
Data protection: an analysis of the principle of purpose.

Proteção de dados: uma análise sobre o princípio da finalidade.

Received: 2023-04-16 | Accepted: 2023-05-20 | Published: 2023-05-29

Vítor Hugo Póvoa Villas Boas

ORCID: <https://orcid.org/0000-0002-8370-1763>

Universidade Federal do Tocantins-UFT/Escola Superior da Magistratura Tocantinense-ESMAT, Brasil

E-mail: vitorvbmestrado@gmail.com

Gustavo Paschoal Teixeira de Castro Oliveira

ORCID: <https://orcid.org/0000-0002-3045-2097>

Universidade Federal do Tocantins-UFT/Escola Superior da Magistratura Tocantinense-ESMAT, Brasil

E-mail: paschoal@mail.uft.edu.br

Rodrigo de Lima Vaz Sampaio

ORCID: <https://orcid.org/0000-0002-3831-705X>

CEU Law School/São Paulo, Brasil

E-mail: limavsampaio@uol.com.br

ABSTRACT

The General Data Protection Law – LGPD strengthened the protection of personal information at the national level and equated it with international legal discipline. Inspired by the General Data Protection Regulation – GDPR, the LGPD establishes the principle of purpose as one of the keys to understanding it. In the search to better reflect on the performance of the principle of purpose in the context of the General Data Protection Law – LGPD, through a qualitative and revisional approach, this article aimed to present some reflections on the importance of the principle of purpose in the application of the LGPD. From the theory of the principles of Humberto Ávila it was found that the principle of purpose goes beyond the boundaries of norm of orientation to constitute an instrument of delimitation and action in the search for the protection of personal data in the context of contemporary life, directing the LGPD to new horizons regarding the relational process of personal rights of a fundamental nature and the purpose as a principle.

Keywords: LGPD; Digital Law; Principle of Finality; Theory of Principles; Protection of sensitive data.

RESUMO

A Lei Geral de Proteção de Dados – LGPD robusteceu a tutela das informações pessoais no âmbito nacional e a equiparou à disciplina jurídica internacional. Inspirada no *General Data Protection Regulation – GDPR*, a LGPD estabelece o princípio da finalidade como uma das chaves para compreendê-la. Na busca de melhor refletir sobre a atuação do princípio da finalidade no contexto da Lei Geral de Proteção de Dados – LGPD, por meio de uma abordagem qualitativa e revisional, o presente artigo teve como objetivo apresentar algumas reflexões sobre a importância do princípio da finalidade na aplicação da LGPD. A partir da teoria dos princípios de Humberto Ávila verificou-se que o princípio da finalidade ultrapassa as fronteiras de norma de orientação para se constituir em instrumento de delimitação e ação na busca da proteção dos dados pessoais no contexto da vida contemporânea, dirigindo a LGPD a novos horizontes quanto ao processo relacional dos direitos pessoais de natureza fundamental e a finalidade como princípio.

Palavras-chave: LGPD; Direito Digital; Princípio da Finalidade; Teoria dos Princípios; Proteção de dados sensíveis.

INTRODUÇÃO

A revolução digital ou do computador, ocorrida na década de 1960, impulsionou o surgimento de novos modelos de negócios, dentre eles, o da mercantilização dos dados pessoais, através da coleta e tratamento.

Hoje, a informação é verdadeira moeda. Através dela, o Estado e as empresas tornam-se mais eficientes porque são capazes de conhecer as necessidades e desejos das pessoas de modo antecipado, o que permite o melhor gerenciamento dos recursos para a consecução dos objetivos almejados. No caso das empresas, a finalidade precípua é o lucro; já para o Estado, o bem-comum.

Desse modo, pode-se afirmar que a informação é poder, e, por essa razão, a sua coleta e tratamento indiscriminado representa uma ameaça à liberdade dos indivíduos e à democracia. Não é à toa que nos governos totalitários sempre houve um controle ferrenho das informações.

Nesse contexto, para fins de se evitar um colonialismo digital, fez-se necessária a regulamentação da matéria através de instrumentos jurídicos que garantissem o direito à privacidade e propiciassem meios para que a coletividade fiscalizasse e controlasse os seus dados.

Além disso, por se tratar de um tema de relevância global e em razão da imaterialidade dos dados e da ausência de fronteiras no cyber espaço, os países adotaram uma disciplina baseada em princípios e fundamentos comuns.

No Brasil, a regulamentação da matéria se deu com a Lei Geral de Proteção de Dados – LGPD, de 14 de agosto de 2018, que, segundo o seu art. 1º “dispõe sobre o tratamento de dados pessoais [...] com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

Apesar de publicada em 2018, a lei entrou em vigor de modo progressivo, sendo a última etapa concluída em 14 de agosto de 2020, isto é, 24 (vinte e quatro) meses após a data de sua publicação.

Dito isso, as empresas e demais entidades precisam se readequar a fim de cumprir o regramento sobre a proteção de dados, sob pena de aplicação das sanções administrativas previstas no art. 52 da referida lei.

Na busca de melhor compreender tais questões o presente artigo, a partir de uma abordagem qualitativa e revisional, desenvolverá de reflexões sobre a perspectiva jurídica da proteção de dados e sua relação com o princípio da finalidade, principalmente quanto ao papel do Estado na busca da proteção dos dados pessoais como direito fundamental do ser humano na contemporaneidade.

Assim, visando a boa compreensão da Lei de Proteção de Dados – LGPD, que exige a análise de um dos seus maiores princípios: a finalidade, a primeira seção tratará dos princípios jurídicos, numa perspectiva revisional a partir do pensamento de Humberto Ávila.

Firmado os pontos fundamentais sobre a teoria dos princípios, será abordada questões específicas sobre a privacidade como direito, para na sequência, se estabelecer a relação entre a proteção de dados e o princípio da finalidade.

Ao final serão abordadas algumas questões sobre a transparência e o tratamento de dados pessoais e o quadro desse tratamento na União Europeia e seu impacto ao tratamento dado na ordem jurídica brasileira com a implantação definitiva da LGPD.

OS PRINCÍPIOS JURÍDICOS

Considerando que a finalidade está prevista no rol de princípios que regem a proteção de dados no Brasil, a compreensão do assunto exige a análise preliminar sobre a conceituação e a distinção entre os princípios jurídicos e as regras.

De início, ressalta-se que o tema é controvertido, o que dificulta a identificação de um denominador comum entre os diferentes métodos elaborados pelos jusfilósofos. Para fins de elucidação, vários foram os autores que se debruçaram sobre o tema, a exemplo de Josef Esser, Karl Larenz, Ronald Dworkin, Robert Alexy, Humberto Ávila etc.

Outro ponto a ser destacado é que a exposição sobre os diferentes critérios para identificação dos princípios e das regras não é o cerne deste artigo, mas apenas um meio para o melhor entendimento acerca da interpretação e aplicação da finalidade na coleta e processamento de informações pessoais.

A reflexão sobre os princípios e as regras perpassa a noção de “norma jurídica”, pois ambas são comumente classificadas como espécies normativas. Para Humberto Ávila (2021), norma jurídica não se confunde com texto normativo. Aquela é o resultado da interpretação deste. Há casos em que de um único dispositivo legal é possível extrair diversas normas. Em outros, há texto, porém, não há norma, a exemplo do preâmbulo da Constituição Federal de 1988.

Isso demonstra que a interpretação é um processo de construção e reconstrução do sentido, conforme expõe Ávila:

De um lado, a compreensão do significado como o conteúdo conceptual de um texto pressupõe a existência de um significado intrínseco que independa do uso ou da interpretação. Isso, porém, não ocorre, pois o significado não é algo incorporado ao conteúdo das palavras, mas algo que depende precisamente de seu uso e interpretação, como comprovam as modificações de sentidos dos termos no tempo e no espaço e as controvérsias doutrinárias a respeito de qual o sentido mais adequado que se deve atribuir a um texto legal. Por outro lado, a concepção que aproxima o significado da intenção do legislador pressupõe a existência de um autor determinado e de uma vontade unívoca fundadora do texto. Isso, no entanto, também não sucede, pois o processo legislativo qualifica-se justamente como um processo complexo que não se submete a um autor individual, nem a uma vontade específica. Sendo assim, a interpretação não se caracteriza com um ato de descrição de um significado previamente

dado, mas como um ato de decisão que constitui a significação e os sentidos de um texto (ÁVILA, 2021, p. 51-52).

Com efeito, isso não significa que o intérprete é livre para atribuir qualquer sentido a um enunciado normativo. As palavras possuem núcleos de sentido preexistentes que constituem o ponto de partida do intérprete. Desse modo, o próprio texto estabelece limites à construção de sentidos (ÁVILA, 2021).

Dito isso, a distinção da norma jurídica em princípio ou regra não é pré-constituída ao processo interpretativo, isto é, dada em caráter antecedente ao ato do intérprete. Na verdade, a definição entre uma ou outra é resultado da construção e reconstrução de sentido do texto. Portanto, não é o texto legal que distinguirá uma espécie da outra, mas sim a atividade do intérprete.

Mencionada a diferença entre norma e texto normativo, passa-se ao exame dos critérios empregados pela doutrina para classificar aquela como princípio jurídico ou regra.

Em linhas gerais, a construção do conceito de princípio está, de certo modo, contraposta ao de regra. A depender dessa conceituação, as diferenças entre as espécies podem ser classificadas como quantitativas ou qualitativas.

Quantitativa é a tese que distingue princípios e regras em razão do grau de generalidade, abstração ou fundamentalidade. Com base nesse critério, o princípio jurídico é considerado mais geral e abstrato que a regra, e, além disso, apresenta um maior grau de fundamentalidade, pois orienta o legislador na edição de novas leis, e o intérprete, na aplicação do direito. Por outro lado, a regra se caracteriza pela especificidade e maior concreção.

Qualitativa é a distinção de natureza lógica, baseada no modo de aplicação e no relacionamento normativo entre princípios e regras, cujos principais expoentes foram Esser, Larenz, Canaris, Ronald Dworkin e Robert Alexy.

Segundo Ávila (2021), os critérios usualmente usados na abordagem qualitativa para diferenciar as espécies normativas são os seguintes: 1) Caráter hipotético-condicional; 2) Modo final de aplicação; 3) Relacionamento normativo; e 4) Fundamento axiológico.

De acordo com o primeiro critério, as regras são aplicadas ao modo *se, então* – à hipótese normativa segue uma consequência predeterminada. Os princípios, por outro lado, apresentam apenas uma diretriz a ser utilizada pelo intérprete para, em momento posterior, encontrar a regra aplicável ao caso.

Com base no segundo critério, a aplicação das regras segue a lógica do *tudo ou nada* – preenchida a hipótese de incidência, ou a regra é válida e, portanto, deve ser aplicada ao caso concreto, ou ela é inválida. Já os princípios jurídicos obedecem à dinâmica do *mais ou menos*, pois contêm apenas fundamentos que devem ser conciliados com os fundamentos dos demais princípios.

No terceiro critério, a distinção entre as espécies normativas baseia-se no método de solução em caso de conflito. Quando duas regras são conflitantes há verdadeira antinomia, solucionável mediante a declaração de invalidade de uma das regras ou a criação de uma exceção. Em sentido oposto, os princípios colidentes são submetidos à ponderação de acordo com a sua relevância para o caso concreto.

Por fim, o quarto critério considera que o fundamento axiológico da decisão a ser tomada reside nos princípios, e não nas regras.

Finda a exposição preliminar sobre as diferenças entre princípios e regras, passa-se ao estudo acerca do direito à privacidade e sua correlação com a proteção de dados.

A PRIVACIDADE

A computação, a internet, o comércio eletrônico e as redes sociais ampliaram os horizontes de atuação do homem contemporâneo, e o moldaram de tal maneira que é impossível imaginar a vida humana sem estes recursos. Trata-se de um fenômeno irreversível.

Junto com o avanço da técnica, surgiram novos meios para a coleta e tratamento de dados, caracterizados pela alta eficiência e baixo custo, em nítido contraste aos métodos utilizados anteriormente, os quais demandavam uma complexa e onerosa estrutura para a obtenção e processamento das informações, o que, até então, só era viável ao Estado.

Com a redução dos gastos e a elevada qualidade dos dados angariados, as empresas e demais entidades privadas passaram a coletá-los e tratá-los com o objetivo de conhecer melhor as necessidades dos consumidores a fim de supri-las.

Vários foram os ganhos propiciados ao sistema capitalista em razão da computação e da internet. Porém, com os avanços vieram também as preocupações: O progresso da ciência representaria uma ameaça à intimidade? Como o Estado deveria lidar com essa questão? A esfera individual estaria fadada a reduzir-se?

Pairava no ar o temor de que o “Admirável Mundo Novo” (*Brave New World*), de Aldous Huxley, e o Grande Irmão, retratado na obra “1984”, de George Owen, se tornassem realidade.

Nesse contexto, os debates acerca da privacidade afloraram.

As reflexões sobre esse tema não são recentes. Desde os tempos mais remotos é possível constatar noções sobre o privado e o público, o individual e o coletivo.

Com efeito, discute-se se o direito à privacidade estaria radicado na própria natureza humana e, portanto, seria geral, universal e atemporal, devendo ser efetivado através das leis positivadas, ou se, na verdade, seria uma construção histórica, mutável de acordo com as particularidades de cada sociedade, considerando as contingências sociais, políticas, econômicas, religiosas.

Para Alan F. Westin (1967), as origens da esfera privada remontam não à natureza racional humana, mas, antes, à sua animalidade. Ao observar o modo de agir dos animais, constata-se que em determinados períodos estes se segregam dos seus companheiros de espécie, permanecendo solitários ou formando grupos menores. Ademais, é próprio do instinto animal a territorialidade, pelo qual o organismo exerce o domínio sobre determinada área, apropriando-se dela, e, por conseguinte, defendendo-a contra invasões de terceiros.

Westin (1967) afirma ainda que, por mais distintas que sejam as sociedades, a exemplo das tribos de índios isolados da Amazônia e das pessoas que vivem nas metrópoles brasileiras, sempre existiriam noções elementares acerca da privacidade.

Por outro lado, Rodotà sustenta que “ em um nível social e institucional [...] o nascimento da privacidade não se apresenta como a realização de uma exigência “natural” de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo (RODOTÀ, 2008, p. 27)”

Desse modo, por se tratar de uma construção histórica, variável de acordo com as peculiaridades de cada povo, reduzir a privacidade a uma definição geral e universal é tarefa difícil, senão impossível (DONEDA, 2019).

Não obstante, ainda que presente ao longo da história, a configuração e sistematização da privacidade tal qual a conhecemos hoje está vinculada à ascensão da burguesia, classe marcada pelo seu forte componente individual e patrimonialista; às novas técnicas de construção habitacional, as quais permitiam a separação dos cômodos e, em especial, do local de trabalho e do lugar onde se vive (distinção entre casa e escritório); e, às transformações socioeconômicas decorrentes da Revolução Francesa (RODOTÀ, 2008).

Isolar-se em um quarto, recolher-se no recôndito do lar, afastar-se da sociedade e dedicar-se a atividades solitárias eram “privilégios” da classe burguesa, que, em grande parte, só foram possíveis graças a existência de condições materiais para tanto, isto é, à propriedade privada. Trata-se, portanto, de um direito “elitista”. Desse modo, é possível afirmar que “pobreza e privacidade estão intimamente e inversamente ligadas” (BANDICH, 1966, p. 414).

No campo jurídico, o marco doutrinário sobre o assunto foi o artigo intitulado “*The Right to Privacy*”, escrito em 1890, por Warren e Brandeis, no qual consta a noção de privacidade como direito de “ser deixado só” (“*to be let alone*”). Não por coincidência, a motivação para a escrita do texto pelos juristas norte-americanos decorre justamente do impacto da tecnologia na esfera privada das pessoas¹ e suas consequências jurídicas.

¹ Recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para assegurar ao indivíduo o que o juiz Cooley chama de direito de “ser deixado em paz”. Fotografias instantâneas e empresas de jornal invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam cumprir a previsão de que “o que se sussurra no closet será proclamado do alto das casas” (tradução nossa).

À época da publicação do artigo na “*Harvard Law Review*”, a imprensa passou a adotar práticas excessivamente invasivas à esfera privada, com o objetivo de veicular notícias sensacionalistas relacionadas à elite. Nesse contexto, Samuel B. Warren, membro de uma importante família de Boston, Massachusetts, incomodado com a exposição da vida íntima da sua família, reuniu-se com seu então recém sócio, Louis D. Brandeis, e escreveu o referido trabalho científico (PROSSER, 1960).

Pela análise do texto, fica clara a ideia de que a esfera privada é sagrada, e, por essa razão, não deve ser perturbada e nem exposta por terceiros, quer sejam pessoas comuns, movidas unicamente pela curiosidade, quer sejam jornalistas ou veículos de comunicação, à procura de escândalos envolvendo pessoas de prestígio social.

Segundo Stefano Rodotà (2018), as inspirações que moveram Warren e Brandeis na elaboração do artigo se distinguem em parte. Aquele, um conservador, buscava a proteção da alta burguesia, enquanto este, um liberal, almejava, além da tutela da vida privada da elite, a defesa das minorias intelectuais e artísticas, que poderiam sofrer danos ou perseguições em razão da indiscrição dos jornalistas.

É possível identificar duas motivações a partir das visões de ambos os autores: a primeira, de manutenção dos privilégios das pessoas “de bem”, que não desejavam ver a sua vida pessoal estampada na capa de tabloides; e, a segunda, a garantia da igualdade de tratamento através da não divulgação de informações pessoais relacionadas aos membros de grupos minoritários.

Ocorre que essa definição é insuficiente para lidar com o problema da coleta e tratamento de dados na era da tecnologia. A solução não está no combate às tecnologias que propiciam a circulação de informações, nem na sua eliminação, mas sim na sua utilização como instrumento democrático para a tutela dos dados por parte de seus titulares.

A informação é um recurso essencial para o desenvolvimento econômico e social. Através dela, o Estado pode elaborar políticas públicas mais efetivas para a satisfação das necessidades da coletividade, e, em matéria tributária, é capaz de verificar a ocorrência ou não de fato gerador e fiscalizar o cumprimento da obrigação de pagar; as empresas tornam-se mais eficientes, otimizando os seus recursos e capital e reduzindo os possíveis custos e prejuízos decorrentes do fornecimento de um produto ou serviço que não supra ou desperte os interesses dos consumidores.

O acesso à informação gera poder ao seu detentor. Não é por acaso que, no Império Romano, realizavam-se censos² com o objetivo de apurar o número de cidadãos e de seus bens. Em momento posterior, quando da implementação do modelo de Estado de bem-estar social

² No Evangelho de São Lucas é relatado que, na época do nascimento de Jesus Cristo, houve um recenseamento ordenado por César Augusto, o qual obrigou José e Maria, que estava grávida, a se deslocarem para a cidade de Nazaré, local onde o messias nasceu.

(“*Welfare State*”), caracterizado pela busca da igualdade material³ entre as pessoas, assistencialismo e intervencionismo, houve uma grande demanda de informações por parte do ente público para a realização dos seus objetivos, o que, por outro lado, não ocorria no Estado Liberal, marcado pela igualdade formal, liberdade contratual, garantia da propriedade privada e absentismo estatal na economia.

Desse modo, torna-se necessário compatibilizar a tutela da privacidade com a transparência, causada pela progressiva abertura da sociedade (RODOTÀ, 2008).

Nesse sentido, o debate sobre a privacidade na sociedade contemporânea, para além da preocupação com o “direito a ser deixado só”, de caráter individualista, pauta-se sobre o uso da infraestrutura da informação para a organização do poder. Se a informação confere aos seus detentores poder, então a possibilidade de os indivíduos e grupos exercerem o controle sobre os dados que lhes dizem respeito constitui-se como contrapoder (RODOTÀ, 2008).

Para tanto, faz-se necessária a implementação de instrumentos jurídicos que garantam a descentralização do controle das informações pessoais coletadas e processadas pelas entidades, públicas ou privadas.

Não basta apenas o direito de acesso à informação conferido individualmente a cada pessoa, o que, aliás, já existia no ordenamento jurídico brasileiro antes do advento da Lei Geral de Proteção de Dados, consoante o disposto nos incisos XIV, XXXIX, “b” e LXXII, da Constituição Federal.

É imprescindível a existência de uma entidade de fiscalização e controle do cumprimento da proteção de dados pessoais por parte dos agentes de tratamento, dotada de autonomia e independência no desempenho de suas funções (DE LUCCA et al, 2020).

Com o intuito de garantir a efetividade da tutela das informações coletadas e tratadas no âmbito nacional, foi criada a Autoridade Nacional de Proteção de Dados – ANPD, incluída na Lei Geral de Proteção de Dados pela Lei nº 13.853, de 8 de julho de 2019.

Além disso, os controladores e operadores podem formular regras de boas práticas e governança com o objetivo de se adequar e melhor cumprir as normas referentes à proteção de dados pessoais, conforme prevê o art. 50 da aludida lei.

Nesse sentido, Cíntia Rosa (2020) aduz que o sistema pelo qual o Brasil optou foi a correção, isto é, a ANPD desempenhará as funções de polícia e regulação sem afastar a possibilidade de os agentes de tratamento de dados elaborarem procedimentos de boas práticas, a nível de autorregulação.

³ De acordo com o conceito de igualdade material ou substancial, os iguais devem ser tratados de forma igual, enquanto os desiguais devem ser tratados de modo desigual na medida da sua desigualdade.

Essa fiscalização exercida pela Autoridade Nacional de Proteção de Dados - ANPD, pelos titulares dos dados, e pelos agentes de tratamento deve estar centrada no princípio da finalidade, o qual será abordado a seguir.

A PROTEÇÃO DE DADOS E O PRINCÍPIO DA FINALIDADE

A terminologia “proteção de dados”, apesar de consagrada nos textos normativos, revela-se inadequada, pois a tutela não recai sobre estes, mas sim sobre a pessoa que os titulariza (DE LUCCA et al, 2018).

Dito isso, ainda que este não seja o objeto desta pesquisa, pode-se afirmar que a proteção de dados está ligada aos direitos da personalidade e, por conseguinte, ao princípio constitucional da dignidade da pessoa humana. Assim, quando se busca o direito de acesso a banco de dados ou a retificação ou remoção de informações pessoais, o ordenamento jurídico busca salvaguardar a pessoa, e não os dados em si.

Para a consecução desse objetivo, a Lei Geral de Proteção de Dados – LGPD⁴ prevê como base principiológica para as atividades de tratamento de dados pessoais a boa-fé objetiva, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Além dos princípios supracitados, os quais encontram-se positivados no art. 6º, a LGPD dispõe que à matéria poderão ser aplicados outros direitos e princípios previstos no ordenamento jurídico pátrio ou nos tratados internacionais em que o Estado brasileiro seja parte. Trata-se, portanto, de rol *numerus clausus*, isto é, exemplificativo.

⁴ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Dentre os princípios retro, destaca-se a finalidade, que se constituiu como verdadeiro limitador da coleta e tratamento de dados, vinculando-a aos fins explicitamente informados ao titular, sem a possibilidade de utilização que lhe seja incompatível.

Tamanha é a sua importância que dela decorrem outros três princípios, a saber: adequação, necessidade e qualidade dos dados. Ademais, a finalidade ainda guarda conexão com o princípio da transparência, também previsto no art. 6º da LGPD.

Para Stefano Rodotà (2008), a finalidade caracteriza-se por ser um dos princípios comuns à atual disciplina jurídica da proteção de dados, e especifica-se nos princípios da pertinência e utilização não-abusiva, e no direito ao esquecimento.

A pertinência e a utilização não-abusiva correspondem, na terminologia empregada pela LGPD, à adequação e à necessidade, respectivamente. Quanto ao direito ao esquecimento, este deve ser compreendido como eliminação dos dados que não são mais necessários ou anonimização das informações, ou seja, a “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”, conforme o disposto no art. 5º, XI da LGPD.

Segundo a definição legal, a finalidade consiste na “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”.

Em primeiro lugar, analisar-se-á os conceitos utilizados no dispositivo legal para fins de melhor compreender o seu sentido. Mais adiante, abordar-se-á sobre os princípios jurídicos corolários da finalidade, quais sejam adequação, necessidade e qualidade dos dados.

Considera-se “tratamento”, para fins da LGPD:

[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração [...]. (BRASIL, 2018).

A operação de tratamento de informações tem, de um lado, uma pessoa natural identificada ou identificável, titular dos dados coletados, e, do outro, um agente de tratamento, que pode ser enquadrado como controlador ou operador. Este é “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”, enquanto aquele é “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018).

O propósito desses agentes deve ser legítimo, isto é, conforme os princípios e regras da Lei Geral de Proteção de Dados – LGPD, e em consonância com o direito, de uma forma geral.

As dez hipóteses (bases legais) em que o tratamento de dados pessoais é permitido estão previstas de forma taxativa no art. 7º da LGPD, *in verbis*:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I - mediante o fornecimento de consentimento pelo titular;
- II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
- VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
- IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou;
- X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O tratamento será considerado legítimo caso uma das hipóteses seja satisfeita, o que não exclui a possibilidade de cumulação de duas ou mais bases legais dentro de uma mesma atividade. Aliás, ressalta-se que o consentimento do titular não é necessário para as hipóteses contidas nos incisos II a X.

Ainda quanto à conceituação de legitimidade, o art. 29 WP da *Opinion 03/2013* define a legitimidade como a necessidade de fundamentação legal para o tratamento, que se estende a outras áreas do direito. Além disso, a noção de legitimidade deve ser interpretada no contexto do processamento.

No que tange à especificidade do tratamento, observa-se que, com a nova legislação, não mais se admite a coleta de dados pessoais para finalidades genéricas ou indeterminadas. O titular deve ter o conhecimento prévio de qual o intuito da captura e do tratamento das suas informações pretendido pelos agentes, para, a partir disso, manifestar a sua concordância ou não com a prática.

Por esse motivo, o art. 8º, “caput”, da LGPD exige que o consentimento inequívoco do titular seja manifestado por escrito, hipótese em que a cláusula deve ser destacada das demais cláusulas contratuais, ou por outro meio capaz de manifestar a sua vontade. Além disso, o §4º, de modo expresso, prevê que as autorizações genéricas serão nulas.

A LGPD também exige que o propósito da coleta e tratamento de dados seja explícito, o que traduz a ideia de clareza e não ambiguidade na intenção do agente de tratamento. Essa exigência não se limita ao momento da coleta, mas se estende durante todo o período de tratamento dos dados. Por esse motivo, o art. 9º da LGPD prevê o direito ao titular de acesso facilitado às informações sobre o tratamento dos seus dados, a fim de controlá-los e fiscalizá-los.

Outro aspecto importante é o da vinculação do agente à finalidade exteriorizada quando do momento da captura dos dados. Com isso, evita-se que as informações sejam posteriormente utilizadas para fins diversos daqueles pretendidos inicialmente, e, mitiga-se o risco do uso por terceiros à revelia do titular (MALDONADO, 2021).

ADEQUAÇÃO, NECESSIDADE, QUALIDADE DOS DADOS E TRANSPARÊNCIA

Em razão de sua densidade normativa, do princípio da finalidade decorrem outros três: adequação, necessidade e qualidade dos dados.

A adequação é definida pela LGPD, em seu art. 6, II, como a “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (BRASIL, 2018).

Desse modo, se uma rede de farmácias coleta informações de alguém para a realização de cadastro cujo intuito é o fornecimento de descontos em medicamentos, e se com esses dados, cuja coleta foi autorizada pelo titular, forem criados perfis individuais que potencialmente podem ser usados pelos planos de saúde para identificar o histórico de doenças dos seus clientes, então, o tratamento será inadequado.

O problema não está na criação de perfis, o que, de fato, pode acontecer, mas sim no fornecimento dos dados do consumidor a terceiros, o que não foi objeto de autorização, e, na sua utilização em desacordo com a finalidade exposta quando da sua coleta.

Além da compatibilidade com os fins apresentados ao titular, o tratamento é limitado “ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (BRASIL, 2018). Trata-se do princípio da necessidade, previsto no art. 6, III, da LGPD.

Cabe ao agente de tratamento, antes da coleta das informações, questionar-se se os dados pretendidos são realmente necessários para a consecução da finalidade almejada, ou se é possível alcançá-la por outros meios. Se sim, quais seriam as informações imprescindíveis para a sua realização.

Por fim, o princípio da qualidade dos dados revela-se como “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (BRASIL, 2018).

A finalidade também está indissociavelmente ligada ao princípio da transparência, pois sem esta não seria possível o controle e fiscalização do cumprimento daquela.

Segundo o disposto na lei, a transparência é conceituada como a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os

respectivos agentes de tratamento, observados os segredos comercial e industrial” (BRASIL, 2018).

O titular dos dados encontra-se sempre em situação de vulnerabilidade. Por isso, carece de ampla informação acerca do tratamento dos seus dados para que possa identificar se há legalidade, legitimidade e cumprimento ou não da finalidade por parte do controlador e do operador.

Também, as informações fornecidas pelo agente de tratamento devem ser claras, diretas e eficazes, de modo a evitar ou mitigar a fadiga informacional, distinguindo-a de outras que não sejam correlatas (MALDONADO, 2021).

O MODELO EUROPEU E A SUA INFLUÊNCIA NA LGPD

Pela análise histórica dos documentos que tratam sobre a proteção de dados, especificamente aqueles produzidos pelos organismos supranacionais, tais quais a Organização para a Cooperação e Desenvolvimento Econômico – OCDE e o Parlamento e o Conselho Europeu, constata-se que a finalidade sempre esteve presente como um princípio limitador da coleta, armazenamento e tratamento de informações pessoais.

Nesse sentido, as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, editadas em 1980 pela OCDE, já estabeleciam que:

As finalidades para as quais os dados pessoais são coletados devem ser especificadas, o mais tardar, no momento da coleta de dados e o uso subsequente limitado ao cumprimento dessas finalidades ou outras que não sejam incompatíveis com essas finalidades e que sejam especificadas em cada ocasião de mudança de propósito. (OECD, 1980).

Do mesmo modo, a Convenção nº 108, de 28 de janeiro de 1981, sobre a proteção de dados pessoais, em seu art. 5º, previa que:

Os dados pessoais em tratamento automático serão: a) obtidos e tratados de forma justa e lícita; b) armazenado para fins específicos e legítimos e não usado de forma incompatível com esses fins; c) adequados, relevantes e não excessivos em relação aos fins para os quais são armazenados; d) precisos e, quando necessário, atualizados; e) preservados de uma forma que permita a identificação dos titulares dos dados por um período não superior ao necessário para os fins para os quais esses dados são armazenados.

Também a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, determina que a finalidade declarada na coleta dos dados vincula a sua utilização, não se admitindo o posterior tratamento de forma incompatível com essa. Ademais, semelhante à Convenção nº 108, também disciplinou que as informações obtidas não devem ser excessivas relativamente à finalidade para as quais foram colhidas.

Atualmente, o regramento básico sobre a tutela de dados pessoais no bloco europeu está contido no “*General Data Protection Regulation - GDPR*” (Regulamento Geral sobre a Proteção de Dados – RGPD), editado em 27 de abril de 2016, o qual, à semelhança dos documentos anteriores, trouxe expressamente o princípio da finalidade, nos seguintes termos:

1. Os dados pessoais são:

[...]

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);

No Brasil, a Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018) foi profundamente influenciada pelo direito comunitário europeu, em especial, pelo Regulamento Geral de Proteção de Dados - RGPD. Por essa razão, o art. 6º da lei nacional enuncia que o tratamento de dados pessoais deve observar o princípio da finalidade, compreendido este como a: “[...] realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. (BRASIL, 2018).”

A semelhança entre os textos normativos indica uma tendência global de uniformização da matéria. Conforme já exposto, isso se deve em razão da própria natureza transfronteiriça e imaterial dos dados. No Cyber espaço, não há uma “aqui” e um “ali”. De qualquer lugar que esteja, uma pessoa pode acessar através do seu smartphone, tablet ou computador qualquer website as informações contidas no rede.

Desse modo, se não houver um tratamento padronizado do assunto, a efetividade da proteção e do controle poderá ser prejudicada. Por esse motivo, a LGPD se assemelha muito ao regulamento europeu.

CONSIDERAÇÕES FINAIS

O avanço da tecnologia propiciou novas ferramentas para a coleta e o tratamento de dados pessoais, e, com isso, questionamentos acerca das suas possíveis implicações no direito à privacidade.

Nesse contexto, o direito buscou, e busca, oferecer respostas às mudanças sociais, adequando o ordenamento jurídico aos novos fenômenos, a exemplo da Lei Geral de Proteção de Dados – LGPD, editada no Brasil como uma resposta à necessidade de garantia dos direitos da personalidade através da proteção de dados.

Para a efetivação da tutela das informações pessoais, a LGPD, em seu art. 6º, estabelece os princípios que regem a proteção de dados no Brasil, dentre os quais encontra-se a finalidade, conceituada como a realização do tratamento para propósitos legítimos, específicos e explícitos, sem possibilidade de tratamento posterior incompatível.

Em razão da sua importância, do princípio da finalidade emanam outros três: adequação, necessidade e qualidade dos dados. Consta-se também que a finalidade está profundamente ligada à transparência, sendo essa um instrumento para a consecução daqueles.

As empresas e demais entidades, públicas ou privadas, devem se adequar às exigências estabelecidas no referido diploma normativo, sob pena de sofrerem sanções legais. Para tanto, a finalidade da coleta e tratamento de dados sempre deve ser explicitada ao titular.

Por fim, ressalta-se que esses princípios estão inseridos na disciplina da atual proteção de dados adotada pelos mais diversos Estados, em razão da tendência de uniformização da matéria, não podendo ser olvidado pela ordem jurídica brasileira, devendo, não no plano legislativo, mas na prática, concretizado, assegurando a proteção aos dados pessoais que se constitui, nessa quadra do século XXI, em direito humano fundamental.

REFERÊNCIAS

ÁVILA, Humberto. **Teoria dos princípios: da definição à aplicação dos princípios jurídicos**. 20. ed. rev e atual. – São Paulo: Malheiros, 2021.

BENDICH, Albert M. “Privacy, Poverty, and the Constitution.” **California Law Review**, vol. 54, no. 2, California Law Review, Inc., 1966, pp. 407–42, Disponível em: < <https://doi.org/10.2307/3479414> >.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm >. Acesso em: 13 set 2021.

DE LUCCA, Newton; MACIEL, Renata Mota. A Lei nº 13.709, de 14 de agosto de 2018: A disciplina normativa que faltava. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; DEZEM, Renata Mota Madeira Maciel (coords.). **Direito & Internet IV: Sistema de Proteção de Dados Pessoais**. São Paulo: Quartier Latim, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados: elementos da formação da Lei geral de proteção de dados**. 2. Ed. – São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice (coords.). **LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 3. Ed. – São Paulo: Thomson Reuters Brasil, 2021.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, de 23 de setembro de 1980. Disponível em: <<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>>. Acesso em: 17 out 2021.

PROSSER, Willian L. Privacy. **California Law Review**, v. 48, n. 383, 1960. Disponível em: <https://lawcat.berkeley.edu/record/1109651>. Acesso em: 05 nov 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008.

SILVA, Luis Virgilio Afonso da. Princípios e regras: mitos e equívocos acerca de uma distinção. **Revista Latino-Americana de Estudos Constitucionais**, Belo Horizonte, n. ja/ju 2003, p. 607-630, 2003. Disponível em: <https://constituicao.direito.usp.br/wp-content/uploads/2003-RLAEC01-Principios_e_regras.pdf>.

UNIÃO EUROPEIA. Comissão Europeia. **Opinion 03/2013 on purpose limitation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 5 out 2021.

UNIÃO EUROPEIA. Conselho Europeu. Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981. Disponível em: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf>. Acesso em: 24 out 2021.

UNIÃO EUROPEIA. Conselho Europeu. Parlamento Europeu. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**. *Jornal Oficial da União Europeia*, 23 de maio de 2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>>. Acesso em: 9 nov 2021.

UNIÃO EUROPEIA. Parlamento Europeu e do Conselho. **Diretiva 95/46/CE, de 24 de outubro de 1995**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. *Jornal Oficial da União Europeia*, 23 de novembro de 1995. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>>. Acesso em: 10 de out 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents

WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.