no Brasil. Busca-se demonstrar que popularização da internet vem sendo permeada pelo monitorados constantemente e camuflado dos usuários, o que não só vulnera o direito à privacidade como também prejudica o direito à autodeterminação. A partir de uma abordagem hipotético-dedutiva lastreada no método da revisão bibliográfica, o estudo trata da insuficiência da tutela legislativa pretérita à edição da Lei n.º 13.709/2018, e das conjunturas fáticas que tornaram necessária uma normatização específica da matéria. Ademais, sob enfoque da constitucionalização do direito civil, são traçados os principais mecanismos de proteção criados pela Lei Geral de Proteção de Dados, e os meios de fiscalização e de punição de eventuais incidentes envolvendo o tratamento de dados pessoais. Com base na análise empreendida, demonstra-se que a LGPD é baseada na concepção expansionista de dados pessoais, e que perfaz instrumento apto a resguardar a intimidade no ambiente virtual e a refrear a estigmatização do usuário das redes. Por fim, trata-se do papel central da Agência Nacional de Proteção de Dados do Poder Judiciário na aplicação de sanções aos agentes de tratamento, com vistas à concretização deste importante direito fundamental, que é diretamente ligado à salvaguarda da Dignidade Humana.

Palavras-chave: Capitalismo de Vigilância. Direito Digital. Lei Geral de Proteção de Dados Pessoais. Novas Tecnologias da Informação e Comunicação. Privacidade de Dados.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

O presente artigo trata da tutela constitucional da proteção de dados no Brasil, sob o enfoque das contingências fáticas que ensejaram a normatização específica da matéria, e da insuficiência da tutela legislativa que precedeu a edição da Lei n.º 13.709/2018 - e a posterior enunciação de previsão constitucional específica a respeito do tema. Diante disto, o estudo visa a demonstrar os principais instrumentos de proteção disciplinados pela Lei Geral de Proteção de Dados (LGPD), e a importância concreta desta na salvaguarda da Dignidade Humana no contexto virtual.

Ademais, a reflexão trazida permeia o papel da Autoridade Nacional de Proteção de Dados (ANPD) na regulamentação das atividades de tratamento de dados e na aplicação de sanções aos agentes de tratamento, assim como a importância de uma atuação enérgica do Poder Judiciário na responsabilização civil relacionada à violação de dados, como forma de dissuadir comportamentos irregulares dos agentes de tratamento.

O trabalho é baseado no método hipotético-dedutiva, e foi desenvolvido através da revisão bibliográfica – notadamente, de artigos científicos atuais que foram publicados sobre a matéria. Através do estudo, pretende-se traçar uma análise abrangente a respeito do tema, que abarque desde os antecedentes normativos e fáticos que ensejaram a edição da LGPD [e a enunciação constitucional do direito à proteção de dados pessoais], os ganhos dela decorrentes em matéria de concretização de direitos fundamentais, e a necessidade de responsabilização efetiva dos responsáveis pelo tratamento inadequado de dados pessoais, para que os preceitos legais e constitucionais sejam efetivamente materializados pelos agentes de tratamento.

Neste desiderato, busca-se contextualizar o leitor quanto cenário de hipervigilância digital dos usuários no contexto virtual, que é uma das principais marcas das práticas do capitalismo hodierno, o capitalismo de vigilância - termo utilizado por Lucca e Martins (2024) para se referir às campanhas promocionais promovidas através da coleta massiva de dados nos sítios eletrônicos. Trata-se da face oculta das muitas das facilidades advindas da popularização da internet, que ensejou a edição da Lei n.º 13.709/2018 e da Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, que incluiu o inciso LXXIX ao artigo 5º da Constituição Federal, resguardando à proteção de dados pessoais status de direito fundamental autônomo.

Ademais, abordam-se algumas das iniciativas legais pretéritas à Lei Geral de Proteção de Dados (LGPD) que salvaguardavam, ainda que de maneira tímida, a tutela dos dados dos usuários de internet no Brasil, sob o enfoque da necessidade da edição de lei específica para tratar do tema. Adiante, é traçado um panorama geral da proteção enunciada pela LGPD, que é permeado pela análise dos principais mecanismos de proteção destinados a resguardar os direitos dos titulares de dados pessoais

Revista ARACÊ
ISSN: 2358-2472

no Brasil, a sua abrangência, a centralidade do consentimento do usuário e as nuanças da hipótese de tratamento de dados baseada no legítimo interesse - tudo sob o enfoque da constitucionalização do direito e do papel da Lei Geral na promoção de direitos fundamentais. Ato contínuo, são enunciados exemplos práticos de aplicação das normas de proteção de dados ao âmbito das relações de trabalho, de forma a resguardar que o artigo não se limite ao plano puramente teórico.

No último capítulo, aborda-se a disciplina sancionatória enunciada pela Lei n.º 13.709/2018. Para tanto, discorre-se sobre o papel da Autoridade Nacional de Proteção de Dados (ANPD) na aplicação de sanções aos agentes de tratamento e sobre os principais contornos da responsabilidade civil por violação às regras de proteção de dados, sob o viés da facilitação da defesa do titular e da importância da punição efetiva das irregularidades cometidas no tratamento de dados pessoais, como meio de compelir os agentes de tratamento a respeitar as normas existentes.

2 MONITORAMENTO DE DADOS, PERFILAMENTO E VULNERABILIDADE DIGITAL NO CAPITALISMO DE VIGILÂNCIA

O acesso à internet foi reconhecido como direito humano pela ONU, na medida em que possibilita o amplo exercício da liberdade de expressão. A salvaguarda desta exige, porém, a criação de mecanismos aptos a compatibilizar este direito fundamental com a proteção à intimidade, à vida privada, à honra, à imagem e à proteção de dados pessoais (Ribeiro, 2022), sob pena de as plataformas digitais se tornarem instrumentos de violação de direitos humanos.

É inegável que o avanço tecnológico é capaz de proporcionar graus de comodidade outrora inimagináveis. Contudo, é fato que muitas das facilidades que atualmente são atribuídas à inteligência artificial e aos modernos algoritmos são fruto da combinação de dados [muitas vezes sensíveis], que permitem aos dispositivos informáticos traçar padrões de comportamento, interesses e tendências do usuário. A manipulação de informações pessoais encarta um risco, quase sempre oculto, de vazamento de dados e de violação à privacidade e à honra, o que exige uma tutela legal assertiva, que seja capaz de compatibilizar o desenvolvimento tecnológico com a garantia de direitos fundamentais (Andréa, Arquite e Camargo, 2020).

Vivemos em meio ao capitalismo de vigilância - termo utilizado por Lucca e Martins (2024) para se referir às campanhas promocionais promovidas através da coleta massiva de dados nos sítios eletrônicos. Esta se dá para fins de traçar perfis de personalidade e de consumo, e de induzir comportamentos – especialmente para que haja maior efetividade em estratégias comerciais. Neste contexto, a disponibilidade de informações sobre as preferências dos consumidores se tornou um importante ativo empresarial (Oliveira, 2018). O chamado *marketing* comportamental perfaz um

Revista ARACÊ
ISSN: 2358-2472

método de publicidade assertivo, que é baseado na formação do perfil individual de consumo de cada usuário da rede, e é obtido através da combinação de dados coletados durante as interações realizadas no âmbito virtual (Verbicaro e Calandrini, 2022).

A arregimentação de dados se dá por meio do acesso a aplicativos gratuitos, da atuação nas redes sociais, da realização de pesquisas e de cadastros virtuais ou, no campo da ilicitude, por meio de spam e de *spyware* (Cavet e Faleiros Júnior, 2024). Esta coleta pode até mesmo transcender o âmbito exclusivamente virtual, a exemplo da empresa administradora de uma linha de metrô de São Paulo que, em 2018, instalou sensores para coletar dados biométricos e reações dos passageiros em relação aos anúncios publicitários exibidos, para fins de criação de padrões anímicos relacionados ao tipo de anúncio e ao seu conteúdo - o que, vale dizer, ensejou a propositura de uma ação civil pública, em cujo bojo ordenou-se a retirada liminar dos equipamentos (Calabrich, 2020).

Uma vez acumulados, os dados são tratados e convertidos em padrões comportamentais e, posteriormente, são vendidos àquele dentre os interessados que estiver disposto a pagar uma quantia monetária maior pela informação - fato que enseja verdadeira objetificação do ser humano, e das suas experiências (Martins e Longhi, 2022).

Através de sequências de comandos pré-definidos, os programas informáticos são capazes de interpretar hábitos e registros para predizer comportamentos e tendências, e de criar uma representação virtual da pessoa humana. Com base nisto, não só os anúncios, mas também as informações que serão disponibilizadas ao usuário passam a ser ditadas por este parâmetro de preferências absorvido pela inteligência artificial. Isto, de forma inequívoca, prejudica a formação de um senso crítico do indivíduo, e o exercício do direito à autodeterminação informativa daquele que usa a internet (Lucca e Martins, 2024), fato que desperta especial preocupação quando se tratam de pessoas jovens, que tendem [ou, ao menos, tenderiam] a alterar substancialmente as suas convicções com a aquisição de maturidade.

Dito de outra forma, o direcionamento de informações e de anúncios publicitários lastreado no *marketing* comportamental acaba interferindo tanto na formação do pensamento crítico do indivíduo quanto nas decisões tomadas no mercado de consumo, que passam a ser norteadas por um reflexo digital da sua personalidade que é combinado com técnicas neurocientíficas de persuasão - que podem, em muitos casos, impedir que o cidadão realize escolhas de forma verdadeiramente livre e esclarecida (relegando o ser humano ao papel de mero coadjuvante dos seus processos de tomada de decisão). Também por envolver uma agressiva invasão à privacidade do usuário, o emprego do perfilamento para influenciar inconscientemente os consumidores a adquirir produtos e serviços exige especial preocupação na atual sociedade de consumo, que é permeada por transações comerciais que,

Revista ARACÊ
ISSN: 2358-2472

predominantemente, não são voltadas a suprir às necessidades pessoais, mas a atender anseios emocionais e desejos supérfluos que são próprios da era da informação (Cavet e Faleiros Júnior, 2024).

Em suma, na atualidade, a combinação de informações através de algoritmos molda as preferências de consumo, o tipo de informação que será apresentada durante a navegação eletrônica e o círculo de pessoas a serem conectadas no ambiente virtual, o que somente é possível em razão da coleta permanente de elevado volume de dados, e da combinação deles, para que sejam empregados nos mais variados desideratos comerciais. Tanto a disponibilidade de dados adquiriu especial valor comercial nos esteios do capitalismo de vigilância que empresas como a Meta e a Microsoft, cujas operações são centradas na coleta e no tratamento de dados pessoais, ostentam enorme valor comercial (Búrigo e Carloto, 2023).

Inobstante o elevado valor mercadológico dos dados pessoais, é fato que os usuários dificilmente compreendem as consequências do fornecimento de dados, e os riscos associados ao armazenamento e à manipulação deles. Amostra disto é o estudo desenvolvido pelo departamento de psicologia da Universidade de Cambrige, no qual se inferiu que 4/5 dos seus participantes franqueariam acesso a informações pessoais suas e dos seus amigos, inclusive indicando os respectivos endereços, em troca do reduzido valor de um dólar (Cavet e Faleiros Júnior, 2024).

O resultado é, porém, compreensível, já que os mecanismos de perfilamento digital envolvem uma realidade bastante nebulosa, em que os agentes econômicos [e o próprio Estado] detém informações amplas sobre os indivíduos, e estes desconhecem as operações realizadas a partir dos seus dados. Exemplo extremo, mas paradigmático de quanto os efeitos da hipervigilância digital podem ser nefastos, foi o desenvolvimento de um sistema pelo governo chinês, em 2018, para classificar os seus cidadãos de acordo com os seus comportamentos e, com base na pontuação atribuída, proibir a compra de passagens de avião e trem – o que permitiu que mais de vinte milhões de viagens fossem barradas até 2020 (Calabrich, 2020).

Diante disto, nota-se que o avanço da tecnologia não apenas proporcionou uma ampliação de acesso a informações e a reconfiguração das relações sociais e de trabalho, mas também eliminou as barreiras de comunicação, diluiu as fronteiras entre o espaço doméstico e o laboral, e exigiu a ressignificação do direito à intimidade e à privacidade, por exemplo (Sturmer e Miranda, 2023).

Considerando o elevado potencial de disseminação das informações nos meios virtuais, a tutela da privacidade, da imagem e da intimidade passou a estar imediatamente ligada à proteção de dados pessoais – em especial, dos dados sensíveis. Estes são os que guardam pertinência com as particularidades de determinada pessoa, que envolvam as suas preferências políticas, religiosas,

Revista ARACÊ
ISSN: 2358-2472

filosóficas, assim como questões relacionadas à saúde, à preferência sexual, que são temas diretamente ligados à esfera privada do ser humano (Andréa, Arquite e Camargo, 2020).

Reforçando a especial importância da proteção de dados, há que se considerar que, para além da sua relevância no que tange à garantia de direitos fundamentais, nem sempre os interesses do Estado e das empresas convergem com os de cada pessoa, ao menos no sentido individual (Calabrich, 2020), o que também tornou premente a normatização do processamento de dados no Brasil.

A necessidade de regulamentação específica da matéria, com o estabelecimento de exigências de padrões de segurança da informação, é evidenciada pelos vários exemplos de incidentes envolvendo vazamentos de dados ocorridos num passado bastante próximo.

Em 2016, houve vazamento de dados relacionados aos doadores de sangue da Austrália, que culminou na publicidade de registros internos afetos às pessoas com comportamento sexual de risco. Em 2017, descobriu-se que um equipamento erótico desenvolvido por uma empresa canadense, que se conectava ao celular, enviava dados em tempo real ao desenvolvedor acerca da sua forma de utilização (Lucca e Martins, 2024).

De igual forma, no ano de 2020, foram registrados diversos vazamentos de dados de pacientes do Sistema Único de Saúde, o que intensificou as discussões sobre a necessidade de aprimoramento dos meios de proteção de dados dos do Poder Público (Cerqueira, 2022).

Outro escândalo de vazamento de dados envolveu o fornecimento de informações de milhões de usuários da rede social *Facebook* para a empresa *Cambridge Analytica*, a partir do ano de 2014 - fato que pode ter sido crucial para influenciar eleitores, com base no estabelecimento dos seus perfis e preferências, e decisivo para a eleição do candidato Donald Trump, nos Estados Unidos da América, no ano de 2016 (Suzin e Aguiar, 2023).

Um acontecimento que, embora não perfaça um incidente de dados, provoca reflexões e evidencia a importância de regras claras que disciplinem a proteção de dados foi a predição da epidemia de gripe suína nos Estados Unidos da América pelos engenheiros da plataforma de pesquisa Google, com base na combinação de padrões de pesquisas realizadas por usuários, e no monitoramento de usuários (Lucca e Martins, 2024). Sem uma normatização adequada da matéria, a constatação poderia ter sido repassada, obviamente em segredo, para a indústria farmacêutica, o que poderia estimular comportamentos oportunistas como o encarecimento de medicamentos, dificultando, pois, o controle da doença (Martins e Longhi, 2022).

Reforçando a importância da tutela da proteção de dados, há que se ponderar que os algoritmos, enquanto sequências de comandos que devem ser executados no tratamento de informações, não são capazes de discernir parâmetros inadequados ou discriminatórios, tampouco de compreender com

Revista ARACÊ
ISSN: 2358-2472

exatidão os contextos - o que se exemplifica pelo robô desenvolvido pela Microsoft para interagir com os usuários de rede social, que precisou ser retirado do ar rapidamente, por ter normalizado o comportamento preconceituoso dos usuários (Calabrich, 2020).

Não se pode deixar de reconhecer que, antes da edição da Lei n.º 13.709/2018, outras leis resguardavam alguma salvaguarda, ainda que de maneira tangencial e genérica, aos dados dos usuários de internet. Neste sentido, por exemplo, o Código de Defesa do Consumidor já regulava os bancos de dados sobre consumidores, e a Lei n.º 12.414/11 (Lei do Cadastro Positivo) já disciplinava o tratamento de dados socioeconômicos para fins de concessão de crédito, enunciando o dever do operador de obter o consentimento do titular previamente ao repasse de dados a terceiros, e proibindo a coleta de informações desconexas com a finalidade visada, assim como o emprego destas para desiderato diverso do repassado ao titular. Da mesma forma, o chamado Marco Civil da Internet (Lei n.º 12.965/2014) normatizou, em 2014, a compatibilização do exercício da liberdade de expressão em meio digital com os direitos dos demais usuários da internet e, no âmbito penal, a Lei n.º 12.737 de 2012 criminalizou a invasão não consentida de dispositivos eletrônicos, após o vazamento de fotografias íntimas da atriz Carolina Dieckmann (Andréa, Arquite e Camargo, 2020).

Com a evolução tecnológica, o tratamento de dados se tornou cada vez mais complexo e suscetível à violação de direitos fundamentais, o que exigiu uma normatização específica do tema. Isto se deu com a aprovação da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), que tutela a coleta e o tratamento de dados pessoais por pessoas físicas e jurídicas, e que é fruto de intensos debates no Congresso Nacional, que foram permeados pela participação de representantes dos diversos setores interessados (Andréa, Arquite e Camargo, 2020).

Outro passo importante na proteção de dados pessoais foi a aprovação da Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, que incluiu o inciso LXXIX ao artigo 5º da Constituição Federal, resguardando à proteção de dados pessoais status de direito fundamental autônomo, conferindo competência legislativa privativa da União para tratar do tema e atribuindo a ela o papel de organizar e fiscalizar a proteção e o tratamento de dados (Cardoso, 2023).

Em suma, até a edição da LGPD e a aprovação da Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, "o direito à proteção de dados pessoais era visto como um desdobramento do direito à intimidade (...). Mas, apesar de se conceber este direito, não era dado o tratamento adequado, o que gerava margem a lacunas e deturpações" (Suzin e Aguiar, 2023).

É que, diante da constatação de que os dados pessoais passaram a ser coletados massivamente em meio à popularização da internet, inicialmente, se vislumbrou necessário resguardar direito ao seu titular de anuir [ou não] o tratamento dos seus dados, como forma de concretizar os seus direitos à

Revista ARACÊ
ISSN: 2358-2472

liberdade e à privacidade. Depois disto, observou-se que o mero consentimento não era suficiente, e que seria necessária uma tutela mais específica das operações de dados, de modo a resguardar a existência de padrões mínimos a serem seguidos no tratamento de informações pessoais (Suzin e Aguiar, 2023).

Cumprido o desiderato de esclarecer os riscos do tratamento de dados em meio ao capitalismo de vigilância, e o contexto fático e legislativo que precedeu à edição da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), cabe-nos analisar brevemente as linhas gerais da tutela da proteção de dados existente no Brasil.

3 LGPD E A TUTELA DA PROTEÇÃO DE DADOS NO BRASIL

É sabido que a proteção da privacidade não é uma preocupação recente, ou mesmo exclusiva da sociedade da informação, na medida em que há artigos debatendo a importância da sua tutela no início da década de 1980. Trata-se de direito fundamental consolidado pela atual ordem constitucional, que é justamente o ponto central da disciplina realizada pela Lei Geral de Proteção de Dados Pessoais (LGPD), que gravita no entorno do direito do cidadão de decidir sobre a utilização [ou não] dos seus dados em operações, e sobre as finalidades que porventura poderão ser atingidas pelos tratamentos autorizados (Cerqueira, 2022).

A Lei Geral de Proteção de Dados Pessoais brasileira tem forte inspiração no Regulamento Geral de Proteção de Dados promulgado pelo Parlamento Europeu no ano de 2018, que enunciou parâmetros rígidos para as atividades de tratamento de dados, e penalidades enérgicas para os casos de descumprimento (Búrigo e Carloto, 2023).

A influência das regras da União Europeia não se resumiu, aliás, à técnica legislativa, já que, paralelamente à necessidade de normatização já delineada acima, a exigência enunciada no Regulamento Geral às empresas europeias, de contratar apenas com firmas estrangeiras cujo país ostentasse proteção legal de tratamento de dados adequada, exigiu que o Brasil disciplinasse a matéria, sob pena das suas empresas não poderem manter relações comerciais com as europeias (Oliveira, 2018).

A Lei n.º 13.709/2018 regulou todas as atividades de tratamento de dados pessoais no país, inclusive as realizadas pelo Poder Público e as desenvolvidas sem finalidade lucrativa. Para tanto, além de enunciar regras a serem observadas nas operações de dados, enumerou princípios que devem nortear a sua aplicação [e de todas as normas que versem sobre a matéria, sejam elas outras leis ou atos infralegais]. Aludida principiologia é lastreada no ideal de proteger a privacidade do titular de dados,

Revista ARACÊ
ISSN: 2358-2472

por meio da tutela legal das informações capazes de permitir, de maneira singular ou associada, a identificação da pessoa natural (Cardoso, 2023).

Logo, a LGPD não protege exclusivamente os dados sensíveis, vez que é fulcrada na concepção expansionista de dados pessoais (Oliveira, 2018), que abarca todos aqueles que permitem a identificação da pessoa de forma direta e, também, os que, quando combinados, igualmente precisam a identidade do titular, conforme sobredito. Exemplificativamente, um dado sobre compra, um dado de navegação e uma informação sobre o deslocamento do indivíduo podem não ser significativos se considerados isoladamente, mas, combinados, permitem a perfeita identificação das preferências sexuais, filosóficas e políticas do usuário da internet (Lucca e Martins, 2024), razão pela qual são abarcados pela LGPD.

Acerca da principiologia adotada pela Lei n.º 13.709/18, destacam-se o "princípio da finalidade (...) vincula o tratamento a um fim específico (...), vedada sua modificação, via de regra, sem a coleta de novo consentimento (...), e o princípio da necessidade, que permite o tratamento apenas dos dados essenciais para se alcançar a finalidade (...)" (Oliveira, 2018). Há, também, um princípio implícito, que advém da confluência das previsões da LGPD sobre a necessidade de neutralização de riscos de danos, que é o princípio da precaução, que impõe um dever positivo aos agentes de tratamento, a quem incumbe desenvolver rotinas de prevenção de incidentes (Martins e Longhi, 2022).

Prática, portanto, semelhante ao tratamento de dados sem prévio consentimento (não amparado pela presença dos requisitos que o dispensam, obviamente), está o desvio de finalidade do tratamento de dados autorizado pelo usuário, já que as operações devem atender à finalidade prenunciada ao titular das informações, e que o uso para outros propósitos perfaz ato ilegal (Cavet e Faleiros Júnior, 2024).

Ao amparar os titulares dos dados, a Lei n.º 13.709/18 conferiu-lhes diversos direitos, como a ciência acerca de operações de dados, a anonimização de informações e a correção de informações equivocadas, por exemplo. Ademais, atribuiu ao agente controlador, assim entendido o operador de dados decide como se dará o tratamento, um dever de transparência quanto ao método empregado, a abrangência das operações, a forma de sistematização, os principais impactos e riscos da manipulação de dados - que devem ser, em regra, esclarecidos ao usuário solicitante e, irrestritamente, à Autoridade Nacional de Proteção de Dados (ANPD) (Calabrich, 2020).

Malgrado a centralidade do consentimento no âmbito da proteção de dados, após a segunda audiência pública realizada no Congresso Nacional durante a tramitação legislativa da LGPD, o legítimo interesse para o tratamento de dados foi inserido entre as hipóteses autorizativas, em atendimento aos anseios de flexibilidade dos agentes de dados, que militavam a impossibilidade de obter anuência do usuário em cada operação de tratamento (Verbicaro e Calandrini, 2022).

Revista ARACÊ
ISSN: 2358-2472

Por exigência legal, a operação deve ser realizada a partir de uma situação concreta, dirigida a um interesse legítimo, e primar pelo respeito às legítimas expectativas do titular de dados. Como "legítimo interesse" é um conceito vago e indeterminado, a sua invocação exige certa razoabilidade do agente, sob pena de aviltar a proteção de direitos fundamentais do respectivo titular (Oliveira, 2018). Por se tratar de hipótese de tratamento que dispensa a anuência do titular de dados, ela merece especial cautela dos operadores do direito, a quem cabe enunciar parâmetros interpretativos capazes de conciliar o ideal de plasticidade intentado pelos empresários com o dever de obediência aos direitos fundamentais do titular de dados.

Além do cumprimento dos requisitos legais, por inevitável, a atuação do agente de tratamento deve ser orientada pelo princípio da finalidade e da necessidade que exigem, respectivamente, que a operação justificada pelo legítimo interesse seja realizada com base em razões alinhadas ao ordenamento jurídico, e que os dados se resumam ao mínimo necessário – sempre observado o direito de informação que assiste ao interessado, e a necessidade de enunciação de justificativa concretas para lastrear a operação (Verbicaro e Calandrini, 2022).

É digno de nota que, ainda que LGPD não discipline exclusivamente as operações envolvendo dados sensíveis, diante do potencial de lastrear estigmas, discriminação e segregação social – que, por vezes, podem dar azo à violência física e a campanhas difamatórias – esta especial classe de informações, de natureza nitidamente existencial, goza [e, diga-se, precisa gozar] de especial proteção legislativa (Lucca e Martins, 2024).

Vale recordar, neste ponto, que após a Segunda Guerra Mundial, os sistemas jurídicos foram ressignificados sob o prisma do reconhecimento da força normativa da Constituição, de modo que todas as normas do ordenamento passaram a estar materialmente subordinadas ao cumprimento dos seus valores centrais, especialmente a Dignidade da Humana e os direitos a ela correlatos (Siqueira Júnior, 2011).

Inspirada nos ideais de proteção e de promoção de direitos fundamentais, a Lei n.º 13.709/2018 resguardou proteção aos dados pessoais tanto sob o viés da privacidade quanto da proibição de tratamento de dados para fins discriminatórios e ilícitos, que possam causar a exclusão ou prejudicar a fruição de direitos inerentes à condição humana, sempre visando à concretização da igualdade material (Lucca e Martins, 2024).

Ilustrando a necessidade de tutelar os dados pessoais sob o viés da não discriminação, em 2018, a empresa Decolar precisou ser sancionada em cifra milionária pela prática de *geopricing*, que consistia na diferenciação de preços de passagens aéreas de acordo com a localização do consumidor. De igual maneira, um sistema de seleção de pessoal da Amazon privilegiava a contratação de homens em

Revista ARACÊ
ISSN: 2358-2472

detrimento de mulheres. Além disso, o algoritmo de reconhecimento do Google Photos identificava pessoas negras como gorilas, e um sistema desenvolvido para auxiliar o Judiciário americano a avaliar chances de reincidência criminal tendiam a prenunciar quase duas vezes mais riscos quando se tratavam de pessoas negras, e considerar pessoas brancas como de baixo risco de voltar a delinquir (Calabrich, 2020).

Diante do vínculo direto entre os dados sensíveis e a concretização de direitos fundamentais, o legislador optou por condicionar o seu tratamento ao consentimento específico, destacado e voltado a desiderato específico previamente declarado, que só não será exigível em situações excepcionais, como o desenvolvimento de políticas públicas, a prevenção de fraudes e de ameaças, e o uso de biometria. De igual forma, a LGPD permitiu que os dados de saúde sejam manipulados para estudos, mas exigiu a sua anonimização, a observância das regras do Código de Ética Médica, a manutenção das informações em ambiente restrito e vedou compartilhamentos de dados de saúde com finalidade lucrativa a outros agentes de tratamento (Lucca e Martins, 2024).

Outra questão que merece destaque é o fato de que, conquanto a redação original da Lei n.º 13.709/18 previsse a possibilidade de revisão de decisões automatizadas por pessoas naturais, esta disposição foi suprimida pela Medida Provisória n.º 869/2018, posteriormente convertida na Lei n.º 13.853/2019, que passou a viabilizar que até mesmo uma eventual revisão possa ser robotizada. Isto se deu sob a premissa de que novos modelos de negócios poderiam ser inviabilizados pela necessidade de pessoal para revisar as decisões algorítmicas, e de que haveria impactos substanciais na análise de risco inerente às operações de crédito. Por outro lado, diante da alteração legislativa, a LGPD passou a exigir que o controlador forneça informações claras acerca dos critérios utilizados na decisão automatizada e que, caso não possa fazê-lo para resguardar segredo industrial, a Autoridade Nacional de Proteção de Dados, sobre a qual se discorrerá adiante, poderá auditar o algoritmo para verificar a existência ou não de critérios discriminatórios, que são vedados pela lei (Calabrich, 2020).

No mais, despeito da aparente divergência entre a disciplina legal do tratamento de dados enunciada pela LGPD e pelo Marco Civil da Internet, é fato que este apenas disciplinou o tratamento de dados de maneira sutil, sendo insuficiente para normatizar a matéria, e que, sob a égide da especialidade legislativa, em caso de conflito normativo, a situação concreta deve ser tutelada por aquela norma. De toda maneira, haver-se-á que buscar, na generalidade dos casos, uma aplicação combinada de ambas, para fins de resguardar maior proteção ao usuário, na medida em que o artigo 64 da LGPD enuncia que o seu conteúdo não exclui o arcabouço protetivo estabelecido por outras normas, nacionais e internacionais, que tratem do tema (Oliveira, 2018).

Revista ARACÊ
ISSN: 2358-2472

Paralelamente, há que se reconhecer que o avanço tecnológico permitiu que o Estado conhecesse detalhadamente as premências da população, e pudesse desenvolver políticas públicas mais assertivas, além de modernizar o sistema de mobilidade urbana (Oliveira, 2018), o que perfaz nada além do que o cumprimento do dever de eficiência incumbido ao Poder Público pela reforma administrativa de 1998, que marcou a transição do modelo de Administração burocrática para o gerencial, orientado a resultados (Leal Júnior e Penha, 2022). O próprio acesso à informação, aliás, permitiu uma verdadeira ressignificação do princípio constitucional da publicidade, que já não se limita à publicização de dados em diários oficiais (Neves, 2018).

De toda forma, a Lei Geral de Proteção de Dados vem sendo invocada com frequência pelos órgãos públicos para justificar recusas de acesso a dados públicos – fato que não se compatibiliza com o sistema constitucional vigente, tampouco com os ditames da Lei n.º 12.527/2011 (Lei de Acesso à Informação, ou LIA) (Cerqueira, 2022).

Neste aspecto, deve-se considerar que o acesso à informação é uma das bases da democracia participativa, e que perfaz o meio resguardado ao cidadão de avaliar o papel desempenhado pelo Estado e as formas de aplicação dos recursos públicos, de reivindicar direitos e de participar da condução dos rumos da Administração Pública (Deienno e Santos, 2014, p.17).

A aplicabilidade da LGPD ao setor público é inequívoca e inarredável. Contudo, isto não significa dizer que os pedidos de acesso devam [ou mesmo, possam] ser indeferidos em homenagem à tutela da proteção de dados, vez que existe uma relação de complementariedade - e não de oposição - entre a LGPD e a LIA, na medida em que tutelam, respectivamente, direitos constitucionais de acesso à informação, e à intimidade e proteção de dados, de modo que cabe aos órgãos públicos estabelecer mecanismos eficientes de classificação dados que permitam uma tutela harmoniosa de ambos. Diga-se: somente as informações de natureza pessoal capazes de identificar o seu titular é que são protegidas de divulgação pela LGPD, não havendo razão para que aquelas que não dizem respeito à identificação de contribuintes, aos dados patrimoniais, à vida privada e à intimidade destes [e, em regra, extensivamente, aos servidores públicos e dos agentes políticos] não sejam divulgadas pelo Estado - desde, obviamente, que não haja incidência de alguma das hipóteses de sigilo enunciadas pela LIA. (Cerqueira, 2022).

Apresentados os principais mecanismos de proteção contemplados pela LGPD para salvaguardar os direitos aos titulares de dados no Brasil, com o fito de ilustrar a importância da LGPD, sobretudo para que o presente artigo não se limite a questões puramente teóricas que, muitas vezes, poderiam ser observadas através da leitura da Lei n.º 13.709/18, passa-se a enunciar, nos próximos

Revista ARACÊ
ISSN: 2358-2472

parágrafos, alguns exemplos práticos de aplicação das normas de proteção de dados ao âmbito das relações de trabalho.

Como a seara laboral envolve a coleta periódica e o tratamento de dados do trabalhador, é fácil inferir que a LGPD irradia os seus efeitos na tutela dos direitos do obreiro, seja ele público ou privado. Neste particular, adquire especial relevo a gestão de dados relacionados à saúde do colaborador, especialmente de atestados e informações relacionadas à condição médica do profissional. Sobre o tema, menciona-se a condenação por danos morais imposta em 2020 à Companhia de Saneamento de Minas Gerais pelo Tribunal Regional do Trabalho da 03ª Região, em razão da permissão de acesso de pessoas não autorizadas a informações de saúde de um empregado, por meio do sistema informatizado interno. Outro exemplo claro da importância da tutela das informações sensíveis do trabalhador foi a anulação, no ano de 2019, de cláusula de uma convenção coletiva de trabalho que dispunha sobre a obrigatoriedade de indicação de CID para fins de abonar faltas, sob a premissa de que a inclusão desta informação somente pode se dar por iniciativa do titular, inclusive sob pena de violação do Código de Ética Médica (Búrigo e Carloto, 2023).

De igual maneira, a tutela da proteção de dados e da intimidade que foi preconizada pela LGPD irradia efeitos diretos sobre as relações laborais permeadas pelo teletrabalho. Como os contratos de trabalho por jornada fixa exigem o pagamento de adicional de horas extraordinárias ou a instituição de folgas compensatórias por horas excedentes, vem sendo frequente o uso de aplicativos de vigilância de empregados. Alguns deles envolvem o monitoramento de telas, a leitura de mensagens de *WhatsApp* e de redes sociais, o rastreamento geográfico, a captação de imagens e sons, por exemplo – fato que é agravado, na maioria dos casos, pela ausência de prévia cientificação do interessado, e pela fragilidade de eventual consentimento franqueado no âmbito laboral, que é marcado por acentuada assimetria. Sob a égide da LGPD, é impensável que o empregador possa empregar muitos destes recursos, especialmente o monitoramento de conversas e imagens através de webcam, vez que a hipótese de tratamento para garantia da segurança do titular é voltada à autenticação biométrica, e que a prevenção de fraudes deve pressupor indício prévio apto à relativização da intimidade. Aliás, até mesmo o monitoramento de geolocalização deve ser empregado com parcimônia, na medida em que é defeso ao empregador traçar perfis de preferência ou os hábitos do empregado fora da jornada laboral através deste tipo de operação (Hentges e Coimbra, 2022).

Na mesma linha, o consentimento do titular de dados adquire especial dificuldade no âmbito do direito trabalhista, que é amplamente marcado pela assimetria entre empregado e empregador. Por esta razão, entende-se necessário que o consentimento válido deve ser condicionado à presença de informação ostensiva quanto à possibilidade de recusa, de eventuais consequências desta e, sobretudo,

Revista ARACÊ
ISSN: 2358-2472

da finalidade visada com o tratamento de dados, do escopo da coleta, e da possibilidade de revogação da anuência a qualquer tempo (Búrigo e Carloto, 2023).

Como os algoritmos vêm sendo utilizados até mesmo na análise de currículos e na seleção de empregados, é necessário resguardar que a programação de dados não enseje qualquer forma de discriminação - prática vedada pela LGPD, que, como exposto, proíbe qualquer tratamento de dados com viés ilícito ou discriminatório e, também, pela Lei n.º 9.029/95, que veda a limitação de acesso ao trabalho por motivos de raça, sexo, preferências individuais, idade e afins. Para tanto, entende-se que as regras de proteção de dados contidas na LGPD somente serão cumpridas se os sistemas informatizados forem programados para perquirir exclusivamente a aptidão profissional do candidato, independentemente da análise de dados alheios a este desiderato, como o sexo, o estado civil ou as posições pessoais do interessado. Paralelamente, parece indispensável o desenvolvimento de rotinas de conferência periódica dos perfis que vêm sendo selecionados pelos sistemas eletrônicos, para que se possa inferir se, na prática, o algoritmo não está adotando parâmetros segregatícios (Sturmer e Miranda, 2023).

Esgotado o escopo do presente tópico, passa-se a apresentar algumas breves notas quanto aos mecanismos sancionadores desenvolvidos pela LGPD, e as regras de responsabilização civil por violação de deveres relacionados ao tratamento de dados nela contidas.

4 LGPD E OS MECANISMOS DE RESPONSABILIZAÇÃO POR VIOLAÇÃO ÀS REGRAS DE TRATAMENTO DE DADOS

Diante da constitucionalização do direito administrativo, qualquer sanção por descumprimento de deveres nas operações de dados deve ser precedida de processo administrativo de natureza sancionatória permeado pelo contraditório e pela ampla defesa. Ademais, por exigência da LGPD, eventual penalidade deverá observar critérios como a gravidade do fato, a existência ou não de má-fé e a reincidência do agente (Andréa, Arquite e Camargo, 2020).

Segundo a Lei n.º 13.709/2018, cabe à Autoridade Nacional de Proteção de Dados (ANPD), além de regulamentar as atividades de tratamentos de dados sob o viés da mínima intervenção e de firmar entendimentos quanto à interpretação da LGPD, aplicar sanções no caso de descumprimento de deveres pelo agente de tratamento. Embora a ANPD não possa, por conta de um veto presidencial à Lei n.º 13.853/2019, suspender a atividade de tratamento de dados pessoais no caso de constatação de irregularidades, ela pode aplicar penalidades de advertência, de multa de até 2,00% do faturamento da empresa, de multa diária para readequação (limitado, em qualquer caso, a cinquenta milhões de reais),

Revista ARACÊ
ISSN: 2358-2472

de publicização da irregularidade constatada, da eliminação dos dados atinentes à irregularidade e de bloqueio destas a regularização (Calabrich, 2020).

Vale mencionar que a Autoridade Nacional de Proteção de Dados, com papel regulamentar e sancionador somente entrou em efetiva atividade externa no ano de 2021, como órgão integrante da estrutura Administração Direta Federal – portanto, sem independência técnica e financeira. Somente com a conversão da Medida Provisória n.º 1.124/2022 na Lei n.º 14.460/2022 é que a ANPD passou a atuar de maneira autônoma, na qualidade de autarquia especial (Cardoso, 2023).

Aludida autarquia tem, pois, o papel de "atuar preventivamente na construção de um diálogo racional e permanente com os agentes econômicos e a sociedade civil, mas também, de maneira enérgica e eficaz, reprimir exemplarmente condutas ilícitas" (Verbicaro e Calandrini, 2022).

Há que se ponderar que a ANPD tem função crucial na fiscalização das operações de dados lastreadas no legítimo interesse - que, por perfazer conceito dotado de alto grau de abstração, exige uma atuação fiscalizatória proativa do Poder Público. Por previsão do § 3º do artigo 10 da LGPD, a autarquia pode solicitar relatório de impacto à proteção de dados em virtude do emprego do legítimo interesse como hipótese de tratamento (que, diga-se, tem se mostrado bastante usual). Como este pressuposto autorizativo prescinde do consentimento, e os tratamentos de dados são pouco acessíveis [e, até mesmo, compreensíveis] aos usuários, vislumbra-se que as operações baseadas no legítimo interesse são fulcradas na confiança do titular em relação à licitude da atuação dos agentes de tratamento – o que exige, para fins de amparo às legitimas expectativas do titular de dados, o desenvolvimento de mecanismos eficientes de controle da ANPD, seja por meio da atuação fiscalizatória, educativa, ou mesmo sancionatória, sempre voltada a evitar abusos e o comprometimento da política nacional de dados (Verbicaro e Calandrini, 2022).

Quanto à responsabilidade civil, vislumbra-se que, ao regulamentar a questão, a Lei n.º 13.709/2018 não se limitou a tutelar o ressarcimento de danos, vez que também prenunciou a necessidade de prevenção de incidentes envolvendo o tratamento de dados. Neste sentido, o artigo 6º, X, da LGPD atrelou questões inerentes à responsabilização do agente à prestação de contas ao usuário quanto aos mecanismos empregados para a proteção dos dados pessoais e a demonstração da sua eficácia. Os incisos VII e VIII do mesmo artigo, por sua vez, disciplinam a necessidade de desenvolvimento de rotinas aptas a prevenir incidentes de dados, e de adotar métodos capazes de proteger os dados do acesso não autorizado, da perda e da alteração indevida. Os artigos 42 a 45, de maneira complementar, regulam o dever de indenizar danos sofridos pelo titular de dados em virtude de falhas nas operações de dados – que costumam trazer consequências graves à imagem e à privacidade do usuário (Ribeiro, 2022).

Revista ARACÊ
ISSN: 2358-2472

Sob a égide do artigo 927, Parágrafo Único do Código Civil, que positivou a adoção da teoria do risco no Brasil, deve-se interpretar o artigo 42 da LGPD como enunciador de responsabilidade objetiva por danos causados nas operações de tratamento de dados, haja vista que a atuação do controlador e do operador de dados, por natureza, expõe os direitos dos titulares a riscos. É impensável, neste contexto, que em virtude da menção de que a obrigação de indenizar adviria de dano causado por violação à legislação que trata de proteção dados, o legislador tenha estatuído hipótese de responsabilização subjetiva (Martins e Longhi, 2022) - o que seria sobremaneira pernicioso por vulnerar demasiadamente o titular de dados em um contexto de assimetria informacional e de enorme opacidade das operações de dados pessoais.

Malgrado não haja reprodução do artigo 927, Parágrafo Único do Código Civil na LGPD, é fato que a tutela conferida pelo legislador civilista já enunciou, de maneira suficiente, que o agente cuja atuação seja capaz de colocar direitos de terceiros em risco deve reparar danos independentemente de perquirição de culpa, ou valoração do nível de cumprimento do dever de cuidado. Noutros termos, embora a LGPD não tenha definido expressamente o regime de responsabilidade civil aplicável no seu âmbito normativo, uma interpretação sistemática da legislação civil permite inferir a hipótese de tratamento de dados atrai a responsabilização objetiva do agente, já que a natureza da atividade expõe o titular dos dados a riscos de danos (Cardoso, 2022).

Até porque, vale repetir, os danos advindos de incidentes de segurança são intrínsecos às operações de dados e, desta forma, os riscos decorrentes deles igualmente o são. Há que se considerar, neste ponto, que sob o prisma da responsabilização objetiva, o agente de tratamento será estimulado a investir em parâmetros mais rígidos de segurança para evitar incidentes e, portanto, o pagamento de indenizações. O contrário também é válido. Na hipótese de responsabilização subjetiva, a vítima acabará tendo que internalizar, em regra, os danos advindos do tratamento de dados realizado por terceiros (que, vale repetir, perfaz uma atividade altamente lucrativa aos fornecedores), o que ensejará menores níveis de cuidado pelo operador de dados. Nem mesmo se pode aventar, neste ponto, que a responsabilização objetiva impediria a evolução tecnológica, já que este argumento fora levantado [e superado] no contexto da edição do Código de Defesa do Consumidor (Martins e Longhi, 2022).

Este, aliás, irradiará efeitos sobre a grande maioria das relações travadas no âmbito virtual (desde que preenchido, obviamente, o seu pressuposto de incidência, que é o enquadramento das partes nos conceitos normativos de fornecedor e de consumidor), de modo que não há justificativa jurídica para que a regra de responsabilidade objetiva daquele subsistema seja afastada apenas por se tratar de tratamento de dados.

Revista ARACÊ
ISSN: 2358-2472

A forte inspiração da LGPD no código consumerista, vale advertir, é evidenciada pelas regras de distribuição do ônus da prova. Destaca-se, neste ponto, a existência de regras na LGPD que imputam ao controlador o encargo de comprovar a anuência expressa e específica do titular (e não genérica, ou voltada a uma finalidade diversa da empregada pelo agente de tratamento), no caso de operações de dados lastreadas no consentimento. Também, o permissivo legal para que o juiz a possa inverter o ônus da prova quando a alegação do titular for verossimilhante, ou quando evidenciada a hipossuficiência ou dificuldade excessiva de produção de prova pelo interessado, nos mesmos moldes do Código de Defesa do Consumidor – fato que demonstra uma clara preocupação do legislador de equilibrar a desigual relação entre o agente de tratamento e o titular de dados, e de evitar a adoção de práticas abusivas ou desleais (Cardoso, 2023).

Quanto à abrangência subjetiva da responsabilidade civil, a LGPD prevê que o controlador será, em regra, responsável por reparar os danos causados ao usuário em virtude de incidente na operação de dados. O operador [desde que, obviamente, tenha participado diretamente do processamento de dados que gerou o dano], por sua vez, responderá solidariamente com aquele quando descumprir as regras enunciadas pelo controlador (dentre elas, a política de privacidade e os códigos de conduta da organização) e as regras de proteção de dados, ou no caso de cumprir ordens ilícitas do controlador - sempre observado, em qualquer caso, o direito de regresso do interessado em face dos corresponsáveis. Em síntese: o controlador será o responsável por reparar os danos, seja de forma singular ou conjunta com o operador, a depender do caso, e o operador somente será responsabilizado quando tiver incorrido em uma das hipóteses arroladas pelo legislador (Cardoso, 2022).

A responsabilização solidária enunciada pela LGPD irradia importantes efeitos para o âmbito das relações entre empresários. É que uma situação bastante comum no mercado de consumo é a formação de redes contratuais com segregação das funções de controlador e de operador de dados, ou mesmo o compartilhamento de informações entre diversas empresas. Este intercâmbio de dados exige não só que o titular seja informado acerca da troca de informações e da finalidade desta remessa, mas também que o responsável pelo envio se responsabilize pela adequação do sistema de tratamento do agente destinatário perante o particular interessado. Isto exige, por inevitável, a adoção de mecanismos de gestão conjunta de riscos relacionados ao vazamento de informações, ao desvio de finalidade das operações de tratamento, à adulteração de dados, ao emprego de dados para fins ilícitos, por exemplo, que perfazem meios de evitar que uma empresa seja penalizada em virtude de irregularidades perpetradas por um parceiro comercial, ainda que tenha agito de forma correta. Vale recordar que, além do dever de indenizar os danos sofridos pelos titulares, as práticas irregulares podem ensejar a aplicação de penalidades administrativas, como multas de até cinquenta milhões de reais e que a

Revista ARACÊ
ISSN: 2358-2472

divulgação do incidente de dados pode, por si só, ensejar grande repercussão no mercado negocial, como a perda de parceiros e de valor mercadológico. Bem por isso, malgrado o desenvolvimento de mecanismos mitigadores de riscos não tenha sido arrolada como um dever pela LGPD, entende-se altamente recomendável que os contratos empresariais disciplinem de forma assertiva não só o compartilhamento de dados, mas também, ao menos, a garantia contratual de obediência às normas de proteção de dados, o dever de esclarecer aos usuários sobre o compartilhamento de dados com o parceiro negocial, a criação de mecanismos de auditoria periódica dos próprios sistemas de prevenção e, ainda, dos existentes na empresa parceira, a sujeição de empregados a termos de confidencialidade e a destinação de dados em caso de rompimento negocial (Andrade e Teles, 2020).

A responsabilidade por reparar o dano será excluída quando restar comprovado que o agente não foi quem realizou o tratamento de dados em referência, que não houve violação aos deveres legais de proteção de dados, ou que o risco é atribuível à vítima ou a terceiros, nos termos do artigo 43 da LGPD (Brasil, 2018).

Para que se possa, porém, perquirir se o tratamento de dados foi ou não adequado [que é uma das hipóteses eximentes de responsabilidade], deve-se observar os parâmetros enunciados no artigo 44 da mesma lei, que envolvem não apenas a obediência às normas legais, mas também o fornecimento de padrões de segurança legitimamente esperados pelo titular segundo a forma de realização do tratamento de dados, os riscos que dele razoavelmente decorrem e as técnicas disponíveis no momento da operação questionada. Em termos práticos: uma operação pode ser reputada irregular a despeito da fiel observância da legislação, quando se distanciar de normas de segurança da informação, dos regulamentos internos ou do dever de emprego do melhor método de tratamento disponível, por exemplo (Cardoso, 2022).

Por fim, vislumbra-se adequado o reconhecimento da existência de dano extrapatrimonial *in re ipsa* nos casos de violação das regras de tratamento de dados pessoais sensíveis, como forma de coibir práticas ilícitas. Sobretudo diante do potencial de causar danos de natureza existencial que é intrínseco a qualquer incidente de dados, e da necessidade de estimular o desenvolvimento de rotinas de máxima cautela nas operações de tratamento de dados sensíveis (Lucca e Martins, 2024).

5 CONCLUSÃO

Do exposto, infere-se que a popularização da internet trouxe enormes facilidades no âmbito das interações sociais, das telecomunicações, das relações de trabalho, mas tem sido permeada pela hipervigilância digital dos usuários, e pela coleta massificada de dados pessoais com a finalidade de traçar perfis de consumo e predizer comportamentos - que são o marco distintivo do chamado

Revista ARACÊ
ISSN: 2358-2472

capitalismo de vigilância. Paralelamente à fragilização do poder de escolha do consumidor por meio de técnicas neurocientíficas de persuasão, à criação de necessidades voláteis inerentes à sociedade de informação e aos prejuízos à autodeterminação informativa, a tutela normativa do direito à vida privada precisou ser reforçada, como forma de ordenar o tratamento massificado de dados pessoais no Brasil.

Neste contexto, conforme demonstrado, a LGPD foi aprovada para salvaguardar direitos fundamentais (sobretudo, a privacidade e a intimidade), e refrear operações de dados com finalidades discriminatória, abusiva ou capaz de vulnerar a fruição de direitos. A sua edição seguiu uma tendência internacional de proteção de dados pessoais, em meio à multiplicação de sérios incidentes de tratamento que encartam potencial de causar dano existencial aos seus titulares, e teve influência direta do Regulamento Geral de Proteção de Dados da União Europeia, que condicionou as parcerias comerciais das empresas europeias com organizações de outros países à tutela legislativa adequada do tratamento de dados pessoais na respectiva localidade.

Como exposto, a tutela da proteção de dados pessoais no Brasil é centrada, em grande medida, no consentimento do titular de dados, e no dever de informação do agente de tratamento quanto à extensão e à finalidade da operação – que deve se resumir, em todos os casos, apenas ao volume de dados indispensável para o desiderato pretendido, e se ater ao objetivo especificado. No mais, embora não se resuma a salvaguardar os dados pessoais sensíveis, é fato que a Lei n.º 13.709/2018 conferiu especial proteção a esta classe de informações, que é diretamente ligada aos aspectos íntimos da personalidade.

Entende-se que um dos méritos da LGPD foi o de tutelar interesses complementares, quais sejam, os interesses econômicos dos agentes de tratamento e o direito à privacidade e à intimidade do titular destes dados. Isso porque, se por um lado a coleta massiva de dados pode expor os usuários de rede a riscos [o que justifica a tutela legal dos seus interesses legítimos], de outro, não há razão para vilanizar a popularização da internet, ou mesmo dos agentes de tratamento de dados, cuja atuação possibilita a fruição de inúmeras comodidades.

Dito de outra forma, o que se deve rechaçar, em qualquer caso, é o emprego de mecanismos virtuais com o fito de tornar o ser humano refém da sua representação virtual, ou mesmo de limitar a fruição de direitos. Mas, o tratamento adequado de dados pessoais, com o desiderato de aprimorar a fruição de utilidades, deve ser estimulado – e é justamente o que visa a tutela engendrada pela Lei n.º 13.709/2018, e o direito fundamental ao tratamento adequado de dados pessoais que foi insculpido no inciso LXXIX ao artigo 5º da Constituição Federal.

De todo o exposto, conjectura-se que a LGPD foi capaz de regulamentar adequadamente o tratamento de dados no Brasil, embora se vislumbre que o efetivo respeito às garantias que foram

Revista ARACÊ
ISSN: 2358-2472

salvaguardadas ao titular de dados somente será obtida por meio de uma atuação mais enérgica da ANPD, seja por meio da atuação fiscalizatória, educativa, ou sancionatória e, também, do alinhamento do Poder Judiciário ao ideal de resguardar indenizações enérgicas em favor das vítimas de violações do direito à proteção de dados pessoais, independentemente da perquirição de culpa do agente de tratamento. Isto não só para salvaguardar a vítima, mas sobretudo para estimular o desenvolvimento de rotinas mais assertivas e eficientes de proteção de dados pessoais.

Espera-se, por fim, que o presente estudo instigue a realização de novas pesquisas a respeito da matéria, sobretudo com o fito de aprimoramento da LGPD, haja vista a necessidade de adaptação constante da legislação às rápidas transformações ocorridas no contexto virtual e, por conseguinte, aos novos desafios à salvaguarda de direitos fundamentais que nele surgem diariamente.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

ANDRADE, Raphael; TELES, Barbara. Alguns reflexos da Lei Geral de Proteção de Dados nas relações interempresariais e as possíveis formas de gerenciamento de riscos relacionados à responsabilização solidária. Revista de Direito e as Novas Tecnologias, São Paulo, vol. 8/2020, Jul - Set / 2020. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89928e000001957db5d89fc6189569&docguid=I927c3e80e10a11eaad20d1cf72cae2ef&hitguid=I927c3e80e10a11eaad20d1cf72cae2ef&spos=1&epos=1&td=1&context=11&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em 22 fev. 2025.

ANDREA, Gianfranco Faggin Mastro; ARQUITE, Higor Roberto Leite; CAMARGO, Juliana Moreira. Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil. Revista de Direito Constitucional e Internacional, São Paulo, vol. 121/2020. p. 115 – 139, Set - Out / 2020. Disponível em: < rdci-121-gianfranco-andrea-e-outros.pdf>. Acesso em 22 fev. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 mar. 2025.

BÚRIGO, Artur Bolan; CARLOTO, Selma. A efetividade dos direitos fundamentais e a proteção à privacidade no contexto das relações de trabalho: uma análise à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) e o desbalanceamento de poder. Revista dos Tribunais, São Paulo, vol. 1057, ano 112, p. 137-149, novembro 2023. Disponível em: < https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89817e000001957db7c6ed2dd30297&docguid=I03dba9f0793111ee918cf16d96029b87&hitguid=I03dba9f0793111ee918cf16d96029b87&spos=1&epos=1&td=1&context=21&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 21 fev. 2025.

CALABRICH, Bruno Freire de Carvalho. Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais. Revista de Direito e as Novas Tecnologias, São Paulo, vol. 8/2020, Jul - Set / 2020. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89817e000001957db819514bddd0a3&docguid=I01c65d10d2a711eaa3bfd5d545d9a492&hitguid=I01c65d10d2a711eaa3bfd5d545d9a492&spos=1&epos=1&td=1&context=31&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em 23 fev. 2025.

CARDOSO, Oscar Valente. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. Revista de Direito Privado, São Paulo, vol. 111. ano 23. p. 109-123, jan.-mar. 2022. Disponível em: http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2022-5147. Acesso em: 20 fev. 2025.

Revista ARACÊ
ISSN: 2358-2472

CARDOSO, Oscar Valente. O Ônus da Prova na Lei Geral de Proteção de Dados Pessoais. Revista dos Tribunais, São Paulo, vol. 1047/2023, p. 161 – 175, jan./2023. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89b1d5000001957dc7a6804554ff6b&docguid=I4842fee0770711ed8f58bed88a734e4b&hitguid=I4842fee0770711ed8f58bed88a734e4b&spos=1&epos=1&td=1&context=199&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>, Acesso em: 02 mar. 2025.

CAVET, Caroline Amadori.; FALEIROS JR., José Luiz de Moura. A publicidade direcionada por dados à luz da Lei Geral de Proteção de Dados Pessoais. Revista de Direito do Consumidor, São Paulo, vol. 154, ano 33, p. 161-187, jul./ago. 2024. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89817e000001957db953026e651e6e&docguid=I587f0da05e9e11ef9715ee068a6b1ec0&hitguid=I587f0da05e9e11ef9715ee068a6b1ec0&spos=1&epos=1&td=450&context=50&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 25 fev. 2025.

CERQUEIRA, Julie Silveira. A confluência entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados. Revista de Direito e as Novas Tecnologias, São Paulo, vol. 17. ano 5, out./dez. 2022. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a898b7e000001957dba2893731103b0&docguid=I5aad61606bb811ed8aac921ee1e5e871&hitguid=I5aad61606bb811ed8aac921ee1e5e871&spos=1&epos=1&td=288&context=66&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 24 fev. 2025.

DEIENNO, Renata; SANTOS, Stela Queiroz dos. Normas Gerais, Destinatários, e Princípios do Acesso à Informação. In: ALMEIDA, Herivelto de; LEHFELD, Lucas de Souza; GUEDES, Marcio Bulgarelli (org.). Comentários à Lei de Acesso à Informação. Santa Cruz do Sul: Essere Nel Mondo, 2014.

HENTGES, Suelen; COIMBRA, Rodrigo. As novas formas de controle do empregado e a Lei Geral de Proteção de Dados. Revista dos Tribunais, São Paulo, vol. 1041. ano 111. p. 241-258, julho 2022. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a898b7e000001957dbb1ad62f9ba5c8&docguid=I269d8c60e2b511ec8b52abff02381d09&hitguid=I269d8c60e2b511ec8b52abff02381d09&spos=1&epos=1&td=4000&context=84&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 25 fev. 2025.

LEAL JÚNIOR, João Carlos; PENHA, Renata Mayumi Sanomya. Eficiência, Consensualismo e os Meios Autocompositivos de Solução de Conflitos na Administração Pública. Revista dos Tribunais, Belo Horizonte, vol. 1038/2022, p. 51 – 67, abr./2022. Disponível em: https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89ca140000019545026d8cd6cdebc7&docguid=Ia9a70620b62a11ec9c2abe4b74fa6f44&hitguid=Ia9a70620b62a11ec9c2abe4b74fa6f44&spos=1&epos=1&td=6&context=53&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 20 fev. 2025.

Revista ARACÊ
ISSN: 2358-2472

LUCCA, Newton de; MARTINS, Guilherme Magalhães. A proteção dos dados pessoais sensíveis na Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, vol. 153. ano 33. p. 15-30, mai./jun. 2024. Disponível em: <http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2024-9337>. Acesso em: 25 fev. 2025.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. Responsabilidade civil na Lei Geral de Proteção de Dados, consumo e a intensificação da proteção da pessoa humana na internet. Revista de Direito do Consumidor, São Paulo, vol. 139. ano 31. p. 101-124, jan.-fev./2022. Disponível em:<https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a898b7e000001957dbc9b42a3ab7d42&docguid=I7ea41e20628511ecb033c78e1088bbbf&hitguid=I7ea41e20628511ecb033c78e1088bbbf&spos=1&epos=1&td=3&context=109&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 21 fev. 2025.

NEVES, Rodrigo Santos. Audiências de Conciliação e a Fazenda Pública: o Dogma da Indisponibilidade do Interesse Público do Juízo. Revista dos Tribunais, Belo Horizonte, vol. 990/2018, p. 289 – 306, abr./2018. Disponível em: https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89ca14000001954505d37f6e1a346a&docguid=I541a77902bf611e8916f010000000000&hitguid=I541a77902bf611e8916f010000000000&spos=1&epos=1&td=1&context=149&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 01 fev. 2025.

OLIVEIRA, Ricardo Alexandre de. Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico. Revista dos Tribunais, São Paulo, vol. 998/2018, p. 241 – 261, dez. /2018. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89a3e2000001957dbd4cf3f839a281&docguid=I19df6040ecb711e8810c010000000000&hitguid=I19df6040ecb711e8810c010000000000&spos=1&epos=1&td=1&context=124&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em 21 fev. 2025.

RIBEIRO, Ronetna Klaryssa Priscila Vieira Laviola. Responsabilidade civil objetiva dos provedores de aplicação por conteúdo postado por terceiros à luz e sob a vigência do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Revista de Direito e as Novas Tecnologias, São Paulo, vol. 14. ano 5, jan./mar. 2022. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89a578000001957dbdf9a39934ae3e&docguid=I03322750a42011ecbdd68452654b6c9c&hitguid=I03322750a42011ecbdd68452654b6c9c&spos=1&epos=1&td=1&context=140&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 21 fev. 2025.

Revista ARACÊ
ISSN: 2358-2472

SIQUEIRA JÚNIOR, Paulo Hamilton. Pós Positivismo. Revista do Instituto dos Advogados de São Paulo, São Paulo, vol. 28/2011, p. 239-265, jul./dez.2011. Disponível em: https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89d21f000001946556f38c616c9db9&docguid=Ibab718e02d2f11e1860900008517971a&hitguid=Ibab718e02d2f11e1860900008517971a&spos=16&epos=16&td=20&context=40&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 09 jan. 2025.

STÜRMER, Gilberto; MIRANDA, Diogo Antonio Pereira. A utilização de algoritmos na fase pré-contratual laboral: uma análise da seleção automatizada de empregados no Brasil e a Lei Geral de Proteção de Dados Pessoais. Revista de Direito do Trabalho e Seguridade Social, São Paulo, vol. 232. ano 49. p. 55-68, nov./dez. 2023. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89b480000001957dbf46e9d213573d&docguid=I73e0212077ad11eeb70fca6bfa4e4a9f&hitguid=I73e0212077ad11eeb70fca6bfa4e4a9f&spos=1&epos=1&td=1&context=160&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 24 fev. 2025.

SUZIN, Joseli Beatriz; AGUIAR, Daiane Moura de. Dados Sensíveis e a Telemedicina: Proximações com a Lei Geral de Proteção de Dados. Revista de Direito e Medicina, São Paulo, vol. 14/2023, jan./jun. 2023. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89a578000001957dc287ec82711080&docguid=I9f0c1490cd2011edae20a0ef97223717&hitguid=I9f0c1490cd2011edae20a0ef97223717&spos=1&epos=1&td=1&context=185&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 09 mar. 2025.

VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (LGL\2018\7222) (Lei Geral de Proteção de Dados Pessoais). Revista de Direito do Consumidor, São Paulo, vol. 139. ano 31. p. 73-99, jan.-fev./2022. Disponível em <https://www.researchgate.net/publication/358748033_A_PROTECAO_DA_CONFIANCA_DO_CONSUMIDOR_E_A_BASE_DO_LEGITIMO_INTERESSE_NA_LEI_137092018_LEI_GERAL_DE_PROTECAO_DE_DADOS_PESSOAIS>. Acesso em: 24 fev. 2025.