Análise dos limites de aplicação do legítimo interesse para o tratamento de dados no Brasil à luz da Lei Geral de Proteção de Dados[1]

João Bernardo Bordin[2]

Resumo: Este artigo científico analisa os limites do tratamento de dados no ordenamento jurídico brasileiro frente à LGPD. É temática de relevância em razão da própria competência que é dada à ANPD. A metodologia utilizada é a qualitativa de pesquisa aplicada, com objetivos descritivos e pesquisa bibliográfica. Por objetivos, buscou-se analisar a aplicação do modo legal de tratamento de dados com base no legítimo interesse, bem como a fragilidade do princípio em comparação à privacidade do usuário. Justifica-se a temática para debate, devido ao avanço tecnológico das relações, que geraram novas formas de tutelar os direitos fundamentais da privacidade e intimidade. Conclui-se, que houve deficiência na construção da LGPD, não sendo criado mecanismos eficientes na proteção dos dados pessoais, e abrindo espaço para interpretações, demandando portanto alteração legislativa, que vise buscar o consentimento expresso e inequívoco, resguardando de maneira eficiente os direitos constitucionais do cidadão.

Palavras-chave: Consentimento; Legítimo interesse; Lei geral de proteção de dados.

1 Introdução

O avanço tecnológico das relações do homem com a *internet* criou a necessidade de monitorar e regular o armazenamento e compartilhamento de dados por parte dos interessados. Enquanto a tecnologia avança em velocidade extrema, não foi proporcional à capacidade jurídica de acautelar as relações, causando ânsia no legislador em trazer uma resposta normativa no mesmo nível de crescimento do cenário digital.

Na busca pela eficiência, dentre outros textos legais, criou-se a lei geral de proteção de dados, baseada fortemente na legislação equivalente europeia, trazendo conceitos de preservação dos dados pessoais na *internet*, entre eles o princípio do legítimo interesse, Lei nº 13.709/2018.

Nesse estudo, analisa-se os limites de aplicação do legítimo interesse para o tratamento de dados no Brasil, à luz da LGPD. Explorando os aspectos legais e éticos envolvidos nesse tipo de tratamento, identificando os desafios e as perspectivas para sua aplicação efetiva.

A pesquisa é motivada pela necessidade de compreender até que ponto o legítimo interesse pode ser invocado como justificativa para o tratamento de dados pessoais, sem comprometer os direitos fundamentais dos indivíduos, como a privacidade e a autodeterminação informativa, analisando portanto a legislação brasileira sobre proteção de dados pessoais, investigando o papel do operador e do controlador no tratamento dessas

---

[1] Artigo científico produzido na Faculdade de Direito da Universidade de Passo Fundo/RS, no ano de 2024.

[2] Aluno do Curso de Direito da Faculdade de Direito da Universidade de Passo Fundo. E-mail institucional: 173105@upf.br ou joaobernardobordin@gmail.com, com orientação da professora Mestre Marlova Stawinski Fuga.

informações e examinando a finalidade do legítimo interesse como base legal para o tratamento de dados.

A pressa trazida pela necessidade de regulamentar o assunto trouxe consigo omissões e divergências de entendimento sobre o assunto, justificando portanto, a realização desta pesquisa. Além disso, é evidente a importância de se estabelecer um equilíbrio adequado entre a proteção da privacidade dos cidadãos e a promoção do desenvolvimento tecnológico e econômico, uma vez que o uso das ferramentas digitais é inevitável.

Os subtemas abordados neste projeto incluem a proteção de dados pessoais na sociedade da informação, destacando os desafios e as oportunidades trazidas pela era digital; o papel do operador e do controlador no tratamento de dados, examinando as responsabilidades e obrigações de cada parte envolvida nesse processo; e a finalidade do legítimo interesse como base legal para o tratamento de dados, analisando os critérios e limites estabelecidos pela LGPD para sua aplicação. Nesse diapasão, buscará demonstrar como urge a necessidade de aplicar limites taxativos das hipóteses de tratamento sobre o prisma do legítimo interesse.

2 A proteção de dados pessoais na sociedade da informação

Para compreensão da aplicabilidade do princípio do legítimo interesse, e análise de sua efetividade no Direito brasileiro, é necessário conhecer, em um primeiro momento, o que é a Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados.

A preocupação com a proteção de dados e a privacidade remonta a várias décadas antes da criação da conhecida LGPD. O surgimento e a rápida expansão da tecnologia, da informação, e da *internet* levaram a um aumento significativo na coleta, armazenamento e uso de dados pessoais. À medida que as pessoas compartilhavam cada vez mais informações online, surgiram preocupações sobre como esses dados eram utilizados e se a privacidade dos indivíduos estava sendo adequadamente protegida. No final do século XIX, a mídia impressa e a fotografia revelada já levantavam preocupações devido à sua capacidade de alcance e durabilidade, a *internet* e o *big data*[3] não têm limites, e estão criando novos domínios que precisam ser regulamentados pelo campo do direito. Através da aplicação de técnicas automatizadas para coletar e combinar dados, uma ampla variedade de informações é

[3] Big data é um conjunto de dados enorme e complexo, especialmente de novas fontes de dados. Esses conjuntos de dados são tão volumosos que o software tradicional de processamento de dados simplesmente não consegue gerenciá-los. No entanto, esses grandes volumes de dados podem ser usados para resolver problemas de negócios que a ciência não conseguiria resolver antes (Pretti, 2018).

extraída, e essas informações podem ser utilizadas para diversos fins, desde análises estatísticas até a criação de perfis que embasam a tomada de decisões em todos os aspectos da vida do indivíduo.

A Constituição Brasileira de 1988 não possui um artigo específico que trate exclusivamente da proteção de dados privados digitais, pois foi promulgada muito antes da popularização da *internet* e do surgimento das questões relacionadas à privacidade digital. No entanto, a Constituição assegura o direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, garantindo a proteção contra eventuais violações desses direitos. O sigilo de dados também está estabelecido no sigilo de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas.

O eventual avanço tecnológico e dos meios de comunicação trouxe a necessidade de implementar uma lei que protegesse e versasse de forma direta e específica sobre o assunto. É importante destacar que no Brasil, até o ano de 2014, não havia norma específica que garantisse a privacidade das informações dos usuários que navegam no mundo virtual. Dessa forma, nos conflitos que envolvessem a violação da privacidade dos dados dos usuários na *internet*, aplicava-se por analogia o inciso X, do artigo 5º da Constituição Federal de 1988[4], por não existir uma lei específica que pudesse solucionar os conflitos existentes que ocorrem através do ambiente virtual. Além disso, vazamentos e violações de dados em grande escala ocorreram tanto no Brasil como no mundo todo, expondo informações sensíveis de milhões de pessoas. Para muitos autores, o que balizou e acelerou via pressão popular uma regulamentação, foi o vazamento da empresa de *marketing* digital Exactis que expôs aproximadamente 340 milhões de registros contendo informações pessoais de consumidores e empresas. Os dados vazados incluíam uma ampla gama de informações, como nomes completos, endereços residenciais, números de telefone, endereços de *e-mail* e detalhes demográficos - além disso, dados relacionados a características demográficas e comportamentais, como idade, gênero, ocupação e hábitos de consumo, também foram expostos (Greenber, 2018).

O direito à privacidade é considerado um elemento fundamental dentro do conjunto de direitos de personalidade e na proteção da dignidade, estando intrinsecamente ligado aos direitos fundamentais de intimidade e inviolabilidade do domicílio, que é o local em que a

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

vida privada se desenrola. A concepção mais reservada do direito à vida privada está intimamente associada a outro direito fundamental: o direito à intimidade.

Embora sejam direitos independentes, a análise conjunta dos direitos à privacidade e à intimidade é, de certa forma, necessária, uma vez que refletem diferentes dimensões de um mesmo direito maior. Nesse contexto, enquanto o direito à privacidade abrange uma esfera mais ampla, o direito à intimidade se refere a uma esfera mais restrita e, como o próprio nome sugere, mais íntima. Além disso, esses direitos desempenham um papel essencial na salvaguarda da autonomia e da dignidade das pessoas, especialmente em um mundo cada vez mais permeado por tecnologias de vigilância e coleta de dados, que apresentam desafios significativos à proteção da privacidade e da intimidade. Portanto, a interligação desses direitos desempenha um papel crucial na defesa da integridade pessoal e da liberdade individual em uma sociedade em constante evolução.

A privacidade transcende esses conceitos e representa a liberdade do indivíduo de revelar informações pessoais, pensamentos, ideologias, identidade e ações somente quando desejar. Ter controle sobre essas informações é crucial, e a imposição compulsória ou dissimulada representa uma violação desse direito. Importante destacar que essa liberdade vai além da esfera da vida privada, tornando-se um direito público aplicável a toda a sociedade. Aborda-se não apenas o respeito à intimidade do indivíduo, que é garantido por direitos como a inviolabilidade do domicílio, o sigilo de correspondência, o segredo profissional, ou o clássico direito de ser deixado em paz. Reconhece-se que, com as mudanças sociais, surgem novos direitos que são essenciais para reconhecer a natureza humana.

De outra banda, as lições trazidas por Maldonado (2019, p.12) demonstram que embora os esforços das mais diversas regulamentações sobre proteção de dados pessoais, vive-se em um mundo de *big data*, onde estas informações são processadas por todos, pelas empresas ou pelas próprias pessoas, e a todo momento, em um volume jamais antes visto. Outra definição do termo é dado por Günther, que define *big data* em grandes volumes de dados amplamente variados que são gerados, capturados e processados em alta velocidade. Como tal, esses dados são difíceis de processar usando as tecnologias existentes. Ao adotar tecnologias analíticas avançadas, as organizações podem usar *Big Data* para desenvolver *insights*, produtos e serviços inovadores (Günther, 2017).

O uso do *Big Data* acarreta em dois principais aspectos negativos: potenciais violações da privacidade e a discriminação. Entretanto, estes não são os únicos resultados desfavoráveis possíveis. A diminuição da autonomia, a despersonalização do indivíduo, a classificação desfavorável de pessoas ou grupos, a imposição unilateral de informações e o

confronto com dados indesejados são preocupações inerentes ao processamento de dados (Günther, 2017).

Evidente o conflito entre um direito fundamental da pessoa humana e a realidade de um mundo conectado, o avanço tecnológico, especialmente no que diz respeito à coleta, armazenamento e análise de dados em larga escala, tem proporcionado um aumento sem precedentes na capacidade de monitoramento e rastreamento das atividades das pessoas. Por outro lado, a proteção da privacidade é um direito fundamental, reconhecido em várias constituições e tratados internacionais. Ele é essencial para garantir a dignidade humana, a liberdade de expressão e o exercício de outros direitos fundamentais. O direito à privacidade implica o controle sobre as informações pessoais e a capacidade de decidir o que é compartilhado e com quem.

É de grande importância refletir sobre a quantidade de vezes que é consentido ou de forma deliberada se dá para as diversas empresas dados e informações de hábitos durante um período do dia. Academia, faculdade, redes sociais, cartão de crédito, GPS, shopping entre outros. A soma destas informações entregues a estas empresas define a personalidade, os hábitos e costumes, bem como as preferências, os lugares que o usuário frequenta, quem são as companhias, os amigos e até o que não se gosta. É necessário então, que cada uma dessas empresas tome bons cuidados sobre estes dados e não os negocie. Diante deste prisma, a legislação brasileira criou a LGPD, que tem como objetivo proteger os direitos fundamentais de privacidade e liberdade dos cidadãos em relação aos seus dados pessoais, regulando o tratamento de dados pessoais, nos meios digitais ou físicos, realizado por pessoas naturais ou pessoas jurídicas, de direito público ou privado, tendo entrado em vigor no Brasil em setembro de 2020.

Muito inspirada no Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia, tem como conceito central garantir o controle dos cidadãos sobre seus dados pessoais, fazendo com que as empresas e organizações que coletam, armazenam, processam ou compartilham dados pessoais devem fazê-lo de forma transparente, obtendo o consentimento adequado dos indivíduos e utilizando medidas de segurança para proteger esses dados (DPO, 2018).

Apesar de haver muitas similaridades entre a LGPD e o GDPR, os dois dispositivos possuem diferenças importantes, principalmente na sua rigidez e detalhamento, sendo a norma Brasileira menos detalhista e com menores imposições, não exigindo por exemplo que sejam feitos Relatórios de Impacto de Proteção de Dados, uma exigência da normativa estrangeira, que analisa a atividade de uma determinada empresa ou pessoa, e os riscos de exposições de

dados inerentes a essa atividade, avaliando então, posteriormente, o sistema de proteção existente para verificar se há ou não vulnerabilidades que propiciem que os eventos de riscos identificados venham a se concretizar. (Lima, 2020) Ainda, pela leitura do texto legal, a LGPD deixa lacunas para a Autoridade Nacional de Proteção de Dados[5] preencher, e que acaba trazendo fragilidades e obscuridades.

E por mais que a LGPD tenha iniciado sua vigência em setembro de 2020, a ANPD somente começou a atuar, com poder de aplicar sanções administrativas, em agosto de 2021, trazendo uma lacuna de aplicação, que somada a uma lenta capacidade de regular todas as hipóteses deixadas pela legislação, fez com que o direito fique desprotegido e refém da boa-fé dos operadores no período. Importante que compreenda-se o papel da autoridade, que conforme conceituado por Lima, obtém o poder de aplicar sanções, controlar e fiscalizar, o que implica na faculdade da entidade em requisitar informações dos responsáveis pelo tratamento de dados, ao titular dos dados e a terceiros quando for o caso, além de realizar diligências, procedimentos de auditoria e inspeções em entidades públicas e privadas que realizam atividades de tratamento de dados pessoais, punindo-as quando necessário (2020, p.111).

Se não bastasse para a autoridade, as dificuldades já apresentadas, para a autora, os demais desafios na tutela destes direitos são a sua capacidade de aplicação, diante da circulação transfronteiriça das informações; e definição de padrões técnicos que estabeleçam um ambiente verdadeiramente seguro para a coleta e tratamento de dados pessoais (Lima, 2020, p. 131).

A proteção de dados representa um princípio fundamental da liberdade e dignidade individuais. Nesse sentido, não se pode aceitar que os dados sejam utilizados de forma a converter um indivíduo em um objeto sujeito a vigilância constante. Enfrenta-se a possibilidade de sermos observados por meio de câmeras de vídeo e tecnologias biométricas, e os indivíduos podem ser alterados pela inserção de chips e etiquetas inteligentes, que podem ser lidas por meio de identificação por radiofrequência. Esse cenário nos coloca cada vez mais na condição de pessoas na rede, indivíduos permanentemente conectados, gradualmente

[5] A Autoridade Nacional de Proteção de Dados, ou ANPD, foi criada pela Medida Provisória n. 869, de 27 de dezembro de 2018, posteriormente convertida na Lei n. 13.853, de 14 de agosto de 2019. Por sua vez, o Decreto 10.474, de 26 de agosto de 2020, aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da ANPD, com entrada em vigor na data de publicação da nomeação do Diretor-Presidente da ANPD no Diário Oficial da União, ocorrida em 06 de novembro de 2020, quando, então, a ANPD efetivamente iniciou suas atividades. A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia federal de natureza especial do Brasil que, atualmente, se encontra vinculada ao Ministério da Justiça e Segurança Pública e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (BRASIL, 2023).

adaptados para transmitir e receber informações que permitem o escaneamento e perfilamento de nossos movimentos, hábitos e contatos. Isso modifica o significado e o conteúdo da autonomia dos indivíduos, o que é incompatível com a própria natureza da proteção de dados como um direito fundamental.

Para aqueles acostumados em usufruir de produtos e serviços de forma física e presencial, nunca houve impasses em resolver conflitos ou problemas jurídicos com o provedor. Entretanto, em um mundo digital o produto ou serviço prestado não tem local físico para ser retirado ou consumido, e quando se trata de tratamento de dados pessoais, o emaranhado é ainda maior. Veja-se, pois apesar de parecer simples, a empresa de bairro que coleta e possui dados pessoais de toda uma comunidade não possui fisicamente estes dados que, após a coleta, são transferidos para um servidor localizado fora do Brasil.

Antevendo a potencial situação de conflito, o legislador já abordava a necessidade de prevenir abusos decorrentes das alterações geográficas, conforme expresso por Cíntia Rosa Pereira de Lima em sua obra, anteriormente à LGPD, o Marco Civil da *Internet* dispôs, em seu artigo 11[6], regras sobre o âmbito de aplicação espacial da lei quanto à proteção dos dados pessoais e à privacidade. O MCI estabeleceu a aplicação da legislação brasileira para os casos em que qualquer etapa do ciclo do tratamento de dados tenha sido realizada no Brasil (coleta, armazenamento ou uso dos dados), inclusive, aos casos de pessoas jurídicas, sediadas no exterior, que ofertem serviço no Brasil. Nesse sentido, a LGPD vai além, pois prevê a aplicação da lei brasileira não apenas aos cidadãos brasileiros, mas toda e qualquer pessoa que esteja no Brasil, quando qualquer operação de tratamento de dados pessoais tenha sido realizada (Lima, 2020, p. 82).

Explica ainda assim a autora, que o âmbito de aplicação da LGPD perpassa, portanto, na consideração territorial do espaço digital, quanto ao conflito de jurisdições e de leis aplicáveis dele decorrentes, e sobre uma análise temporal (pelo decurso do tempo em que detém efeitos a LGPD). Quanto ao aspecto espacial, o artigo 3º da LGPD dispôs sua aplicação sobre os dados que tenham sido, embora tratados em outro território, coletados em território nacional, bem como sobre aqueles coletados e tratados no Brasil, além do tratamento relacionado à oferta de bens ou serviços aos titulares dos dados pessoais (2020, p. 74).

A LGPD vai além das fronteiras nacionais e alcança empresas e organizações estrangeiras que processam dados pessoais de indivíduos no Brasil. Essa abrangência

---

[6] Artigo 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de *internet* em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

extraterritorial é fundamentada no princípio de proteção dos direitos de privacidade e liberdade dos cidadãos brasileiros, independentemente da localização das empresas responsáveis pelo tratamento de seus dados. Significando que empresas estrangeiras que operam no Brasil ou que coletam dados pessoais de brasileiros devem cumprir as disposições da LGPD, garantindo a segurança e o tratamento adequado desses dados.

A exigência de mecanismos concretos para assegurar a segurança da informação está intrinsecamente ligada à proteção dos atributos personalíssimos do titular dos dados. A confidencialidade, a integridade e a disponibilidade dos dados são parâmetros essenciais para garantir que as informações pessoais permaneçam protegidas contra acesso não autorizado, alteração indevida ou indisponibilidade.

É evidente a ênfase dada pelo legislador à proteção dos dados pessoais, visando resguardá-los de acessos não autorizados e de eventos acidentais ou ilícitos que possam resultar em danos. Essa preocupação se manifesta em vários pontos da LGPD, refletindo o compromisso com o uso adequado e legal dos dados pessoais.

Nesse sentido, a segurança da informação é considerada um desdobramento de um novo direito fundamental à proteção de dados pessoais. À medida que a tecnologia avança, as pessoas estão cada vez mais expostas a possíveis violações de privacidade e a abusos no uso de suas informações pessoais. Assim, é fundamental que a legislação e as normas se adaptem a esse contexto, reconhecendo a importância da segurança da informação como parte integrante desse novo direito. (Lima, 2020)

As reflexões feitas na obra de Cíntia Rosa Pereira de Lima demonstram que a exigência de mecanismos concretos para atender ao imperativo de segurança descrito no dispositivo reverbera, em última instância, na proteção a atributos personalíssimos do titular; noutros termos, a segurança da informação é um desdobramento de um novo direito fundamental à proteção de dados pessoais, o que confere à norma em questão maior densidade axiológica no contexto propugnado pela norma, que deve se voltar ao atendimento de inúmeros parâmetros, como a confidencialidade, a integridade e a disponibilidade (2020, p. 351).

Além disso, a proteção dos dados pessoais vai além do aspecto individual. Ela contribui para a manutenção da confiança nas instituições, tanto públicas quanto privadas, e fortalece as relações de troca de informações em uma sociedade cada vez mais conectada. Quando as pessoas têm confiança de que suas informações estão protegidas, elas se sentem mais dispostas a compartilhar dados necessários para a realização de transações, pesquisas ou qualquer outra interação que envolva informações pessoais.

No entanto, a privacidade, devido à sua estreita ligação com os dados pessoais, está constantemente sendo comprometida, e a maioria das pessoas desconhece as implicações do compartilhamento de seus dados pessoais. Ao clicar em um botão em um site ou ao baixar um aplicativo para alterar a aparência de suas fotos em troca do envio de dados de reconhecimento facial e informações de registro em redes sociais, muitas vezes estão abrindo mão de sua privacidade sem perceber. O registro conveniente em um clique, a falta de informação sobre o que está sendo compartilhado e com quem, juntamente com a falta de compreensão dos riscos na *internet*, levam as pessoas a se exporem excessivamente na rede. A privacidade praticamente desaparece à medida que os dados pessoais são fornecidos de forma despreocupada, muitas vezes em nome de economizar tempo ou melhorar a experiência de uso da *internet*, ou em troca de experiências supostamente gratuitas. (Blum, 2022)

No mesmo sentido, frequentemente observa-se uma situação de monopólio efetivo no mercado. Nesse cenário, as empresas atuam fornecendo serviços aos consumidores e a outras empresas, desempenhando um papel crítico no tratamento dos dados dos consumidores. Isso gera um vasto conjunto de informações que têm o poder de reduzir os custos de transação no mercado, tornando-o mais eficiente. A eficiência é o que é comercializado para as empresas que oferecem produtos ou serviços.

Financeiramente, o lado dos consumidores é subsidiado pelo lado dos fornecedores, no entanto, existe uma contrapartida real que o indivíduo paga em forma de dados pessoais. Para que a empresa seja atrativa no segmento dos fornecedores, é necessário que ela tenha um grande volume de dados pessoais em processamento e que a utilização desses dados resulte em uma eficiência notável em comparação com os métodos tradicionais de comunicação com potenciais consumidores. O modelo de *two-sided market*[7] deve alcançar, ou chegar muito perto, de uma posição de monopólio no mercado de dados pessoais, a fim de atrair empresas fornecedoras de produtos ou serviços, ilustrando a dinâmica complexa e desafiadora do universo digital. (Moncau, 2020)

É evidente a delicadeza e a importância do bom manejo dos dados pessoais na *internet*, mas que apesar de ser obrigatório o consentimento e a concordância por parte do

[7] Plataformas que conectam dois lados de uma cadeia, conhecidos como “two-sided markets” — como fazem Uber, Airbnb e tantos outros. Esse modelo ficou famoso com o advento da *internet* e dos celulares, pois tal infraestrutura permitiu que pessoas fragmentadas em diversos pontos pudessem ser conectadas com maior facilidade sem a necessidade de grandes estruturas físicas e de seleção. É o compartilhamento de informações entre aqueles nas pontas, estabelecendo uma relação entre consumidor, servidor e interessado, aonde cada um possui um pedaço de informação/conteúdo que pode ser aproveitado pelo seguinte. Em síntese, é uma plataforma econômica intermediária com dois grupos de usuários distintos que oferecem benefícios de rede um ao outro (Vilas Boas, 2018).

usuário, se confia exclusivamente na figura do controlador para decidir e tratar essas informações.

3 O papel do operador e do controlador no tratamento de dados

É importante destacar que o operador de dados é considerado um processador de dados, enquanto o controlador é o responsável final pelas decisões relacionadas ao tratamento de dados. Ambos têm obrigações específicas para garantir a proteção dos direitos dos titulares dos dados e o cumprimento das leis de proteção de dados aplicáveis. Ambos controladores e operadores têm papéis distintos, mas interdependentes, no tratamento de dados pessoais, ao trabalharem em conjunto, eles garantem, em tese, que os dados sejam processados de forma segura, transparente e em conformidade com as leis de proteção de dados, protegendo assim os direitos dos titulares dos dados. Ao aprovar o texto da LGPD, o termo “responsável” foi substituído por “controlador”, pois é o agente que determina as decisões sobre o tratamento de dados pessoais, enquanto o “operador” realiza o tratamento em nome do “controlador” e seguindo as instruções deste (BRASIL, 2018).

Ambas figuras podem ser pessoas naturais ou jurídicas, de direito público e privado, definidas como controladoras quando atuarem de acordo com os próprios interesses, com poder de decisão sobre as finalidades e os elementos essenciais de tratamento, e operadoras quando atuarem de acordo com os interesses do controlador, podendo atuar apenas na definição de elementos não essenciais à finalidade do tratamento (BRASIL, 2018).

Para ilustrar, uma *startup* opta por enviar promoções aos seus clientes com o objetivo de impulsionar as vendas de um produto específico. Para isso, contratam uma agência de *marketing* digital, que elaborará a estratégia de divulgação com imagens de indivíduos utilizando o produto. A *startup* fornece todos os critérios para a campanha, incluindo o público-alvo e os requisitos para a aparência física dos modelos fotográficos. A agência de *marketing* digital trata dados pessoais para fornecer o serviço à *startup*, ao selecionar modelos fotográficos e armazenar suas imagens. Após a conclusão do serviço pela agência, um membro da equipe da *startup* envia as promoções aos clientes.

Neste exemplo, a *startup* atua como controlador, definindo o tratamento de dados e seus elementos essenciais. A agência de marketing digital age como operadora ao tratar os dados conforme a finalidade determinada pelo controlador. O funcionário, ao enviar os *e-mails* aos clientes, age sob a direção da *startup* e não é considerado um agente de tratamento.

Portanto, é evidente o poder de decisão que é concedido ao controlador, pois em que pese não realize sozinho todas as decisões de um certo processo, recai sobre ele a influência e controle das principais providências a serem tomadas, em síntese, as resoluções essenciais para o correto cumprimento da finalidade desejada.

Ao operador cabe realizar as medidas, normalmente técnicas, para dar o efetivo cumprimento naquilo determinado pelo controlador. Dentre as medidas pode-se citar a escolha do software que realizará o tratamento dos dados, bem como celebrar eventuais contratos e acordos para o sucesso da atividade, mas sempre sobre o guarda-chuva do limite imposto pelo controlador.

Apesar de terem funções distintas, quanto à responsabilidade, o artigo 42 da LGPD[8] determina que o controlador e o operador são solidariamente responsáveis pelos danos que causarem a outrem no exercício de atividade de tratamento de dados pessoais.

Sendo que, nas palavras de Cíntia Rosa Pereira de Lima, muito embora a lei não tenha estabelecido se tratar de responsabilidade objetiva ou subjetiva, entende-se que, pela própria estrutura de excludentes da responsabilidade civil, previstas no artigo 43 da LGPD[9], ser responsabilidade objetiva. Assim, a responsabilidade do controlador ou do operador somente pode ser afastada quando provarem a ocorrência das hipóteses ali destacadas (2020, p. 353).

Essa interpretação sugere que a responsabilidade pelo tratamento de dados pessoais é ampla e recai sobre os controladores e operadores, colocando a carga da prova sobre eles para demonstrar a ausência de responsabilidade. Essa abordagem visa fortalecer a proteção dos direitos dos titulares dos dados, incentivando o cumprimento das normas de privacidade e segurança estabelecidas pela LGPD (Roncatto, 2023)

Como bem observado por Fabiano Menke e Guilherme Goulart, o princípio da boa-fé objetiva está previsto no artigo 4.º, III, do Código de Defesa do Consumidor[10] e também no

---

[8] Artigo 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

[9] Artigo 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

[10] Artigo 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: (...) III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (Artigo 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;

caput do artigo 6.º da LGPD[11], quando esta enumera os princípios de proteção de dados. É preciso lembrar também da importância do Código Civil para a delimitação e limites das funções da boa-fé objetiva, quando a utiliza como apoio de verificação de licitude, de acordo com o artigo 187[12], cânone de interpretação, conforme o artigo 113[13] e cláusula geral dos contratos, no artigo 422[14]. Além disso, a boa-fé também é geradora de deveres, sobretudo com a consideração dos chamados deveres anexos e de proteção. É de se notar a importância do direito obrigacional em tais relações, pois, no mais das vezes, o tratamento de dados pessoais é acompanhado da prestação de um serviço ou fornecimento de produto, ou seja, não é o objeto principal da prestação. Assim, os deveres anexos e de proteção são plenamente aplicáveis às relações obrigacionais que envolvem tratamento de dados. Isso significa que há a possibilidade de a prestação principal ser perfeitamente adimplida, mas os deveres de proteção não. Essa relação, diante também do princípio da boa-fé objetiva, constitui um fundamento ético para a atividade, conforme um de seus aspectos. Trata-se de garantir a confiança na relação, no sentido de o sujeito confiar que seus dados serão adequadamente protegidos pelo responsável (2021, p. 342).

As condições estabelecem um ônus probatório para os controladores e operadores, exigindo que demonstrem a sua não participação nas ações que levaram à violação dos dados pessoais ou que o dano ocorreu devido a fatores além de seu controle, destacando a importância de cumprir com as obrigações e adotar medidas adequadas para evitar violações da legislação de proteção de dados pessoais.

A decisão histórica do Tribunal Constitucional alemão, no caso da Lei do Recenseamento de População, Profissão, Moradia e Trabalho de 25 de março de 1982, representa um marco na evolução do conceito de privacidade. O Tribunal argumentou que existia um direito à "autodeterminação informativa" com base nos artigos da Lei Fundamental que protegem a dignidade humana e o livre desenvolvimento da personalidade (Moncau, 2020). A lei em questão buscava coletar informações dos cidadãos sobre profissão, moradia e local de trabalho para fornecer dados à administração pública sobre crescimento populacional, distribuição espacial da população e atividades econômicas do país. No entanto, o Tribunal considerou parcialmente inconstitucional a lei, declarando nulos os dispositivos que

[11]Artigo 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...)

[12]Artigo 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

[13]Artigo 113. Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração.

[14]Artigo 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé.

permitiam a comparação dos dados coletados e sua transferência para outros órgãos da administração (Moncau, 2020).

Essa decisão estabeleceu os fundamentos da teoria da proteção de dados pessoais e influenciou as normas subsequentes em nível nacional e europeu, reconhecendo o direito subjetivo fundamental do indivíduo e colocando-o como protagonista no processo de tratamento de seus próprios dados. Assim, a decisão limitou o poder legislativo, exigindo a configuração de um direito à autodeterminação da informação (Moncau, 2020).

Aproveitando as lições de Laura Schertel Mendes, e conforme se observa, à medida que a tecnologia possibilita o armazenamento e a rápida e eficaz manipulação de dados pessoais, surge uma interligação entre a proteção da privacidade e as informações pessoais. Nesse cenário, ocorre uma modificação não apenas no conteúdo do direito à privacidade, mas também na terminologia utilizada, como a emergência de conceitos como privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros. Isso resulta em uma evidente evolução no âmbito teórico e prático do direito à privacidade, tanto na doutrina quanto na prática jurídica (2014, p. 32).

Como bem complementa a autora, e tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade (Mendes, 2014, p. 33).

O direito à privacidade é, inicialmente, um direito de status negativo, também conhecido como direito de liberdade ou direito negativo, pois impõe ao Estado o dever de não interferir (Menke, 2021). Em outras palavras, o respeito à privacidade implica em proibições ao Estado, protegendo a esfera jurídica do titular. A privacidade garante ao indivíduo o direito de não ser perturbado, preserva sua individualidade e identidade pessoal, e lhe concede o poder de resistir e agir contra o acesso de terceiros a seus direitos. O titular do direito à privacidade possui autonomia em sua vida privada, o que lhe permite excluir interferências de outras pessoas (aspecto positivo). Quando se trata de dados pessoais, que estão relacionados à vida privada da pessoa e fornecem informações sobre sua personalidade, o acesso e a manipulação desses dados estão condicionados ao respeito pela privacidade do titular.

Em suma, a privacidade desempenha um papel central no contexto da autodeterminação informativa, fornecendo aos indivíduos o controle e a capacidade de decidir

como suas informações pessoais são utilizadas, promovendo assim uma proteção adequada dos dados pessoais e preservando a dignidade e a liberdade dos indivíduos.

4 A finalidade do legítimo interesse

O legítimo interesse é elencado no inciso IX do já citado artigo 7º[15] como base legal capaz de autorizar o tratamento de dados pessoais.

A finalidade do princípio do legítimo interesse é fornecer flexibilidade para as organizações no tratamento de dados, por um mecanismo que busca encontrar um equilíbrio entre a necessidade de realizar determinadas atividades e a salvaguarda dos direitos fundamentais de privacidade e proteção de dados vistos acima.

O princípio reconhece que, em certas circunstâncias, pode haver um interesse legítimo para uma organização em coletar e tratar dados pessoais, mesmo na ausência de consentimento, desde que não prevaleça sobre os direitos e liberdades fundamentais dos indivíduos. Entretanto, conforme ver-se-á a seguir, o texto e a aplicação com a realidade são confusos e não refletem de forma totalmente precisa os princípios da lei. Situação bem exemplificada por Lima em sua detalhada obra, destacando que o uso legítimo dos dados pessoais pelo controlador só será válido para fins legítimos, os quais devem ser determinados com base em situações concretas (conforme estipulado no artigo 10[16] do mesmo diploma) (2020, p. 152).

Para ilustrar, considera-se um cenário hipotético em que um aplicativo de transporte, com o consentimento do usuário, armazena informações com o objetivo principal de identificar as áreas com maior demanda de usuários e os destinos mais comuns. No entanto, essa empresa não está autorizada a modificar o tratamento desses dados pessoais para outros propósitos sem obter previamente o consentimento legítimo do usuário.

---

[15] Artigo 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

[16] Artigo 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Outro exemplo envolve uma *startup* que solicita o endereço de e-mail do cliente exclusivamente para fins de autenticação no sistema. Nesse caso, não é permitido automaticamente utilizar esse endereço de e-mail para enviar ofertas ou publicidade. É evidente que, a partir da entrada em vigor da LGPD, não é mais admissível o tratamento de dados pessoais com propósitos genéricos ou indefinidos. O tratamento deve ser conduzido de forma específica, legítima, explícita e transparente, exigindo que as empresas informem claramente como cada dado pessoal será utilizado (Lima, 2020, p. 152).

Ainda como complementa a autora, é de se notar que o legislador, aparentemente ciente da indefinição do texto que inseriu nesse inciso, tentou melhor esclarecê-lo adiante, dedicando, para tanto, todo o artigo 10, o que causa uma confusão maior ainda. O problema é que o artigo 10 contém redação de duvidosa qualidade, não apenas sob o prisma da técnica legislativa, mas da própria expressão da linguagem: define algo por ele mesmo. É assim que o tal legítimo interesse só poderá fundamentar tratamento de dados para finalidades legítimas. E estas incluem, mas não se limitam ao que dizem os dois incisos que seguem o caput do artigo 10. Ou seja, o artigo ao mesmo tempo que define, deixa sem definição sobre a abrangência desse princípio, tornando fraca a segurança daquilo que ele mesmo deveria fortalecer (Lima, 2020, p. 153).

Ainda da análise do artigo 10, Cíntia Rosa Pereira de Lima faz uma perfeita síntese sobre as falhas e fragilidades do texto, pois quando se examinam os dois parágrafos, a situação torna-se ainda mais nebulosa. O primeiro considera finalidade legítima como o apoio e promoção das atividades do controlador. Mas que atividades exatamente se enquadram nessa definição? A Lei não especifica. Seria qualquer atividade, então? Independentemente do que o controlador faça, apoiar ou promover essas atividades automaticamente se tornam finalidades legítimas aos olhos da Lei? (2020, p. 154).

Por outro lado, o segundo parágrafo do artigo 10 declara: "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei". A presença de vários pronomes oblíquos e possessivos introduz ambiguidade no texto. A quem se referem os "seus" direitos - são os direitos do titular ou do controlador mencionado no parágrafo anterior? Da mesma forma, quem é o beneficiário (substituído pelo pronome "o"): o titular ou o controlador? De quem são as "legítimas" expectativas mencionadas no parágrafo, que se dizem ser "dele"? (Lima, 2020, p. 155).

Como ressaltado pela autora citada, parece que este parágrafo do texto nacional é nada mais que uma versão simplificada, fraca e mal elaborada do recital número 47 da lei europeia,

que, em sua extensão, tenta estabelecer diretrizes interpretativas para determinar o que constitui o tal legítimo interesse que será mencionado posteriormente no artigo 6 da mesma norma (UE, 2018) . A transparente opção do legislador em fazer o texto legal de forma ambígua, é o que faz a compreensão do artigo difícil, pois ao dedicar o trecho a este princípio, leva a imaginar que será feita uma afunilação dos princípios norteadores daquele tratamento tão delicado, mas no final apenas enche de mais incertezas aquele que terá que aplicá-lo[17] (Lima, 2020, p. 155).

Na tentativa de elucidar o que diz esse segundo inciso, a autora arrisca definir como a defesa dos direitos do controlador, nas relações jurídicas que beneficiem o titular, consideradas as expectativas razoáveis deste, bem como seus direitos e liberdades. Entretanto, não se compreende a razão de não relacionar taxativamente os princípios balizadores, deixando ao puro bom senso dos operadores e controladores definir se nossos dados pessoais são passíveis de encaixe nesse rol (Lima, 2020, p. 155).

Seja qual for a circunstância fática definida nessa permissão, o parágrafo 1° do artigo 10 determina que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. No parágrafo 2°, do mesmo artigo, exige-se do controlador a adoção de medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

A questão principal é que vive-se em um mundo em que o processamento de dados pessoais é realizado de forma ininterrupta por diversos agentes do mercado, que buscam a todo momento, obter vantagens competitivas frente a seus concorrentes. Durante muito tempo o direito à privacidade do artigo 5º, X, da Constituição Federal foi suficiente para resguardar o titular dos dados de tratamentos abusivos, contudo, os interesses do mercado começaram a

[17]Considerando n°47 - Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta (UE, 2018).

conflitar com os direitos fundamentais dos indivíduos e o poder de um cidadão em lutar contra os monopólios de dados é mínimo. Ainda mais quando a legislação que foi construída para resguardar esse tão valoroso princípio constitucional abre brechas para interpretações (Lima, 2020).

É comum que os controladores utilizem essa base legal para atividades de *marketing*, promoção de produtos e prospecção de clientes. Nesses casos, os controladores realizam o tratamento de dados pessoais com o objetivo de aumentar as vendas, a receita e oferecer um serviço ou produto mais completo para os clientes, obtendo benefícios diretos a partir desse tratamento de dados.

É válido citar a legítima expectativa como ponto de interesse, já que por muitos é usada como suporte para validação do uso desenfreado do legítimo interesse. A legítima expectativa prevê que seja aproveitada a coleta de dados quando seu uso, mesmo que não autorizado, sirva para promover produto e serviço que o consumidor já esteja com a expectativa de usufruir. Um exemplo bastante comum é o monitoramento do histórico de compras do cartão de crédito realizado pelos bancos, a fim de identificar movimentações estranhas e possíveis roubos, o que é um benefício de segurança ao cliente.

Deve-se considerar qual seria a expectativa razoável de uma pessoa comum diante da relação jurídica que mantém com o controlador, frequentemente representado por alguém que presta serviços ou vende produtos ao titular. Em outras palavras, é necessário ponderar qual seria a concepção predominante dentro de uma comunidade, de acordo com suas normas e práticas comuns. (Lima, 2020)

Em fevereiro de 2024, a ANPD emite um *guia orientativo das hipóteses legais de tratamento de dados pessoais quanto ao legítimo interesse*, admitindo a obscuridade da lei neste sentido, e tentando - de modo falho - direcionar o agente para realizar o bom tratamento. No documento, a entidade indica que o tratamento de dados com respaldo no legítimo interesse deve ser precedido de um teste de balanceamento, que considera de um lado os interesses do controlador ou terceiro, e de outro, os direitos e liberdades fundamentais dos titulares. Ocorre que, a utilização do procedimento proposto é apenas sugestivo, permitindo que cada organização realize o equilíbrio pela metodologia mais adequada à sua realidade organizacional e às especificidades do tratamento realizado (BRASIL, 2024).

Porém, tal interpretação assume uma relação de confiança e igualdade, agora quando o titular de dados não possui qualquer relação jurídica com o controlador, nunca contratou com este para nenhum serviço ou nenhuma compra, a questão da legítima expectativa ganha outros contornos. Um exemplo: no caso de alguém que nunca tenha feito cadastro em determinado

site e receba e-mails de promoção deste, a análise da legítima expectativa se torna mais difícil. É comum na legislação encontrar expressões vagas e indeterminadas, o que a torna mais sujeita a interpretações. A falta de definições específicas na LGPD a diferencia do GDPR, seu pilar basilar, levando ao afastamento de seu propósito original e criando espaço para situações que geram insegurança jurídica (Oliveira, 2020).

E como é notório em nosso dia a dia, a realidade não condiz com o texto legal, e que por diversas vezes ao longo dos dias recebe-se mensagens, e-mails e ligações de empresas e serviços que nunca fora contratada e surge o questionamento: como é que essa empresa tem meus dados? A previsão (ou falta dela) legal que gere o tratamento de dados pessoais é a situação que dá causa à violação do direito fundamental. Não há espaços para interpretações quando o objeto da discussão é a privacidade e os dados pessoais do cidadão, a legislação deve ser taxativa, e prever todas as hipóteses de tratamento de dados.

Isso porque a evolução traz um risco maior que somente ter o número de CPF, ou a conta bancária vazados, um objeto móvel como *smartphones* contém informações de hábitos, costumes, preferências e relações sociais - ao sair de casa com o celular no painel do carro, se dirigir até a escola das crianças e em seguida ao trabalho, realizando esse trajeto todos os dias da semana, por anos, utilizando um aplicativo de GPS, irá conter mais informações do que se imagina. Essa simples tarefa cotidiana contém dados de horários de saída e chegada nos locais, itinerário utilizado, geolocalização, pessoas que lhe acompanham, velocidade aplicada e hábitos de direção.

O aplicativo de GPS, utiliza de todas essas informações para sugerir a melhor rota até o ponto final, realizando até mesmo uma comparação com os dados dos demais usuários da via para otimizar o trajeto, sugerindo sempre o caminho mais eficiente.

Na mesma linha de ações cotidianas, está o acesso às academias e estabelecimentos sociais, que muito comumente utilizam de biometria ou *scan* facial como método de ingresso. Além destes métodos serem uma forma única de reconhecimento e identificação de uma pessoa, eles carregam consigo as informações de horário de chegada e saída, frequência de comparecimento, condição de saúde e, no mínimo, dados de pagamento (Lima, 2020).

Da mesma forma, ao assistir um vídeo no *YouTube*, incluindo ali informações referentes ao gosto musical, qual o tipo de informação buscada, tempo de retenção de tela, assuntos de preferência, rejeição, e infinitos outros elementos que se pode ficar nomeando, desta e de outras atividades cotidianas.

Uma parcela significativa do êxito dessa prática voltada para a vigilância reside no fato de que sempre há um incentivo para compartilhar informações pessoais. Em troca de

dados, frequentemente se recebe acesso a conteúdo exclusivo, experiências personalizadas ou o pleno uso de serviços. É este o valor que atualmente se confere aos dados pessoais - um benefício de pequena escala.

Ou seja, ao praticar essas ações, se fornece dados não somente de identificação, mas sim informações intrínsecas de pessoalidade do digitador, do que se gosta, por onde se anda, e a pessoa com quem se mantém relacionamentos, entre outros.

É evidente que as informações são úteis até mesmo para a própria utilização dos aplicativos, que são criados para aquele objetivo, e o usuário o instala buscando aquele resultado e eficiência. Porém, fica claro que essas informações de hábitos e preferências são até mais delicadas e pessoais que os dados de CPF e conta bancária, pois se de alguma forma o detentor destes dados usar do princípio do legítimo interesse para repassá-los à um terceiro, que utilizará das informações para promover seus serviços ou até mesmo manipulá-los de forma maliciosa, buscando aproveitar-se dos dados para cometer crimes, estará trazendo um prejuízo irreparável ao usuário.

De amplo debate na comunidade internacional, é a busca pelo consentimento informado livre e esclarecido, que ultrapassa o mero clique no “li e aceito” ou no “li e concordo”, mas que traz para toda aquela ocasião especial, aonde há a manipulação de dados aquém do básico para operação, uma confirmação adicional para o usuário, consentindo para aquela finalidade determinada. Esse conceito de consentimento é trazido até mesmo no próprio texto da LGPD, aonde em seu artigo 5°, XII, traz a definição de consentimento, como: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”, demonstrando por mais uma vez a ambiguidade e deficiência do legítimo interesse, evidenciando que se é realizado toda uma conceituação acerca da privacidade, para em seguida flexibilizá-la (BRASIL, 2018)

Cumpre esclarecer que este trabalho não tem como objetivo coibir toda a forma de promoção de serviços e produtos que utilizem o *cross data*[18] - mas sim possibilitar que o cidadão tenha o poder sobre essas informações, que lhe seja ofertado a condição de explicitamente consentir com a manipulação de seus costumes e preferências, e principalmente que a legislação de seu País não permita - a mínima possibilidade - de um controlador ou operador trabalhar sobre a linha cinzenta da omissão e da interpretação.

[18]Cross data é a realização de cruzamento e análise de dados de diferentes canais, nos quais os cientistas de dados são capazes de identificar segmentos de público e segmentação comportamental que podem ser usados para atingir usuários por meio de campanhas publicitárias online. Estes dados são uma fonte preciosa de informação sobre quem são os seus clientes. Incluindo dados demográficos, dados sobre os seus interesses e comportamentos de compra online (Cortês, 2024).

A necessidade de existir uma rigidez alta sobre esse tema reside especificamente na delicadeza já demonstrada, que é somada ao alto nível de irrecuperabilidade do prejuízo, uma vez que não é possível voltar atrás em um vazamento de dados, sendo que em posse das informações pessoais de um indivíduo, o controlador mal intencionado poderá fazer o que bem entender com elas.

O entendimento sobre o assunto nos Tribunais de Justiça ainda é raso, sendo que a maioria das decisões ainda estão sendo proferidas em sede de 1° grau, uma vez que a própria legislação ainda está sendo lentamente abordada nesse sentido. O Supremo Tribunal de Justiça, através da Segunda Turma, firmou recentemente entendimento que o titular de dados vazados deve comprovar dano efetivo ao buscar indenização[19]. Em contrapartida, a 26ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo, entende que a mera divulgação de dados pessoais do autor em página eletrônica, acessível por terceiros, ainda que por curto período de tempo, é hábil a ensejar indenização por danos morais[20].

Outra consequência da forma em que o legítimo interesse foi designado na LGPD, são os inúmeros projetos de lei em tramitação no poder legislativo, sugerindo alterações na Lei n° 13.709/18 para aplicá-la com mais rigidez no tratamento de dados. Dos mais interessantes projetos, destaca-se o PL n° 4960/2019, que regulamenta as informações dispostas em plataformas de informação de grande escala, e busca dar total iniciativa, critério e poder de consentimento ao titular dos dados, impedindo que qualquer controlador externo manipule dados sem o consentimento do usuário através de uma experiência simples, eficiente e segura, detalhando especificamente a finalidade determinada para aquela ação, tendo inclusive o cidadão a possibilidade de revogar a qualquer momento a autorização antes concedida. Salienta-se também os PLs n° 4901/2019 e n° 522/2022, que conceituam verificação biométrica e dado neural, respectivamente, e em ambos os casos obrigam o consentimento expresso e inequívoco do indivíduo proprietário dos dados, proibindo interpretações tácitas e utilização de legítimo interesse por parte dos controladores e operadores.

Por mais que debater eventuais responsabilizações não seja o objeto deste artigo, traz-se os entendimentos e projetos para demonstrar que a prestação jurisdicional, bem como o próprio Poder Legislativo, estão com dificuldades em cobrir a falha deixada pelo texto legal, e em suas decisões e ideias demonstram através da controvérsia, que o assunto está longe da pacificação e da resolução de problemas.

---

[19]AREsp n. 2.130.619/SP, relator Ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, DJe de 10/3/2023.

[20]TJSP; Apelação Cível 1003122-23.2020.8.26.0157; Relator (a): Renato Sartorelli; Órgão Julgador: 26ª Câmara de Direito Privado; Foro de Cubatão - 4ª Vara; Data do Julgamento: 22/06/2021; Data de Registro: 22/06/2021

5 Considerações finais

Este estudo ateve-se em demonstrar a clara ausência de vontade do legislador em construir mecanismos eficientes na proteção dos dados pessoais. A criação da Lei Geral de Proteção de Dados, embora baseada na eficiente *General Data Protection Regulation* europeia, falha em não abraçar a parte mais robusta e protecionista do texto estrangeiro, deixando de tutelar na totalidade as informações pessoais inseridas nos bancos de dados. Embora queira que o agente aja com base nos princípios da boa-fé, dar a liberdade para agir sobre dados delicados com discricionariedade torna a legislação fraca e passível de interpretações conturbadas.

Vale destacar, que a competência da Autoridade Nacional de Proteção de Dados em aplicar sanções administrativas como multas e advertências não resolve a omissão do texto legal, visto que os efeitos de um tratamento irregular de dados são imediatos, trazendo prejuízos ao titular no momento seguinte ao gerenciamento das informações, posto que é impossível desfazer um envio de propaganda para a caixa de e-mail, excluir uma informação de preferência já utilizada e aplicada, ou impedir o compartilhamento de dados vazados.

O princípio do legítimo interesse, destacado principalmente pelos artigos 7°, IX e 10° da Lei n° 13.709/18 é omisso e frágil, a função da criação de uma lei específica serve justamente para especificar e delimitar os direitos, e não deverá servir como muleta para utilização de operadores de forma cinzenta, trabalhando na linha tênue do consentimento não expresso do cidadão e do oferecimento de serviços personalizados.

Em um mundo cada vez mais digital, em que por diversas vezes se expõe dados de preferências, costumes e identificação para diferentes controladores, é primordial que se avance em busca do consentimento e da proteção daquilo que é intrínseco ao homem, promovendo seu livre arbítrio, garantindo os direitos constitucionais de forma direta, sem textos omissos que abrem possibilidade para que cada um faça a definição do seu próprio legítimo interesse, visando não somente adotar uma legislação específica sobre o tema, mas sim criar um modelo regulatório eficiente.

Referências

BLUM, Rita Peixoto F. **O Direito à Privacidade e a Proteção dos Dados do Consumidor**. São Paulo: Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556277066. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277066/. Acesso em: 18 mai. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.** Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 mai. 2023.

_____. **Constituição da República Federativa do Brasil de 1988**. Promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 mai. 2023.

_____. **Lei n° 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 18 mai. 2023.

_____. **Lei n° 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília. Disponível em: www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 18 mai. 2023.

CORTÊS, Adriano. O tráfego da Internet faz campanhas de marketing focadas. **Ph3a**, 2024. Disponível em: https://www.ph3a.com.br/blog/o-trafego-da-internet-faz-campanhas-de-marketing-focadas/. Acesso em: 10 abr. 2024.

DPO EUROPE GMBH. **Regulamento Geral sobre a Proteção de Dados (RGPD, GDPR)**. 2018. Disponível em: https://gdpr-text.com/pt/ - acesso em 15 jun. 2023.

LIMA, Cíntia Rosa P.. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 18 mai. 2023.

_____. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados** : de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco civil da *Internet* (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo Almedina Brasil, 2020 1 recurso online (Teses). ISBN 9788584936397. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788584936397. Acesso em 15 jun. 2023.

MALDONADO, Viviane. **LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de implementação.** 3. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2022.

MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - **Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental**, 1ª Edição. São Paulo: Editora Saraiva, 2014. E-book. ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502218987/. Acesso em: 03 jun. 2023.

MENKE, Fabiano; GOULART, Guilherme. Segurança da informação e vazamento de dados. In: BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JR., Otavio Luiz Rodrigues (coords.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 339 – 360.

MONCAU, Luiz. **Direito ao Esquecimento: Entre a Liberdade de Expressão, a Privacidade e a Proteção de Dados Pessoais**. São Paulo (SP): Editora Revista dos Tribunais. 2020. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/2-os-fundamentos-de-um-direito-ao-esquecimento-direito-ao-esquecimento-entre-a-liberdade-de-expressao-a-privacidade-e-a-protecao-de-dados-pessoais/1201075293. Acesso em 22 mai. 2023

OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPD: Lei Geral de Proteção de Dados Pessoais**. 1ª Edição. São Paulo: Thomson Reuters Brasil, 2020.

PRETTI, Mariana. Big Data: entenda o que é e para que serve esta tecnologia revolucionária. **C2ti**, 2018. Disponível em: https://c2ti.com.br/blog/big-data-entenda-o-que-e-e-para-que-serve-esta-tecnologia-revolucionaria. Acesso em: 05 out. 2023.

RONCATTO, Carolina. **Efetividade da tutela dos direitos de personalidade no processo informacional: da privacidade aos desafios da proteção de dados.** Revista de Direito Civil Contemporâneo. Volume 36. ano 10. São Paulo: Ed. RT, jul./set. 2023. Disponível em: https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a0000018b72ab3809641a8e36&docguid=Ia0c5a090462311eebb1dc6d97f43e091&hitguid=Ia0c5a090462311eebb1dc6d97f43e091&spos=2&epos=2&td=2016&context=18&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1. Acesso em: 05 out. 2023.

UE. **The European Parliament and of The Council. Considerando 47 da General Data Protection Regulation (EU GDPR)**. 2018. Disponível em português em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 22 mai. 2023.

VILAS BOAS, Artur. Começando um marketplace: um guia para o próximo “Uber de X”. **Medium**, 2018. Disponível em: https://medium.com/deep-wylinka/come%C3%A7ando-um-marketplace-um-guia-para-o-pr%C3%B3ximo-uber-de-x-d85397d1144e. Acesso em: 22 mai. 2023.