UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Leonardo Hoss

PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE SOB A PERSPECTIVA DO CONSENTIMENTO

Porto Alegre
2019

LEONARDO HOSS

PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE SOB A PERSPECTIVA DO CONSENTIMENTO

Monografia apresentada ao Departamento de Direito Privado e Processo Civil da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do grau de bacharel em Direito.

Orientador: Prof. Fabiano Menke

Porto Alegre
2019

LEONARDO HOSS

PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE SOB A PERSPECTIVA DO CONSENTIMENTO

Monografia apresentada ao Departamento de Direito Privado e Processo Civil da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do grau de bacharel em Direito.

Aprovada em 17 de julho de 2019.

BANCA EXAMINADORA:

_____
Professor Fabiano Menke
Orientador

_____
Professor Gerson Luiz Carlos Branco

_____
Professor Rodrigo Ustárroz Cantali

AGRADECIMENTOS

Agradeço, em primeiro lugar, aos meus pais, pelo amor e apoio incondicionais durante toda a minha trajetória. Vocês são o motivo de eu ter chegado até aqui.

Ao meu irmão Guilherme, por conviver comigo e com as minhas manias há mais de vinte anos.

Aos amigos que o Direito me deu, Laura, Paulo, Anna, Monalisa, Julie, Patrícia e Letícia, pelas risadas e momentos de descontração. A faculdade não teria sido a mesma sem vocês.

Finalmente, aos professores da Faculdade de Direito da UFRGS, por todos os ensinamentos passados ao longo da nossa convivência.

RESUMO

A sociedade da informação, marcada pela ubiquidade da tecnologia, trouxe à luz um dos mais importantes temas jurídicos da atualidade, a proteção de dados pessoais. A presente monografia analisa, sob a perspectiva do consentimento, o desenvolvimento da disciplina de proteção de dados pessoais no contexto internacional e brasileiro, apresentando a sua evolução histórica e legislativa, com o intuito de definir o papel do consentimento no âmbito da proteção de dados pessoais. Para tanto, é examinada a natureza jurídica do consentimento, a relação deste instituto jurídico com o assunto proteção de dados, além da sua influência sobre as normas de proteção de dados que vigem atualmente na Europa e no Brasil, o GDPR e a LGDP, respectivamente. A principal conclusão é que o consentimento passou por várias transformações desde o momento em que foi inserido no âmbito da proteção de dados pessoais, mas jamais deixou de ser um elemento fundamental à disciplina.

Palavras-chave: Proteção de dados pessoais. Consentimento. Privacidade. LGPD. GDPR.

ABSTRACT

The information society, marked by the ubiquity of technology, has brought to light one of the most pressing legal issues of our time, data protection. This thesis analyzes, under the perspective of consent, the development of data protection, both internationally and in Brazil, by presenting its historical and legislative evolution, in order to define the role of consent within the scope of data protection. Furthermore, this thesis will be examining the legal nature of consent, the relation between consent and data protection, and the influence of consent over the current data protection laws in Europe and in Brazil, the GDPR and LGPD, respectively. The main conclusion is that consent has undergone several changes since the moment it was included in the discussion about data protection, but it never ceased to be a fundamental component of the subject.

Keywords: Data protection. Consent. Privacy. LGDP. GDPR.

SIGLAS E ABREVIATURAS

Art. 29 WP – *Article 29 Working Party*

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

FIPPs – *Fair Information Practice Principles*

GDPR – *General Data Protection Regulation*

LC – Lei Complementar

LGPD – Lei Geral de Proteção de Dados

MCI – Marco Civil da Internet

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

"Privacy guidelines" – *OECD guidelines on the protection of privacy and transborder flows of personal data*

UE – União Europeia

SUMÁRIO

INTRODUÇÃO

Ao longo da história, os modos de organização social sempre foram estruturados a partir de um elemento central, responsável por ditar os mais variados aspectos das sociedades humanas. Na sociedade agrícola, esse elemento foi a terra; na sociedade industrial, destacam-se o capital, a matéria-prima e a capacidade de trabalho. Já na sociedade contemporânea, o desenvolvimento se encontra centrado no fenômeno da informação[1].

A informação é um assunto que há muito tempo vem ocupando as mais variadas disciplinas jurídicas: seja no direito constitucional, com a liberdade de expressão e a liberdade de imprensa; seja no direito penal, com a proteção contra a divulgação de informações difamatórias, caluniosas ou injuriosas; seja no direito comercial, com a garantia de sigilo empresarial. Tão antigas quanto essa ocupação são as tentativas do Direito de regular o fenômeno informacional, justamente por reconhecer a sua importância na vida dos indivíduos e da sociedade como um todo[2].

As últimas décadas, no entanto, vêm apresentando desafios sem precedentes aos sistemas jurídicos, na medida em que as novas tecnologias da informação passaram a influenciar quase todos os aspectos da vida dos cidadãos, seja na forma como eles se relacionam, lidam com as suas finanças ou buscam entretenimento. Com a ampliação das formas de comunicação, de representação da personalidade e da circulação de conhecimento, ampliaram-se também as formas de exposição indesejada, de discriminação e de restrição à liberdade individual[3].

Nesse contexto conturbado, em relação ao qual o Direito ainda dá seus primeiros passos (especialmente o direito brasileiro), ganha força um dos aspectos jurídicos mais relevantes da sociedade da informação: a proteção de dados pessoais.

---

[1] SILVA, Daniel Pereira Militão da. Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo. São Paulo, 2009, pp. 43-47.

[2] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 19.

[3] Ibidem, p. 20.

Historicamente, a disciplina da proteção de dados pessoais tem sido tratada como uma espécie de evolução do direito à privacidade, que surgiu nos Estados Unidos ao final do século XIX, em reação à invenção das fotografias instantâneas e de outros artefatos que potencializavam violações à vida privada dos indivíduos[4].

Desde então, o desenvolvimento exponencial das tecnologias de comunicação, armazenamento e transmissão de dados, vem provocando mudanças dramáticas na forma como lidamos com a informação. Assim, naturalmente, a disciplina da proteção de dados foi sendo moldada pelos novos tempos, de modo a não ficar obsoleta diante das novas práticas sociais e econômicas propiciadas pelo progresso tecnológico.

Em vista disso, neste trabalho buscar-se-á analisar a evolução do conceito de proteção de dados pessoais na experiência jurídica internacional e brasileira, sob a perspectiva de um dos elementos fundamentais ao assunto: o consentimento. Como será demonstrado, o consentimento é uma dos principais alicerces da matéria, o que lhe garantiu um papel de grande relevo na trajetória evolutiva das leis de proteção de dados. Objetiva-se definir, com isso, *o papel do consentimento no âmbito da proteção de dados pessoais*. Para tanto, o trabalho foi dividido em três capítulos.

No primeiro, apresenta-se a evolução histórica do conceito de proteção de dados pessoais no âmbito internacional, desde as suas raízes no direito à privacidade até os dias atuais. É abordada, ainda, a decisão da Corte Constitucional alemã sobre a Lei do Censo de 1983 e o desenvolvimento geracional das leis de proteção de dados pessoais.

No segundo capítulo, será exposta a forma pela qual o consentimento se relaciona com o assunto proteção de dados pessoais e quais são alguns dos problemas existentes nessa relação. Além disso, tratar-se-á da natureza jurídica do consentimento, bem como da sua trajetória no direito comunitário europeu, sempre à luz da disciplina da proteção de dados. Com o intuito de esboçar esse percurso, serão analisadas inicialmente as *privacy guidelines* da Organização para a Cooperação e Desenvolvimento Econômico e, ao fim do capítulo, o mais recente regulamento do bloco europeu sobre a matéria: o *General Data Protection Regulation* (GDPR).

[4] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. 4, n. 5, 1890, p. 193.

Já no terceiro e último capítulo, será apresentado um breve retrato de como o ordenamento jurídico brasileiro desenvolveu legislativamente o tema da proteção de dados pessoais. Abordar-se-á, também, a relação do consentimento com a nova Lei Geral de Proteção de Dados (LGPD) e, por fim, se buscará definir o que seria um consentimento válido no âmbito dessa lei.

CAPÍTULO 1 – A PROTEÇÃO DE DADOS PESSOAIS: ORIGEM E DESENVOLVIMENTO

1.1. A evolução do conceito de privacidade

Os primeiros debates doutrinários ocorridos sobre o direito à privacidade se deram ao final do século XIX, em reação ao surgimento de novas tecnologias e novos métodos de difusão de informações, como as fotografias instantâneas. Tais métodos viabilizaram novas formas de invasão à vida privada e doméstica dos indivíduos, o que é evidenciado pelo pioneiro artigo sobre direito à privacidade de Samuel D. Warren e Louis D. Brandeis, intitulado "The Right to Privacy[5]", o qual foi publicado na Harvard Law Review no ano de 1890 e iniciou um longo debate a respeito dos limites e natureza do direito à privacidade.

Inicialmente, de acordo com os autores, a lei garantia ao indivíduo soluções apenas para interferências físicas contra a vida e a propriedade – *the right to life;* a lei protegia o sujeito de agressões, em suas variadas formas; a liberdade significava simples abstenção por parte do Estado; e o direito à propriedade assegurava ao indivíduo as suas terras e seu gado[6]. De maneira gradual, o escopo da lei se expandiu, passando a garantir ao indivíduo o direito de aproveitar a vida. Além disso, o direito à liberdade passou a assegurar o exercício de diversos direitos civis; e o direito à propriedade passou a englobar todas as formas de posse, tanto tangível, quanto intangível.

De modo a dar continuidade a essa evolução, Warren e Brandeis identificaram que as "recentes invenções e modelos de negócios chamam atenção para o próximo passo que precisa ser tomado para a proteção da pessoa e para garantir aquilo que o juiz Cooley havia chamado de 'o direito de ser deixado só[7]". Os dois, então, passam a identificar e delinear um direito à privacidade no âmbito da *common law*, a partir de precedentes jurisprudenciais de tribunais ingleses,

[5] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. 4, n. 5, 1890, pp. 193-220.
[6] Ibidem, p. 193.
[7] Ibidem, p. 195, tradução livre. "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone'."

distinguindo-o dos institutos de *slander* e *libel*[8] (calúnia e difamação, respectivamente), demonstrando a sua independência em relação às leis de proteção de direitos autorais (*copyright laws*[9]) e afastando-o da noção anterior que associava a proteção da vida privada à propriedade. Em seus próprios termos: "o princípio que protege escritos pessoais e todas as outras produções pessoais, não contra o roubo ou outra espécie de apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade"[10].

Nessa busca por delinear o que seria o direito à privacidade dentro da *common law*, Warren e Brandeis apontam, igualmente, quais deveriam ser os limites desse direito, traçando orientações gerais a serem utilizadas pelos julgadores diante de casos concretos.

Em uma primeira análise, os autores indicam que o direito à privacidade não deveria proibir a publicação do que é de interesse público ou geral, devendo ser distinta a proteção conferida ao cidadão comum e à pessoa pública, e.g. um possuidor de cargo eletivo. O direito à privacidade também não deveria proibir a publicação de questões privadas quando isso fosse feito sob a égide da lei, como

[8] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. 4, n. 5, 1890, p. 197. "Owing to the nature of the instruments by which privacy is invaded, the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel […] The principle on which the law of defamation rests, covers, however, a radically different class of effects from those for which attention is now asked. It deals only with damage to reputation, with the injury done to the individual in his external relations to the community, by lowering him in the estimation of his fellows. […] In short, the wrongs and correlative right recognized by the law of slander and libel are in their nature material rather than spiritual."

[9] Ibidem, p. 200. "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. […] No other has the right to publish his productions in any form, without his consent. This right is wholly independent of the material on which, the thought, sentiment, or emotions is expressed. It may exist independently of any corporeal being, as in words spoken, a song sung, a drama acted. Or if expressed on any material, as in a poem in writing, the author may have parted with the paper, without forfeiting any proprietary right in the composition itself. The right is lost only when the author himself communicates his production to the public, – in other words, publishes it. It is entirely independent of the copyright laws, and their extension into the domain of art. The aim of those statutes is to secure to the author, composer, or artist the entire profits arising from publication; but the common-law protection enables him to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all. The statutory right is of no value, unless there is a publication; the common-law right is lost as soon as there is a publication."

[10] Ibidem, p. 205, tradução livre. "The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality".

perante um tribunal ou assembleias legislativas, ou no cumprimento de algum dever legal[11].

Também não caberia à lei se intrometer nos casos em que a invasão à privacidade ocorresse pela transmissão oral de uma informação que não causasse danos ao indivíduo; e o direito à privacidade cessaria no momento em que o próprio indivíduo publicasse as questões antes qualificadas como privadas, ou quando desse o seu consentimento[12].

Além disso, a veracidade ou falsidade da informação publicada pelo agressor deveria ser considerada irrelevante, pois o que se busca tutelar é a privacidade do indivíduo e não o conteúdo da informação divulgada. Assim, a ausência de dolo por parte do agressor não desqualificaria a violação do direito à privacidade, que seria afetado independentemente da intenção do malfeitor[13].

Do contexto desse artigo, que se tornou um paradigma para o estudo jurídico da privacidade[14], extraem-se duas características marcantes que justificam a sua notoriedade: (I) o ponto de partida foi o surgimento de um novo fato social, representado pelas mudanças trazidas para a sociedade pelas tecnologias de informação (jornais e fotografias instantâneas) e a comunicação de massa, fenômeno este que estende a sua atualidade aos dias de hoje; (II) o novo “direito à privacidade” era de natureza pessoal, e não se valia do arcabouço jurídico de tutela da propriedade para proteger os aspectos da privacidade[15].

Do mesmo modo, nota-se o caráter fortemente individualista do direito à privacidade em sua origem, sedimentado por Warren e Brandeis como o direito a ser deixado só (*right to be let alone*). Tratava-se, claramente, de um direito negativo, na medida em que a única função do Estado nesse contexto era a de não intervir na esfera privada do indivíduo[16].

---

[11] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. 4, n. 5, 1890, pp. 214-217.
[12] Ibidem, pp. 217-218.
[13] Ibidem, p. 218.
[14] GALLAGHER, Susan E. Introduction to "The Right to Privacy" by Louis D. Brandeis and Samuel Warren: A Digital Critical Edition. University of Massachusetts Press.
[15] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 97.
[16] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 28.

Passados alguns anos da publicação de Warren e Brandeis, essa tendência individualista atingiu um ponto de inflexão ao projetar-se para o recém-estruturado panorama do *welfare state*. Não mais bastava visualizar a privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem a privacidade como uma preferência individual, ligada basicamente ao conforto e à comodidade do cidadão. A própria ideia da privacidade como algo de que um cidadão respeitável poderia tranquilamente abrir mão (conhecida também como a "transparência de quem não tem nada a temer"), deixa de fazer sentido em face à crescente complexidade da matéria adquirida no decorrer do século XX[17].

Tal evolução do direito à privacidade, aliada aos novos desafios impostos ao ordenamento jurídico pelo tratamento informatizado de dados, fez surgir uma nova dimensão desse direito, a proteção de dados pessoais. Essa transformação fica mais evidente a partir da década de 1970, quando diversos países passaram a editar leis específicas de proteção de dados pessoais e este conceito passou a ser defendido por tribunais superiores[18], como se verá nos subcapítulos seguintes.

Percebe-se, afinal, que a elevada complexidade adquirida pela matéria com o advento do Estado Moderno[19], somada às grandes inovações tecnológicas, contribuiu decisivamente para modificar o sentido e o alcance do direito à privacidade. De um direito de dimensão notadamente negativa, passou a ser considerado um pressuposto indispensável a uma sociedade democrática moderna, na medida em que garantiu ao indivíduo controle sobre as suas informações pessoais[20].

1.2. A decisão da Corte Constitucional alemã: Lei do Censo de 1983

[17] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, pp. 141-142.
[18] Ibidem, p. 29.
[19] Compreendido aqui como o novo modelo de Estado surgido após a Segunda Guerra Mundial, na segunda metade do século XX.
[20] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 29.

Na evolução do conceito de proteção de dados pessoais, a decisão do Tribunal Constitucional alemão, no julgamento da Lei do Censo alemã (*Volkszählungsgesetz*) de 1983, é considerada um marco[21].

Essa lei determinava o recenseamento geral da população alemã, visando à coleta de dados dos cidadãos referentes à profissão, à moradia e ao local de trabalho, com o objetivo declarado de fornecer à administração pública informações acerca do crescimento populacional, da distribuição espacial da população no território, sua composição segundo características demográficas e sociais, e das atividades econômicas desenvolvidas no país[22].

Ocorre que, o § 9º da Lei previa a possibilidade de que os dados coletados fossem cruzados com outros registros públicos, além de autorizar a transmissão de dados tornados anônimos a outras repartições públicas para "fins de execução administrativa[23]".

Tal vagueza da lei de recenseamento foi objeto de uma série de reclamações perante o Tribunal Constitucional alemão, sob o fundamento de que estaria sendo violado o direito ao livre desenvolvimento da personalidade dos reclamantes. Sob essa lógica, a Corte declarou a inconstitucionalidade parcial da Lei do Censo, determinando que os dados coletados fossem utilizados para fins exclusivamente estatísticos[24].

A decisão da corte constitucional alemã, dada a sua *ratio decidendi*, estabeleceu os alicerces da teoria da proteção de dados pessoais e de todas as subsequentes normas nacionais e europeias sobre o assunto, na medida em que: a) reconheceu um direito subjetivo fundamental no direito à proteção de dados pessoais; e b) alçou o indivíduo ao papel de protagonista no processo de tratamento

---

[21] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, G.F.; SARLET, I.W.; COELHO, A.Z.P., coord. Direito, inovação e tecnologia. São Paulo: Saraiva, 2015, p. 208. De acordo com Menke, a decisão fixou várias diretrizes a respeito da disciplina da proteção de dados, as quais vieram a influenciar legislações, doutrina e jurisprudência de diversos países.

[22] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Konrad-Adenauer-Stiftung E.V., 2005, pp. 233-234.

[23] Ibidem, p. 234. "O § 9 da Lei previa, entre outras, a possibilidade de uma comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa".

[24] Ibidem, p. 244.

de seus dados[25]. A fim de elucidar um pouco mais esses pontos, será feita uma breve releitura do julgado em questão.

Na primeira parte da decisão, a Corte exibe a sua preocupação com as condições modernas de processamento de dados, que possibilitam o armazenamento praticamente ilimitado de informações pessoais, as quais ficam à disposição quase imediata de quem as detêm. Ademais, é referido que essas informações podem ser combinadas com outros bancos de dados, formando um quadro da personalidade bastante completo, sem que a pessoa atingida sequer tenha controle sobre tal fato.

Nesse sentido, o Tribunal argumenta que a Constituição alemã protege o direito geral da personalidade, e que a capacidade do indivíduo de autodeterminar seus dados pessoais seria parcela fundamental do seu direito de livremente desenvolver sua personalidade. Todavia, sustenta a Corte, aqueles que não conseguem determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas ou não, poderiam ser inibidos substancialmente em sua liberdade de planejar ou decidir com autodeterminação[26].

Por tal razão, conclui a corte constitucional, o livre desenvolvimento da personalidade pressupõe a proteção do indivíduo contra o levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais[27]. Isto é, a proteção de dados pessoais foi alçada ao patamar de um direito fundamental, visto que, caso esse direito não fosse tutelado pelo ordenamento jurídico, o indivíduo não conseguiria autodeterminar as suas informações pessoais e, por consequência, não conseguiria desenvolver livremente a sua personalidade.

Já na segunda parte da decisão, é destacado que a lei imputava como obrigatório o fornecimento de dados por parte dos cidadãos, não havendo a opção de recusa, por se tratar justamente de uma lei de recenseamento. Por tal razão, o

[25] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 31.

[26] MENKE (2015, p. 211) refere que a autodeterminação informativa dá ao indivíduo o poder de ele próprio decidir acerca da divulgação e utilização de seus dados pessoais. Afinal, ainda de acordo com o autor, uma das preocupações fundamentais do instituto da proteção de dados é a de que o indivíduo não seja manipulado por informações que os seus interlocutores tenham sobre a sua pessoa, sem que ele saiba disso.

[27] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Konrad-Adenauer-Stiftung E.V., 2005, pp. 236-238.

tribunal alemão instituiu dois pressupostos para que se tornasse legítima essa coleta de dados: (I) a finalidade de uso dos dados deveria ser prevista em lei, de forma precisa; e (II) os dados coletados deveriam ser adequados e necessários[28] para que fosse atingida a referida finalidade[29].

Nesse contexto, no qual o consentimento dos titulares de dados pessoais não teve um papel de protagonismo, a Corte, em contrapartida, impôs limites mais rigorosos à coleta e utilização dos dados pessoais. Afinal, caso não o tivesse feito, a pessoa poderia ser transformada em um simples objeto de informação, no contexto de um tratamento irrestrito dos dados relativos à sua pessoa.

Percebe-se, por conseguinte, a importância dada pelo Tribunal Constitucional alemão, ao analisar a Lei do Censo de 1983, à figura do consentimento, na medida em que o seu afastamento somente seria autorizado diante de uma questão de interesse público (no caso, o recenseamento da população[30]) e dentro de certos limites legais constitucionais[31]. Nota-se, igualmente, que a Corte consolidou o indivíduo como protagonista no processo de tratamento de seus dados, fato extremamente importante no processo evolutivo das leis de proteção de dados pessoais, como será visto a seguir.

1.3. Desenvolvimento geracional das leis de proteção de dados pessoais

[28] Neste ponto é válido reparar que o tribunal alemão iniciou a construção do que é hoje chamado de "princípio da necessidade" pelo art. 6º, III, da Lei Geral de Proteção de Dados Pessoais (Lei 13.708/2018).

[29] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Konrad-Adenauer-Stiftung E.V., 2005, p. 240.

[30] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Konrad-Adenauer-Stiftung E.V., 2005, p. 241. "A estatística tem papel importante para a política governamental, que está vinculada aos princípios e diretrizes da *Grundgesetz*. Se o desenvolvimento socioeconômico não deve ser aceito como destino imutável, mas entendido como uma tarefa permanente, é necessária uma informação abrangente, contínua e constantemente atualizada sobre os contextos econômico, ecológico e social. Somente com o conhecimento dos dados relevantes e a possibilidade de se utilizar para a estatística as informações por eles transmitidas, com a ajuda das chances que o processamento eletrônico de dados oferece, é que se cria a base de ação indispensável para uma política estatal orientada pelo princípio do Estado social".

[31] Ibidem, p. 235.

Desde a década de 1970, na Europa, o termo “proteção de dados” se tornou comumente utilizado em legislações nacionais e europeias para descrever o direito do indivíduo de ter controle sobre os seus próprios dados. Esse movimento legislativo evidenciou a consciência das pessoas comuns e da classe política em relação aos problemas trazidos pelas novas tecnologias de processamento de dados, que passaram a possibilitar graves violações à esfera privada dos indivíduos[32].

Como se pode perceber, desde o momento em que os avanços tecnológicos passam a permitir a coleta, armazenamento e processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais[33]. Nota-se, então, uma alteração não somente do conteúdo do direito à privacidade, mas também da forma como ele é tratado, passando a ser designado “privacidade informacional”, “proteção de dados pessoais”, “autodeterminação informativa”, entre outros[34].

Nesse contexto, a primeira geração das normas de proteção de dados surgiu de forma reativa ao processamento massivo de dados pessoais dos cidadãos nas administrações públicas e nas empresas privadas, principalmente em razão do advento de grandes bancos de dados centralizados. Temia-se a emergência da figura *orwelliana* do *Big Brother*[35], que colocaria em xeque os direitos e liberdades fundamentais presentes na maioria das sociedades democráticas. Tais fatores acabaram por moldar a estrutura, a linguagem e a abordagem presentes nas leis da primeira geração[36].

Consequentemente, as normas de primeira geração centraram os seus esforços em regular a questão do processamento de dados, afinal, se o ato de processar dados era o problema, este deveria ser o foco da normatização. Um

[32] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001, p. 219. “To be sure, data-protection laws have been enacted in the vast majority of European nations since 1970. Not only do they signify the awareness of both politicians and the public to the problem of informational privacy; they also evince the dramatic technological changes in information processing”.

[33] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 32.

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

[35] A menção é feita por MAYER-SCHÖNBERGER em alusão ao famoso romance de George Orwell, intitulado 1984, no qual o Estado monitora a tudo e a todos.

[36] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001, p. 223.

exemplo disso é a grande atenção dada por essas leis às concessões de autorizações para a criação de bancos de dados, que seriam fiscalizados de modo posterior por órgãos públicos. Tais leis também davam grande destaque ao controle do uso de informações pelo Estado e suas estruturas administrativas, que eram os destinatários principais destas normas[37]. São exemplos de normas de primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos Estados Unidos, foi aprovado nesse período o *Privacy Act* (1974), também direcionado principalmente à administração pública[38].

Nota-se, portanto, que as primeiras leis de proteção de dados foram alocadas dentro de um propósito maior de domesticação da tecnologia pelo Estado, já que ela era vista como uma ferramenta muito poderosa e, em razão disso, deveria ser utilizada como um meio para mudanças políticas e sociais[39]. Entretanto, não demorou muito para que essas leis se tornassem ultrapassadas, visto que o processamento de dados transcendeu a esfera governamental, ocorrendo um grande aumento no número de atores e de bancos de dados, de forma que um controle baseado em autorizações, o qual demandava um minucioso acompanhamento, tornou-se virtualmente ineficaz[40].

A segunda geração das leis sobre a matéria surgiu a partir do final da década de 1970, momento em que os grandes bancos de dados estatais estavam sendo substituídos por diversos bancos de dados espalhados pelo plano estatal e privado. As técnicas autorizativas para o funcionamento dessas estruturas foram perdendo efeito, o que provocou uma mudança no âmago regulatório. A estrutura legal anterior, focada amplamente na normatização dos fenômenos tecnológicos, deu espaço a uma legislação focada nas noções de privacidade e proteção de dados pessoais, vistas como liberdades negativas, a serem exercidas pelo próprio cidadão com base na ideia de consentimento. Isto é, se as leis anteriores incumbiam ao Estado licenciar a criação e o funcionamento de todos os bancos de dados, a

[37] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 208.
[38] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001, p. 224.
[39] Ibidem, p. 223.
[40] Ibidem, p. 224.

segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los[41]. Tal modificação pode ser vista, inclusive, no próprio nome da lei francesa de proteção de dados de 1978, intitulada *Informatique et Libertés*[42]. São exemplos, para além do regramento francês, de normas de segunda geração as leis nacionais de proteção de dados da Áustria, França, Dinamarca e Noruega[43].

Tal evolução refletia o descontentamento de cidadãos que sofriam com a utilização de seus dados pessoais por terceiros e careciam de meios para defender adequadamente seus interesses. Assim, desenvolveu-se um sistema legal (e constitucional, em alguns casos[44]) que fornecia instrumentos para o cidadão identificar o uso não autorizado de suas informações pessoais e uma forma de propor a sua tutela[45].

No entanto, essas leis de segunda geração também apresentavam seus problemas, na medida em que se percebeu que o fornecimento de dados pessoais pelos cidadãos havia se tornado um requisito essencial para a sua efetiva participação na vida em sociedade. Desde burocracias governamentais, o exercício da cidadania pelo voto, até o acesso a bens de consumo (como abrir uma conta no banco, por exemplo) exigiam o fornecimento de dados pessoais como uma condição indispensável; e o questionamento ou interrupção de tais fluxos de dados pelo cidadão – ou seja, a atuação direta da "liberdade negativa" do cidadão de impedir a propagação de suas informações pessoais – implicava frequentemente na exclusão do indivíduo de algum aspecto da vida em sociedade. Nas palavras de Mayer-Schönberger, somente os eremitas alcançariam a proteção plena de seus dados, dado o custo social que o indivíduo teria de pagar por isso[46]. Enfim, percebeu-se que o exercício puramente individual dessa liberdade envolvia consequências muito

[41] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 209.
[42] "Informática e liberdades", em tradução livre.
[43] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 40.
[44] Segundo DONEDA (2006, p. 209), as constituições portuguesa (1976) e espanhola (1978) já apontavam no sentido de que os próprios cidadãos buscassem a tutela dos seus dados pessoais.
[45] Ibidem, p. 210.
[46] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001, p. 229. "But what price does one have to pay for that? Is it acceptable that such data-protection liberties can be exercised only by hermits? Have we reached an optimum of data protection if we guarantee privacy rights that, when exercised, will essentially expel the individual citizen from society?"

maiores do que aquelas puramente relacionadas à questão da proteção de dados pessoais, as quais cobravam um preço que pouquíssimos indivíduos estariam dispostos a pagar.

Surge, então, uma terceira geração de leis na década de 1980, representada de modo emblemático pela decisão do Tribunal Constitucional alemão, já mencionada anteriormente neste trabalho[47]. Nessa decisão, o tribunal declarou a inconstitucionalidade da Lei do Censo, de 1983, definindo que os cidadãos possuem o direito à autodeterminação informativa e ampliando o protagonismo do indivíduo na proteção de seus dados pessoais. Pode-se dizer que a principal distinção em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão, e não apenas como a opção entre tudo ou nada[48].

Essas leis também refletiam as mudanças ocorridas no contexto tecnológico, no qual as novas tecnologias de rede e de telecomunicações haviam ampliado a capacidade e a dinâmica de transmissão de dados. Fazia-se presente, de mesmo modo, uma crescente dificuldade em localizar fisicamente os bancos de dados, pois as informações passaram a ser armazenadas em redes e não mais em um local centralizado e identificável de processamento[49].

São exemplos dessa geração as leis dos Estados alemães posteriores à decisão do Tribunal Constitucional, a emenda à Lei Federal de Proteção de Dados Pessoais alemã de 1990, a emenda à lei de proteção de dados da Áustria de 1986, a alteração da lei de proteção de dados da Noruega e a previsão constitucional da proteção de dados pessoais na Holanda[50].

Nota-se que essas leis de terceira geração visualizavam a participação do indivíduo como o principal alicerce de sua estrutura. Percebeu-se, contudo, que na realidade não seriam muitas as pessoas dispostas a exercitar suas prerrogativas de autodeterminação informativa, isso porque, de forma muito semelhante ao que ocorreu com a segunda geração das normas de proteção de dados pessoais, os

[47] Subcapítulo 1.2.
[48] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 42.
[49] Ibidem, p. 42.
[50] Ibidem, p. 42.

custos sociais e econômicos envolvidos geralmente as compeliam a anuir com situações que não eram as ideais[51].

Além disso, tendo em vista que o consentimento do indivíduo autorizava o processamento de seus dados pessoais, caso houvesse alguma violação ao seu direito à privacidade, não teria ele condições de buscar a reparação de tal violação, ao passo que havia consentido com o tratamento de seus dados[52].

A quarta geração de normas de proteção de dados, como as que existem hoje, buscou resolver os problemas apresentados nos períodos anteriores. Nessas leis, percebe-se a consciência do problema de que a tutela dos dados pessoais não poderia ser baseada simplesmente na escolha individual, ao passo que prevê instrumentos que elevam o padrão coletivo de proteção. Vislumbra-se, igualmente, uma forte dose de pragmatismo, voltada para a busca de resultados concretos, os quais as gerações anteriores falharam em obter[53].

Em um primeiro momento, algumas das normas buscaram fortalecer a posição dos indivíduos em face às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio existente nessa relação e tornando mais efetivo o seu controle sobre os dados pessoais[54]. Isso foi viabilizado, por exemplo, a partir da instituição da "no fault compensation[55]" para reclamações individuais a respeito da violação à proteção de dados pessoais nas leis nacionais da Alemanha e Noruega.

Paradoxalmente, algumas leis retiraram da esfera de controle do indivíduo determinados assuntos, por compreenderem que algumas modalidades de tratamento de dados pessoais são tão relevantes para o cidadão que necessitam de uma proteção mais robusta, a qual não poderia ser alcançada por meio de uma

[51] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 212.
[52] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, pp. 42-43.
[53] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 212.
[54] Ibidem, p. 212.
[55] De acordo com o site de consultoria jurídica US Legal, "No-fault compensation refers to a compensation scheme based on the principle that injured persons are entitled to receive compensation for their injuries, without proving fault against the opposite party". Essencialmente, os indivíduos que fossem a juízo alegando alguma violação à proteção de seus dados não precisariam comprovar a culpa da parte ofensora/oposta. Em relação ao direito brasileiro pode ser traçado um paralelo com a inversão do ônus da prova, instituto incorporado pela LGPD em seu art. 8º, § 2º: "Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei"; e em seu art. 42, § 2º: "O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa".

simples disposição individual. Tal fenômeno pode ser observado na proibição, total ou parcial, imposta ao tratamento de dados pessoais considerados sensíveis, que são aqueles cujo tratamento tem grande potencial de acarretar discriminação, tais como os dados relativos a etnia, orientação sexual, opinião política e religião[56].

Outra característica peculiar da quarta geração de leis de proteção de dados consiste no surgimento de normas setoriais, conexas aos regramentos gerais de proteção de dados, cuja função é ampliar a proteção do indivíduo nos diversos setores em que é possível o tratamento de seus dados pessoais (setor de saúde ou setor bancário, por exemplo), de modo que a legislação passe a contemplar as diversas especificidades setoriais existentes. Dessa forma, percebe-se na maioria dos países europeus a existência de um regramento geral sobre proteção de dados, além de leis setoriais suplementares[57]. Ainda, é marcante nessa geração a disseminação do modelo das autoridades administrativas independentes, responsáveis pela implementação e aplicação da legislação de proteção de dados[58].

De acordo com Mayer-Schönberger[59], a Diretiva Europeia sobre proteção de dados pessoais de 1995[60] reflete essa evolução geracional pela qual passou a disciplina de proteção de dados pessoais na Europa, visto que está em sua essência a participação do indivíduo no processo de tratamento de dados pessoais e, ainda, prevê que o tratamento de dados sensíveis fique condicionado ao consentimento expresso e informado do indivíduo[61].

Pelo que pôde ser visto até o momento, nota-se que a disciplina da proteção de dados pessoais passou por uma transformação dinâmica e expressiva nas últimas décadas, especialmente em razão dos avanços na área da tecnologia. Além disso, destaca-se a incessante busca dos legisladores, em reação às demandas sociais, por um modelo de normas que garanta ao indivíduo um ambiente no qual ele tenha condições de desenvolver a própria personalidade, livre de ingerências externas, fato que se mantém relevante até os dias de hoje. Afinal, como bem

[56] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 43.
[57] Ibidem, pp. 43-44.
[58] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 213.
[59] *Apud* MENDES, 2014, p. 44.
[60] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[61] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 44.

definiu a Corte Constitucional alemã no ano de 1983[62], a proteção dos dados pessoais do indivíduo é um pressuposto para que ele não seja submetido a formas de controle social que, em última análise, anulariam sua individualidade, cercearam sua autonomia privada e, por conseguinte, inviabilizariam o livre desenvolvimento de sua personalidade.

[62] Subcapítulo 1.2.

CAPÍTULO 2 – O CONSENTIMENTO NO ÂMBITO DA PROTEÇÃO DE DADOS PESSOAIS

Como referido no capítulo anterior, a regulação jurídica do tratamento de dados pessoais está amparada na ideia de que o indivíduo deve ter autonomia para controlar a utilização (ou não) dos seus dados pessoais na sociedade, a fim de que ele possa desenvolver espontaneamente a sua personalidade, livre de ingerências externas. Cabe ao Estado, portanto, por intermédio de leis, prover os mecanismos necessários para que o cidadão possa exercer o controle do fluxo de informações a seu respeito[63].

Dessa forma, para que o indivíduo possa exercer o seu direito de autodeterminação informacional, faz-se necessário um instituto jurídico por meio do qual se manifeste a sua vontade de autorizar, ou não, o processamento de seus dados pessoais: o consentimento. É deste instrumento que o direito lança mão para fazer valer a autonomia privada do cidadão[64].

2.1. O consentimento e suas falhas na relação com a proteção de dados pessoais

De acordo com Danilo Doneda, "o consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade[65]". Assim, o seu uso como instrumento emblemático para a tutela dos dados pessoais deve ser analisado a partir dos efeitos da sua aplicação em situações reais, no âmbito da proteção de dados pessoais.

Sob tal viés prático, a questão do consentimento no âmbito da proteção de dados pessoais enfrenta algumas dificuldades. Em primeiro lugar, apresenta-se o problema da eficácia do consentimento no tratamento de dados pessoais, tendo em vista que o fato de o indivíduo não consentir pode acarretar na sua exclusão do

[63] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 60.
[64] Ibidem, p. 60.
[65] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 372.

mercado de consumo e da sociedade. Além disso, há o problema da violação da proteção de dados pessoais que ocorre posteriormente ao tratamento ter sido consentido pelo titular dos dados; e, ainda, há a questão do consentimento aplicado ao tratamento de dados sensíveis[66].

Como demonstrado na análise da evolução geracional das leis de proteção de dados pessoais[67], tanto a segunda quanto a terceira geração de normas visaram a firmar a participação do indivíduo no processo de tratamento de dados. Contudo, os altos custos sociais (e monetários, por vezes) que os cidadãos teriam de suportar para exercer o seu direito à autodeterminação informacional acabaram por tornar ilusória essa participação. Vale trazer à tona, novamente, o exemplo empregado por Mayer-Schönberger, de que somente os eremitas alcançariam a proteção plena de seus dados, dado o custo social que o indivíduo teria de pagar por isso[68].

O autor também levanta outro ponto importante no que se refere à relação entre consentimento e a proteção de dados pessoais: já que o consentimento do indivíduo autoriza o processamento dos seus dados, na eventualidade de violação ao seu direito à privacidade, como poderia ele buscar a tutela dessa violação, se havia – em um primeiro momento – autorizado o tratamento de seus dados pessoais?[69] Sob uma ótica muito similar, Doneda faz menção ao "paradoxo da privacidade": na medida em que o consentimento centraliza a disciplina da proteção de dados pessoais, aquele que teve o seu direito violado só poderia obter a tutela em um momento posterior à concessão deste consentimento, valendo-se da arguição de alguma falha na concessão dele (e.g. um vício de consentimento). Isso implica que o cidadão tenha que, em primeiro lugar, conceder acesso a seus dados para, somente então, se valer dessa tutela[70].

---

[66] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 61.

[67] Vide subcapítulo 1.3.

[68] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001, pp. 228-229. "But what price does one have to pay for that? Is it acceptable that such data-protection liberties can be exercised only by hermits? Have we reached an optimum of data protection if we guarantee privacy rights that, when exercised, will essentially expel the individual citizen from society?"

[69] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 61.

[70] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, pp. 374-375.

Para a solução dessas questões, é fundamental compreender que o consentimento possui dois perfis no âmbito da proteção de dados pessoais. No primeiro, o consentimento se apresenta como o instrumento da autodeterminação do indivíduo em face de seus dados pessoais e, portanto, como instrumento de tutela da pessoa. Já no segundo, o consentimento é o mecanismo de legitimação para que esses dados sejam, de alguma forma, utilizados por terceiros. A ideia de que alguém estaria abrindo mão da proteção de seus dados pessoais ao consentir, portanto, é equivocada, visto que se trata apenas de um exercício de escolha do indivíduo, na esfera da sua autodeterminação informacional[71].

Por fim, também deve ser enfrentada a questão do consentimento quando ele se defronta com os chamados dados sensíveis, isto é, dados cujo tratamento pode ser potencialmente discriminatório[72]. Para a solução dessa questão, muitas das normas de proteção de dados retiram da esfera de controle do indivíduo esses assuntos, sob o argumento de que se trata de algo tão relevante para o cidadão, que ele não poderia dispor a respeito. Outra solução que pode ser observada nas normas de proteção de dados é a exigência de que o consentimento – quando se busca o tratamento de dados sensíveis – seja dado de forma específica e destacada, como é o caso da Lei Geral de Proteção de Dados (LGPD) em seu art. 11[73].

2.2. A natureza jurídica do consentimento

A natureza jurídica do consentimento no âmbito da proteção de dados pessoais é, de acordo com Laura Schertel Mendes, um tema bastante polêmico. Na

[71] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, pp. 378. Como será mais bem detalhado no subcapítulo 3.1.2., a proteção da privacidade foi classificada pelo Código Civil como um direito da personalidade. Assim sendo, a privacidade tornou-se um atributo irrenunciável. Parte da doutrina compreende, ainda, que a proteção de dados pessoais também seria, por extensão, um direito da personalidade e, logo, irrenunciável.

[72] De acordo com a Lei Geral de Proteção de Dados brasileira (lei nº 13.709, de 14 de agosto de 2018), dado sensível é aquele "[...] sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;".

[73] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; [...]

Alemanha, segundo a autora, existem três correntes majoritárias que tentam dar uma resposta a essa questão: I) a primeira entende que o consentimento para o tratamento de dados tem natureza de uma declaração de vontade negocial (*rechtsgeschäftliche Erklärung*); II) a segunda defende que se trata de um ato jurídico unilateral sem natureza negocial (*Realhandlung*); III) e a terceira linha sustenta que o consentimento para o tratamento de dados pessoais é um ato que se parece com o negócio jurídico, sem o ser (*geschäftsähnliche Handlung*)[74].

A autora destaca que este último entendimento é predominante nos dias atuais e, segundo ela, o mais correto, pois o consentimento no âmbito do processamento de dados tem natureza claramente atípica, na medida em que é dotado de características negociais e, ao mesmo tempo, possui caráter personalíssimo. De acordo com Kohte[75], seria necessário fazer uma análise casuística para se definir as normas aplicáveis a uma situação concreta. Para este autor, a função do consentimento para o tratamento de dados pessoais é a mesma da declaração de vontade no âmbito de um negócio jurídico, visto que ambos visam à autodeterminação do indivíduo. Em outras palavras, seria possível aplicar a este consentimento as regras relativas aos negócios jurídicos, se assim fosse adequado e necessário.

Complementarmente, Mendes refere de forma exemplificativa que as normas relativas à capacidade civil (arts. 3º e 4º do Código Civil) não se aplicariam necessariamente à questão do consentimento no âmbito da proteção de dados pessoais, diferentemente do que ocorreria numa relação negocial qualquer. Afinal, o fundamental seria identificar se a pessoa tem capacidade de discernimento para autorizar determinado tipo de coleta ou tratamento de dados, sendo prescindível a capacidade civil. Por exemplo, de acordo com o mais novo regulamento europeu sobre o assunto proteção de dados, nomeado *General Data Protection Regulation* (GDPR), a partir dos 16 anos o indivíduo já teria condições para consentir a respeito do tratamento de seus dados pessoais[76]. Nota-se, portanto, o viés personalíssimo do consentimento, para além da sua natureza negocial.

---

[74] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 62.

[75] *Apud* MENDES, 2014, p. 63.

[76] Art. 8º, nº 1: "Quando for aplicável o artigo 6.o, nº 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16

Sob essa perspectiva, a possibilidade de o indivíduo revogar o consentimento dado anteriormente adquire grande importância. Esse direito é essencial para que ele possa autodeterminar as suas informações pessoais e, por conseguinte, desenvolver livremente a sua personalidade.

Na Lei Geral de Proteção de Dados brasileira, esse direito está previsto no art. 8º, § 5º[77]. Vale destacar que, de acordo com esta lei, não há necessidade de justificação para a revogação do consentimento[78], sendo necessária somente a manifestação expressa do titular. De acordo com a doutrina alemã – que também adota esse posicionamento – a revogabilidade do consentimento é condição fundamental para que o indivíduo possa exercer o seu direito à autodeterminação informacional de forma efetiva e sem limites[79]. No mesmo sentido, consigna Danilo Doneda: "A ideia de revogabilidade incondicional deste tipo de consentimento encontra fundamento no fato de que se está protegendo a própria personalidade, entre cujos atributos estaria a indisponibilidade[80]". Além do mais, é impossível que o indivíduo visualize e avalie adequadamente todas as consequências do seu consentimento logo no início do processo de tratamento de dados, o que reforça a tese de que a revogação do consentimento deve depender exclusivamente de sua vontade.

Por fim, conforme retratado no capítulo anterior, o alastramento de autoridades independentes para a implementação e aplicação das leis de proteção

---

anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança [...] Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos". Vale também destacar que não há na LGPD menção expressa a um critério objetivo para definir qual seria a idade necessária para que um indivíduo possa consentir de forma válida para o tratamento de seus dados. A lei apenas se vale do termo "criança" para definir aquele que necessita de representação. Nesse sentido, o art. 14 refere o seguinte: "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente". E o seu § 1º complementa: "O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal".

[77] § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

[78] Traz-se à tona esta discussão, pois em alguns países – como a Espanha – a revogação do consentimento para o tratamento de dados exige uma causa justificada.

[79] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 64.

[80] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 380.

de dados pessoais[81], bem como de leis que retiraram da esfera de controle do indivíduo a escolha sobre o processamento de certos tipos de dados pessoais, como os dados sensíveis, acabaram por relativizar o já mencionado protagonismo do consentimento no âmbito da proteção de dados pessoais. Ao mesmo tempo, embora o papel do consentimento possa ter sido mitigado, o progresso geracional das leis de proteção de dados[82] não eliminou o seu protagonismo, visto que a sua centralidade permaneceu sendo o traço marcante de toda e qualquer abordagem regulatória. Tanto é verdade que, durante esse processo evolutivo, o consentimento passou a ser adjetivado, como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como pode ser visto na Diretiva Europeia sobre proteção de dados pessoais de 1995[83].

Em suma, na evolução das leis de proteção de dados pessoais, o consentimento percorre um caminho pelo qual ele surge, é questionado e se reafirma como sendo o vetor principal da disciplina[84].

2.3. As *privacy guidelines* da Organização para a Cooperação e Desenvolvimento Econômico

Para uma melhor compreensão da trajetória acima descrita, é fundamental a análise das diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sobre a proteção da privacidade e a circulação transfronteiriça de dados pessoais[85].

A OCDE é uma organização internacional criada após a Segunda Guerra Mundial, em 1948[86], cuja missão é promover a construção de melhores políticas econômicas e sociais para um mundo melhor[87]. Atualmente, a organização conta

[81] Ibidem, p. 213.
[82] Conforme retratado no subcapítulo 1.3.
[83] Tal documento será tratado de forma mais específica no subcapítulo 2.4., a seguir.
[84] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 117.
[85] OECD guidelines on the protection of privacy and transborder flows of personal data.
[86] Mais detalhes sobre criação da OCDE em: <http://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm>
[87] "The Organisation for Economic Co-operation and Development (OECD) is an international organisation that works to build better policies for better lives. Our goal is to shape policies that foster prosperity, equality,

com 36 países membros – unidos por valores como a democracia pluralista, o respeito aos direitos humanos e a economia de mercado – e tem como objetivo estabelecer uma relação de cooperação entre eles para a solução de diversos problemas de natureza social, econômica e ambiental[88].

Em 1980, diante da forte relação de dependência desenvolvida entre a tecnologia da informação e o desenvolvimento econômico e social (especialmente na figura do processamento automatizado de dados), a OCDE decidiu emitir dois importantes documentos[89] (*privacy guidelines*, em 1980; e *declaration on transborder data flows*, em 1985), os quais vieram a influenciar mundialmente a evolução do tema da proteção de dados pessoais.

Essas *guidelines*, ou diretrizes, estabeleceram padrões normativos para a proteção dos dados pessoais, visando ao livre fluxo de informações entre os países membros e buscando conciliar o desenvolvimento econômico e a proteção da privacidade das pessoas residentes nestes países[90]. Para tanto, o documento possuía uma primeira parte geral conceitual sobre, por exemplo, a definição de dados pessoais, e uma segunda parte que vinculava os seus países membros a incorporar os princípios previstos em tal documento. O objetivo era criar um ambiente regulatório uniforme entre os países membros, a fim de garantir o livre trânsito de informações sem que houvesse o risco de violações aos dados pessoais ou à privacidade dos indivíduos[91].

Os oito princípios elencados são os seguintes: I) princípio da limitação da coleta (*collection limitation principle*); II) princípio da qualidade dos dados (*data quality principle);* III) princípio da especificação dos propósitos (*purpose specification principle*); IV) princípio da limitação do uso (*use limitation principle*); V) princípio dos padrões de segurança (*security safeguards principle);* VI) princípio da abertura (*openness principle*); VII) princípio da participação individual (*individual participation*

---

opportunity and well-being for all. We draw on almost 60 years of experience and insights to better prepare the world of tomorrow". Disponível em: <https://www.oecd.org/about/>.

[88] Lista de países membros disponível em <https://www.oecd.org/about/members-and-partners/>.

[89] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publications Service, 2001, p. 7.

[90] Ibidem, p. 11.

[91] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, pp. 118-119.

principle) e; VIII) princípio da responsabilidade (*accountability principle*)[92]. Destes oito, percebe-se que a metade deles faz alusão expressa ao titular dos dados. Um deles é nomeado, inclusive, como princípio da participação individual.

Nesse sentido, o princípio da limitação da coleta[93] e o princípio da especificação dos propósitos[94] estabelecem a forma por meio da qual o titular dos dados deve ser informado sobre a finalidade do processamento dos seus dados para que possa, então, autorizar ou desautorizar tal tarefa, de modo a consolidar a sua participação ao longo de todo o fluxo informacional[95].

Ademais, o princípio da participação individual[96] garante ao indivíduo o direito de contestar as informações relativas à sua pessoa que estejam em posse de terceiros, podendo ele retificar, emendar, completar e até mesmo apagar os seus dados pessoais.

Como pode ser visto, trata-se de normas que alçam o titular dos dados pessoais ao papel de protagonista no âmbito da proteção de dados. O próprio conceito do que seria um tratamento de dados adequado e lícito é vinculado ao consentimento do indivíduo[97].

Vale dizer que essas diretrizes normativas consolidadas pelas *guidelines* da OCDE também são chamadas tradicionalmente de *Fair Information Practice Principles* (FIPPs). Isso porque, em 1973, o Comitê de Aconselhamento sobre Sistemas de Dados Automatizados[98], pertencente ao Departamento de Saúde, Educação e Bem-estar[99] do governo dos Estados Unidos, propôs que o congresso

---

[92] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publications Service, 2001, pp. 14-16.

[93] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publications Service, 2001, p. 14. "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

[94] Ibidem, p.15. "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

[95] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 119.

[96] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publications Service, 2001, p. 16. "An individual should have the right: (…) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

[97] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 119.

[98] Advisory Committee on Automated Personal Data Systems.

[99] Department of Health, Education and Welfare.

norte-americano transformasse em lei o chamado "Code of Fair Information Practices", relativo à proteção de dados pessoais dos cidadãos estadunidenses, e que pode se resumido em cinco princípios gerais: transparência, limitação de uso, acesso e retificação, qualidade dos dados, e segurança[100]. Estes princípios, contudo, somente receberam atenção mundial ao serem adotados e aperfeiçoados pela OCDE na forma das *privacy guidelines*.

Novamente, como pode ser percebido a partir da análise das FIPPs, a carga participativa do indivíduo é o elemento central para designar o que seria uma atividade adequada (ou inadequada) de tratamento de dados pessoais. Em virtude dessa visão de que a proteção dos dados do cidadão deveria girar essencialmente ao redor da ideia de autodeterminação informacional, a doutrina situa as *guidelines* da OCDE entre a terceira e a quarta geração de leis de proteção de dados pessoais[101].

O segundo documento publicado pela OCDE, (*declaration on transborder data flows*, de 1985) buscou solucionar os problemas que emergiram em razão do grande fluxo transfronteiriço de dados pessoais. Informações relativas a cultura, tecnologia, atividades comerciais e empresariais, migravam todos os dias de um país a outro, algo que trazia enormes implicações socioeconômicas. Ao incorporam este documento a seus ordenamentos jurídicos, os governos reafirmaram seu compromisso de desenvolver um ambiente regulatório harmônico, que não obstruísse o livre fluxo informacional entre os países membros[102].

Passados aproximadamente 30 anos de sua publicação, à luz das mudanças tecnológicas e da crescente importância das "identidades digitais[103]", as *guidelines*

---

[100] CATE, Fred H. The failure of Fair Information Practice Principles. In: WINN, Jane K. (ed.). Consumer Protection in the Age of the 'Information Economy'. Hampshire: Ashgate Publish, 2006, pp. 3-4. A autora ainda acrescenta que estes princípios serviram de base para uma das leis norte-americanas de proteção de dados que vigora até hoje, o "Privacy Act".

[101] Vide subcapítulo 1.3.

[102] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publications Service, 2001, p. 10. "On the 11 April 1985, OECD Ministers adopted the Declaration on Transborder Data flows. This Declaration addressed the policy issues arising from flows of personal data across national borders, e.g. flows of data and information related to trading activities, intracorporate laws, computerized information services, and scientific and technological exchanges. In adopting this Declaration, OECD governments reaffirmed their commitment to developing common approaches to Transborder data flow issues and, when appropriate, developing harmonized solutions".

[103] The OECD Privacy Framework, 2013, p. 3. "This revision is the first since the original 1980 release of the Guidelines and arises out of a call by Ministers (...) to assess the Guidelines in the light of 'changing technologies, markets and user behavior, and the growing importance of digital identities'".

passaram por um processo de revisão no ano de 2013. Este processo manteve a sua estrutura principal, porém trouxe uma visão mais pragmática ao documento, visando soluções efetivas à questão da proteção da privacidade em uma dimensão global[104].

Por um lado, a ideia de autodeterminação informativa permaneceu intacta, porém com a ressalva de que novas tecnologias emergiram e, com isso, a coleta e o uso dos dados pessoais se tornaram mais complexos e menos transparentes. De acordo com o processo de revisão, seriam necessários, portanto, meios que reduzissem essa opacidade e garantissem ao indivíduo controle sobre os seus dados. Percebe-se, assim, que o consentimento, no âmbito das *guidelines* da OCDE, passou pelo mesmo movimento pendular: ele emergiu, foi questionado e então reafirmado como ponto central da dinâmica regulatória[105].

De outro, a missão de desenvolver um ambiente regulatório harmônico, idealizado na *declaration on transborder data* flows, permanece no horizonte regulatório dos países membros da OCDE. De acordo com o processo revisório, a "interoperabilidade[106]" legal entre os países deve ser melhorada por meio de ações coordenadas para a aplicação e fiscalização das leis de proteção de dados pessoais, já que se trata de um elemento fundamental para o livre fluxo informacional transfronteiriço[107].

Nos termos da própria OCDE, as *privacy guidelines* foram um grande sucesso. Elas estabeleceram o primeiro conjunto de princípios internacionais relativos à proteção de dados e, por meio disso, influenciaram as mais variadas legislações sobre o assunto ao redor do mundo[108]. A coluna vertebral desse processo, como se demonstrou, foi o deslocamento do titular dos dados ao papel de protagonista no processo de tratamento dos seus dados, o que justifica, portanto, a grande importância dada ao consentimento na vasta maioria das leis de proteção de dados editadas desde a década de 1980 até os dias de hoje.

---

[104] The OECD Privacy Framework, 2013. Disponível em: <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>. "Two themes run through the updated Guidelines: A focus on the practical implementation of privacy protection through an approach grounded in risk management, and the need to address the global dimension of privacy through improved interoperability."

[105] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 121.

[106] Interoperability.

[107] Ibidem, p. 121.

[108] The OECD Privacy Framework, 2013, p. 66.

2.4. O consentimento no direito comunitário europeu

Tendo em vista que as primeiras normas de proteção de dados pessoais surgiram na Europa, o direito comunitário europeu reflete bem a trajetória do consentimento neste âmbito legislativo. Desde a influência exercida pelas *privacy guidelines*, editadas pela OCDE em 1980, até o regulamento mais recente oriundo do bloco europeu, o *General Data Protection Regulation* (GDPR), o consentimento vem permeando as regulações europeias sobre proteção de dados pessoais.

A primeira normatização sobre o tema, advinda da influência exercida pelas *guidelines* da OCDE, se dá por meio da Convenção nº 108 de Estrasburgo, editada pelo Conselho da Europa. Nela, os Estados signatários reafirmaram o seu compromisso com a liberdade informacional, independentemente de fronteiras, e se propuseram a conciliar o respeito à privacidade e o livro fluxo informacional[109]. Há neste documento, inclusive, um capítulo inteiro dedicado ao "fluxo transfronteiriço de dados[110]". Já se percebia naquela época, portanto, o alinhamento ideológico entre o organismo internacional e o bloco europeu[111].

No mesmo sentido, em 1995 é editada a Diretiva Europeia 95/46/CE[112], a qual possuía como objetivo, igualmente, o desenvolvimento socioeconômico europeu mediante ações que mitigassem o efeito das fronteiras nacionais[113], tendo em vista o aumento do fluxo "transfronteiras" de dados pessoais[114]. Este regulamento adota, eminentemente, as diretrizes da OCDE como o seu principal alicerce, ao passo que

[109] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Estrasburgo, Conselho da Europa, 1981, p. 1.
[110] Capítulo III – Transborder data flows.
[111] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 122.
[112] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[113] Ibidem, considerando (1): "Considerando que os objetivos da Comunidade [...] consistem em estabelecer uma união cada vez mais estreita entre os povos europeus, em fomentar relações mais próximas entre os Estados que pertencem à Comunidade, em assegurar o progresso econômico e social mediante ações comuns para eliminar as barreiras que dividem a Europa [...]".
[114] Ibidem, considerando (5): "Considerando que a integração econômica e social resultante do estabelecimento e funcionamento do mercado interno nos termos do art. 7º A do Tratado irá necessariamente provocar um aumento sensível dos fluxos transfronteiras de dados pessoais entre todos os intervenientes [...]".

a autodeterminação do indivíduo é o que baliza a legalidade de qualquer atividade de tratamento de dados pessoais[115].

Fica evidente, por conseguinte, a importância dada por esta diretiva ao consentimento do titular dos dados pessoais, especialmente no capítulo II, no qual são estipuladas as condições gerais para tratamento de dados pessoais. Conforme o art. 7º, por exemplo, o consentimento inequívoco do titular constitui pressuposto para o tratamento de dados pessoais, salvo nas hipóteses de previsão contratual ou legal[116]. O consentimento é definido, por sua vez, no art. 2º, h, como "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto (*sic*) de tratamento".

Essa adjetivação do consentimento, como devendo ser inequívoco, livre, específico e informado, é uma das características marcantes do progresso geracional das leis de proteção de dados, na medida em que busca resolver a problemática envolvendo o controle pouco efetivo das informações por parte de seu titular. Nesse seguimento, a diretiva, além de impor o direito de o titular dos dados pessoais controlar as suas próprias informações, impõe deveres àqueles que processam os dados pessoais (*data controllers*), a fim de aperfeiçoar tal estratégia regulatória[117].

Exemplificativamente, o art. 6º, 1, c, cria a obrigação de que o *data controller* colete apenas dados adequados, não excessivos e pertinentes às finalidades para que são recolhidos e posteriormente tratados[118]. Trata-se da ideia de minimização dos dados, a qual permitirá, em suma, que o titular dos dados pessoais maximize a

[115] O capítulo II do documento apresenta as "Condições Gerais de Licitude do Tratamento de Dados Pessoais".
[116] Artigo 7º: "Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se: a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito [...]".
[117] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 123.
[118] Art. 6º, 1: "Os Estados-membros devem estabelecer que os dados pessoais serão: c) adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente".

sua esfera de controle sobre as suas informações pessoais. Afinal, quanto menos dados em fluxo, mais simples se torna o controle sobre eles[119].

A abordagem regulatória da Diretiva Europeia 95/46/CE é centrada, portanto, em dois atores: o titular dos dados pessoais e quem os processa (*data controller*). O regramento, então, por meio de direitos e obrigações simétricas atribuídas a ambos os atores, busca garantir o controle do indivíduo sobre suas informações pessoais[120].

Percebe-se, assim, a evolução da diretiva europeia em comparação às *privacy guidelines* da OCDE. Enquanto aquela determinava que a busca pela minimização do fluxo de dados deveria partir do responsável pela atividade de tratamento de dados (*data controller*), estas imputavam a referida minimização apenas ao titular dos dados, dentro da ideia de autodeterminação informacional. É em virtude dessa diferença que a doutrina posiciona as *guidelines* na terceira geração das leis de proteção de dados pessoais e a diretiva, por sua vez, na quarta geração. Como já referido no subcapítulo 1.3., esta geração busca empoderar o indivíduo ao lhe garantir total controle sobre suas informações pessoais, algo que é alcançado por meio de normas que regem não somente a atuação do titular dos dados, mas de todos os sujeitos participantes do fluxo informacional[121].

Na sequência, a Diretiva Europeia 2002/58/CE[122] surge para regular a questão da privacidade e da proteção de dados no âmbito das comunicações eletrônicas. Nos considerandos dessa diretiva fica clara a preocupação do Conselho Europeu em se adaptar às novas tecnologias, como se vê, por exemplo, no considerando número 5[123].

---

[119] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 123.
[120] Ibidem, pp. 123-124.
[121] Ibidem, p. 124.
[122] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas).
[123] Estão a ser introduzidas nas redes de comunicações públicas da Comunidade novas tecnologias digitais avançadas, que suscitam requisitos específicos de proteção de dados pessoais e da privacidade do utilizador. O desenvolvimento da sociedade da informação caracteriza-se pela introdução de novos serviços de comunicações electrónicas. O acesso a redes móveis digitais está disponível a custos razoáveis para um vasto público. Essas redes digitais têm grandes capacidades e possibilidades de tratamento de dados pessoais. O desenvolvimento transfronteiriço bem sucedido desses serviços depende em parte da confiança dos utilizadores na garantia da sua privacidade.

Nesse sentido, o documento traz algumas questões genéricas importantes, como a reiteração daquilo que foi proposto na Diretiva 95/46/CE no tocante ao consentimento, afirmando que ele deve ser livre, específico e informado, inclusive no meio digital, para que o indivíduo possa ter controle sobre seus dados pessoais[124]. Ainda, assinala que o consentimento sempre deverá ser dado de forma prévia ao tratamento dos dados, salvo em situações excepcionais (e.g., obrigação legal). Essa diretiva, por outro lado, também traz questões altamente específicas, como as relacionadas às formas de coleta de dados pessoais no meio digital (*spyware*, *web bugs*[125] e *cookies*[126]), referindo quando o uso destes meios é legítimo ou não.

Enfim, no ano de 2016, o Conselho Europeu promulga um novo regulamento geral de proteção de dados, em substituição à Diretiva Europeia 95/46/CE, chamado *General Data Protection Regulation*, ou apenas GDPR[127]. Verifica-se, mais uma vez, a preocupação central com a questão do consentimento[128], que é definido da seguinte forma:

> *Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*[129].

Nota-se nessa definição, novamente, uma série de adjetivos associados ao consentimento, sendo que desta vez fica claro que tais adjetivos são cumulativos, tendo em vista o uso do termo “e”. O mais importante nessa definição, contudo, é

---

[124] Vide considerando 17 da diretiva. “Para efeitos da presente directiva, o consentimento por parte do utilizador ou assinante, independentemente de este ser uma pessoa singular ou colectiva, deve ter a mesma acepção que o consentimento da pessoa a quem os dados dizem respeito conforme definido e especificado na Directiva 95/46/CE. O consentimento do utilizador pode ser dado por qualquer forma adequada que permita obter uma indicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática ao visitar um sítio na internet.”

[125] Vide considerando 24 da diretiva.

[126] Vide considerando 25 da diretiva.

[127] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[128] A título de curiosidade, a palavra “consentimento” é citada 72 (setenta e duas) vezes ao longo do documento.

[129] Conforme art. 4º, 11, GDPR.

que o próprio texto do inciso (art. 4º, 11) define qual deve ser o resultado esperado: o consentimento deve corresponder aos anseios do titular dos dados pessoais, seja por meio de uma declaração ou de uma ação afirmativa representativa[130].

Essa nova regulamentação também traz um artigo específico para tratar das condições do consentimento, chamado "condições aplicáveis ao consentimento[131]". Dentre as suas disposições encontra-se, por exemplo, a obrigação de que o pedido de consentimento seja apresentando de forma inteligível, numa linguagem clara e simples[132]. O considerando 42 do regulamento apresenta uma breve síntese de como este encara o tratamento de dados pessoais baseado no consentimento de seu titular:

> *Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado[133].*

[130] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 125.
[131] Conforme artigo 7º, GDPR.
[132] Conforme artigo 7º, 2, GDPR: "Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento."
[133] Considerando 42, GDPR.

Mais uma vez, portanto, o consentimento é tratado como protagonista, sendo um dos principais elementos presentes na nova regulação sobre proteção de dados em vigor na Europa, o *General Data Protection Regulation*.

A trajetória delineada acima demonstra como o progresso geracional das leis de proteção de dados pessoais tomou forma no direito comunitário europeu. Nessa breve síntese, foi dada grande atenção à figura do consentimento, que, como pôde ser visto, esteve na linha de frente ao longo de todo o percurso, desde as *privacy guidelines* da OCDE até o novíssimo regulamento europeu sobre proteção de dados, o GDPR.

À vista disso, verifica-se que o titular dos dados pessoais assumiu o papel de protagonista no tratamento de suas informações a partir da segunda geração de leis de proteção de dados pessoais[134]. Naquele momento, foi adotada uma estratégia regulatória que depositava sobre o indivíduo a responsabilidade de proteger os seus próprios dados pessoais, a qual recorreu à figura do consentimento em busca de sustentação. Assim, a técnica legislativa de exigir o consentimento do titular dos dados pessoais para que eles fossem, então, coletados, utilizados e compartilhados, tornou-se o principal alicerce das leis de proteção de dados ao redor do mundo[135].

Essa noção de autodeterminação informacional permeou grande parte do processo evolutivo das normas de proteção de dados pessoais, das *privacy guidelines* da OCDE até às leis de quarta geração. Desse modo, consolidou-se uma crença reducionista de que a autodeterminação informacional corresponderia em absoluto à autonomia da vontade do titular dos dados[136].

Mesmo com a adoção de algumas medidas que tornaram menos incisiva a atuação do consentimento no âmbito da proteção de dados pessoais, como o surgimento de autoridades independentes para a implementação e aplicação das leis de proteção de dados pessoais[137] e a edição de leis que afastaram da esfera individual a escolha sobre o processamento de certos tipos de dados (como os sensíveis), o consentimento manteve o seu papel central em grande parte das

[134] Vide subcapítulo 1.3.
[135] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 136.
[136] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 137.
[137] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 213.

legislações que versam sobre a matéria. Trata-se de um processo de aposta no indivíduo, visto como um ser capaz, racional e hábil para controlar as suas informações pessoais.

Todavia, parte da doutrina encara essa concepção como algo ultrapassado, que não mais se ajusta à situação atual dos dados pessoais, os quais se tornaram um ativo econômico e acabam, invariavelmente, por modular o livre desenvolvimento da personalidade dos cidadãos[138].

Percebe-se, por fim, certa preocupação dos estudiosos da matéria com a efetividade das normas atuais de proteção de dados pessoais, diante das mudanças sociais e da ubiquidade da tecnologia. Busca-se, notadamente, um aprimoramento dessas leis a fim de que se adequem aos desafios apresentados pela atualidade. Tal objetivo, segundo eles, não seria atingido pela simples desvinculação das noções de proteção de dados pessoais e autodeterminação informacional, as quais deverão permanecer no cerne do debate. Trata-se de um processo natural de evolução, afinal, como visto até aqui, um componente essencial dessa disciplina é a busca permanente pela evolução, de modo a não ficar obsoleta diante dos novos desenvolvimentos tecnológicos e das novas práticas sociais e econômicas propiciadas pela tecnologia[139].

[138] Ver, nesse sentido, BIONI (p. 137) e MENDES (p.82).
[139] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 82.

CAPÍTULO 3 – A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A Constituição Federal[140] (CF), ao tratar do tema da privacidade, é objetiva ao determinar a proteção da intimidade, da vida privada, da honra e da imagem como direitos fundamentais, nos termos do artigo 5º, inciso X[141]. No mesmo sentido, o artigo 5º, inciso XII, inclui no rol de direitos fundamentais a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ressalvadas algumas hipóteses de investigação criminal ou instrução processual penal[142].

Contudo, embora reconheça o direito fundamental à privacidade, a Constituição de 1988 não menciona expressamente a proteção de dados pessoais. Segundo Danilo Doneda, o elemento de maior destaque na Constituição para a proteção de dados seria o *habeas data*, previsto no art. 5º, inciso LXXII[143], da CF, e regulamentado posteriormente pela lei 9.507/97[144].

No entanto, o alcance do *habeas data* é limitado, tanto no que diz respeito à sua forma – pois se trata de uma ação constitucional e não de um direito material expresso[145] –, quanto no que se refere à sua origem – tendo em vista que foi concebido logo após o final da ditadura militar, como um instrumento para a requisição de informações pessoais em mãos do poder público, em particular dos órgãos responsáveis pela repressão durante o período[146], e não com o intuito de

---

[140] Constituição da República Federativa do Brasil de 1988.

[141] Art. 5º: "[...] 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". Para os efeitos deste trabalho, os conceitos de intimidade e vida privada serão tratados como sinônimos de privacidade, embora exista, no direito brasileiro, uma distinção entre os conceitos. Tal diferença fica clara em FERRAZ JÚNIOR, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista Da Faculdade De Direito, Universidade De São Paulo, 88, pp. 3-5.

[142] Art. 5º: "[...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

[143] Art. 5º: "[...] LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

[144] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 326.

[145] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 168.

[146] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 104.

assegurar a proteção de dados do indivíduo diante de um contexto de massificação de informações.

A fim de suprir essa lacuna legislativa, portanto, foram editadas diversas leis a respeito do assunto no decorrer dos últimos anos, culminando na promulgação da Lei Geral de Proteção de Dados, no ano de 2018. Algumas delas serão analisadas com maior afinco nas próximas páginas, mantendo-se o foco na figura do consentimento.

3.1. Legislação esparsa

3.1.1. Código de Defesa do Consumidor

A primeira lei que abordou o tema da privacidade e da proteção de dados pessoais de forma moderna, visando a enfrentar as novas tecnologias de processamento de dados, foi o Código de Defesa do Consumidor[147] (CDC). Tal feito pode ser observado em seu art. 43, responsável por regular os bancos de dados e cadastros de consumidores, nos seguintes termos:

> *Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.*
>
> *§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.*
>
> *§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*
>
> *§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.*
>
> *§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.*

[147] Lei nº 8.078, de 11 de setembro de 1990.

> *§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.*
>
> *§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.*

Nota-se, em primeira análise, a amplitude do dispositivo, a qual pode ser observada já no *caput* do artigo. A lógica legislativa por trás desse regulamento foi alcançar todo e qualquer dado pessoal do consumidor que pudesse estar presente em algum banco de dados, independentemente de sua natureza, como pode ser observado no § 4°, o qual equiparou os registros de dados de consumidores de qualquer gênero às entidades de caráter público.

Percebe-se, ademais, que a legislação consumerista optou por garantir ao consumidor o direito de controlar as suas informações pessoais, seguindo a estratégia regulatória proposta pelas *privacy guidelines* da OCDE[148]. De fato, todas as condutas impostas pelo art. 43 pavimentam o caminho para que o consumidor seja capaz de autodeterminar as suas informações pessoais, como pode ser visto, por exemplo, na exigência de que o consumidor seja notificado da abertura de um banco de dados pessoais que ele não solicitou. Essa exigência de comunicação viabiliza que o consumidor acompanhe o fluxo de seus dados pessoais, aumentado o seu controle sobre eles[149].

Essa noção de transparência (§ 2º) em relação aos dados pessoais é acompanhada pelos direitos de acesso (*caput*), retificação e cancelamento (§ 3º); e pelos princípios da qualidade dos dados (§ 1º) e da limitação temporal (também chamado de princípio do esquecimento)[150]. Todas essas normas são instrumentos disponibilizados pelo CDC ao consumidor para que este, na condição de titular dos dados pessoais, possa exercer a sua autodeterminação informacional[151].

---

[148] Vide subcapítulo 2.3.

[149] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 127.

[150] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 142.

[151] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 128.

3.1.2. Código Civil

A grande façanha do Código Civil[152] (CC) em relação ao assunto privacidade[153] é, notadamente, a inauguração de um capítulo destinado aos direitos da personalidade (Livro I, Título I, Capítulo II), dentre os quais se encontra o direito à privacidade. Como pode ser visto em seu art. 21: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Esse dispositivo é relevante, em primeiro lugar, pois traz para o âmago do direito civil aquilo que já havia sido previsto na CF[154], concretizando a proteção da privacidade como um direito fundamental no âmbito das relações privadas.

Além disso, o CC, ao introduzir o direito à privacidade no capítulo dos direitos da personalidade, evidencia a natureza jurídica do bem que se está protegendo, demonstrando a relação entre a tutela da privacidade e o desenvolvimento da personalidade do indivíduo. Os direitos da personalidade, afinal, são "um conjunto de bens que são tão próprios do indivíduo, que chegam a se confundir com ele mesmo e constituem as manifestações da personalidade do próprio sujeito[155]".

3.1.3. Lei do Cadastro Positivo

A Lei do Cadastro Positivo[156] surgiu com o objetivo de disciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito[157]. Assim, a situação econômica do postulante ao crédito passou a ser analisada não mais

---

[152] Lei nº 10.406, de 10 de janeiro de 2002.

[153] Não há no Código Civil menção expressa à questão da proteção de dados pessoais, razão pela qual, neste ponto, a atenção será voltada à proteção da privacidade, a qual possui uma relação muito estreita com o desenvolvimento da personalidade do indivíduo e com a proteção de dados pessoais, conforme já exposto neste trabalho.

[154] Constituição Federal, art. 5º: "[...] 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;".

[155] BELTRÃO, Silvio Romero. Direitos da personalidade. 2. ed. São Paulo: Atlas, 2014, p. 10.

[156] Lei nº 12.414, de 9 de junho de 2011.

[157] Tal definição pode ser encontrada na ementa da lei.

apenas com base em dívidas não pagas, mas, também, com base em outras informações que podem exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento[158]. Nesse sentido, o fluxo de dados pessoais no mercado financeiro aumentou exponencialmente.

Essa nova legislação acabou por estabelecer, de forma similar ao CDC, o princípio da qualidade dos dados pessoais[159], bem como os direitos de acesso[160], retificação e cancelamento dos dados[161].

Além disso, a lei nº 12.414/2011 consolidou a ideia de autodeterminação informacional – germinada na legislação consumerista – ao estabelecer mecanismos de controle do indivíduo sobre os seus dados pessoais, atribuindo a ele a faculdade de decidir se tem interesse ou não em formar esse novo banco de dados[162] e o poder de decidir o momento em que deseja cancelá-lo[163].

Por fim, vale dizer que a Lei do Cadastro Positivo também foi inovadora ao impor deveres aos gestores dos bancos de dados, como o de não coletar informações excessivas[164] e/ou sensíveis[165] para fins de análise de crédito, além de

---

[158] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 128.

[159] Art. 3º, § 1º: "Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado".

[160] Art. 5º, II: "acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado".

[161] Art. 5º, III: "solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação".

[162] Neste ponto, é importante destacar que a Lei do Cadastro Positivo sofreu alterações relevantes em abril de 2019, as quais entrarão em vigor em julho do mesmo ano. A redação do art. 4º, que antes fazia menção à necessidade de consentimento do titular dos dados para abertura de cadastro positivo em seu nome, passou a dispensar esse consentimento, como se vê na nova redação, estabelecida pela LC nº 166, de 8 de abril de 2019: "Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a: I - abrir cadastro em banco de dados com informações de adimplemento de pessoas naturais e jurídicas; II - fazer anotações no cadastro de que trata o inciso I do caput deste artigo; III - compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de dados; e IV - disponibilizar a consulentes: a) a nota ou pontuação de crédito elaborada com base nas informações de adimplemento armazenadas; e b) o histórico de crédito, mediante prévia autorização específica do cadastrado".

[163] Art. 5º, I: "obter o cancelamento ou a reabertura do cadastro, quando solicitado".

[164] Art. 3º, § 3º, I: "Ficam proibidas as anotações de: informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor".

[165] Art. 3º, § 3º, II: "Ficam proibidas as anotações de: informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

elencar como um direito do titular dos dados que suas informações sejam utilizadas apenas com finalidades creditícias[166].

3.1.4. Marco Civil da Internet

O Marco Civil da Internet[167] (MCI) foi o regramento responsável por instituir uma carta de direitos para a Internet no Brasil[168]. Este conjunto normativo buscou, notadamente por meio de princípios, assegurar os direitos e garantias do cidadão no ambiente virtual. Dentre os direitos considerados como os pilares dessa legislação[169], ao lado da neutralidade da rede e da liberdade de expressão, encontra-se a proteção da privacidade e dos dados pessoais[170].

Seguindo a tônica dos regramentos anteriores sobre o assunto, porém desta vez acentuando-a, o MCI elegeu o usuário como o grande protagonista no que se refere à proteção dos seus dados pessoais. Nesse sentido, nota-se que três dispositivos fazem menção expressa à necessidade do consentimento do usuário para a coleta, o uso, o armazenamento e o tratamento de seus dados, bem como para a sua transferência a terceiros[171]. Ainda, o MCI se dedica a qualificar este consentimento como devendo ser livre, expresso e informado[172][173].

Foram estabelecidos, mais uma vez, deveres aos controladores dos dados, os quais ficaram obrigados a prestar informações claras e completas aos usuários

---

[166] Art. 5º, VII: "ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados".
[167] Lei nº 12.965, de 23 de abril de 2014.
[168] Expressão utilizada por BOFF (2018, p. 96).
[169] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 130.
[170] Art. 3º, II e III: "A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II – proteção da privacidade; III – proteção dos dados pessoais, na forma da lei".
[171] Art. 7º, VII: "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei"; art. 7º, IX: "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais"; e art. 16, II: "Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: [...] II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular".
[172] Art. 7º, VI, VIII, IX e XI.
[173] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 132.

sobre o uso, armazenamento, tratamento e proteção de seus dados pessoais. Estes, inclusive, apenas poderão ser utilizados mediante consentimento expresso do seu titular, a ser ofertado em cláusula contratual destacada, e para finalidades especificadas previamente[174].

Por fim, o MCI estipula ainda que ao usuário é assegurado o direito de requerer a exclusão definitiva dos seus dados pessoais fornecidos a uma determinada aplicação de Internet, assim que encerrada a relação entre as partes[175].

A partir de uma análise de todos esses dispositivos, percebe-se que o raciocínio legislativo por trás do MCI foi o de empoderar o indivíduo para que ele possa autodeterminar as suas informações pessoais. A grande maioria das normas se volta ao usuário (o titular dos dados pessoais) para que ele, uma vez cientificado a respeito do fluxo dos seus dados, possa controlá-lo da formar que preferir, por meio do consentimento[176].

3.2. O consentimento e a Lei Geral de Proteção de Dados

A Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), é a mais nova legislação brasileira a abordar os temas da proteção de dados pessoais e da privacidade. De acordo com Patricia Peck Pinheiro, esse regulamento é responsável por "tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica[177]". Trata-se de uma regulamentação de natureza técnica e sobretudo principiológica, elencando direitos, obrigações e princípios relacionados à proteção de dados pessoais.

---

[174] Conforme art. 7º VI, VIII e IX.
[175] Conforme art. 7º, X.
[176] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 132.
[177] PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018, p. 15.

O objetivo da lei foi proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade do cidadão[178], visando a um equilíbrio entre o fomento do desenvolvimento econômico e a tutela desses direitos fundamentais[179].

Analisando a LGPD sob a perspectiva do consentimento, percebe-se que este é apenas uma – dentre dez – das justificativas para o tratamento de dados pessoais. Conforme a análise de Bioni: "Isso significa que, em termos de técnica legislativa, o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais [...][180]". Tal situação pode ser visualizada mediante a leitura do art. 7º da LGPD, que elenca as hipóteses em que o tratamento de dados poderá ser realizado[181].

Em contrapartida, também é possível dizer que o consentimento ainda é o elemento principal no que se refere ao tratamento de dados pessoais nesse regulamento. Isso porque a presença do termo "consentimento" é recorrente no texto da LGPD[182], o que demonstra uma forte preocupação a respeito da carga participativa do indivíduo no fluxo de suas informações pessoais[183].

---

[178] PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018, p. 16.

[179] De acordo com BIONI (2019, p. 108), as normas de proteção de dados pessoais sempre tiveram essa "dupla função" de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico.

[180] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, pp. 133-134.

[181] 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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; 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".

[182] Mais especificamente, o termo "consentimento" aparece 35 vezes no texto da LGPD.

[183] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, pp. 134.

Nesse sentido, a LGPD atribui uma série de adjetivos ao consentimento, seguindo a tradição do direito comunitário europeu[184]. De acordo com esta lei, o consentimento deve ser livre, informado, inequívoco e referente a uma finalidade determinada[185]. Em alguns casos, o consentimento também deve ser específico[186].

Além disso, a maioria dos princípios estabelecidos pelo art. 6º da LGPD gravita em torno da figura do indivíduo. Princípios como o da finalidade[187], do livre acesso[188], da qualidade dos dados[189] e da transparência[190] são, sobretudo, instrumentos alcançados pela lei ao titular dos dados para que ele possa, a partir de informações claras e completas sobre o tratamento de seus dados, autodeterminar as suas informações pessoais, inclusive corrigindo-as, caso necessário. No mesmo sentido, princípios como o da adequação[191] e da necessidade[192] estipulam que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular, ao passo que demandam que a finalidade especificada para o tratamento seja alcançada mediante o uso de dados pertinentes, proporcionais e não excessivos[193].

No mais, Bioni observa que se fazem presentes na LGPD diversas disposições que dão um regramento específico para "concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento[194]". De modo a corroborar tal afirmação, o autor refere que: (I) em

---

[184] Vide subcapítulo 2.4.

[185] Art. 5º, XII: "Para os fins desta Lei, considera-se: [...] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

[186] É o caso dos artigos 7º, § 5º; 14, § 1º; e 33, VIII.

[187] Art. 6º, I: "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".

[188] Art. 6º, 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".

[189] Art. 6º, 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".

[190] Art. 6º, 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".

[191] Art. 6º, II: "adequação: compatibilidade do tratamento com as finalidades informadas **ao titular**, de acordo com o contexto do tratamento".

[192] Art. 6º, 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".

[193] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 135.

[194] Ibidem, p. 135.

algumas situações previstas na lei o consentimento deverá constar de cláusula destacada das demais[195]; (II) as autorizações para tratamento de dados sem finalidade determinada serão nulas[196] e; (III) caso os dados sejam tratados sem o consentimento do titular, em virtude de alguma das hipóteses de dispensa, ainda deverão ser observados os princípios e garantias gerais da LGPD[197], inclusive sendo autorizado ao indivíduo se opor a esse tratamento caso tais princípios e garantias não sejam respeitados pelo controlador[198].

Nota-se, portanto, que o consentimento é um dos elementos mais importantes no âmbito da LGPD, na medida em que se apresenta como o principal instrumento de controle do indivíduo sobre os seus dados pessoais. Tal controle é essencial para que o cidadão possa autodeterminar as suas informações pessoais e, em última análise, desenvolver livremente a sua personalidade.

3.3. O que seria um consentimento válido para a LGPD?

Diante da evidente importância do consentimento no âmbito da LGPD, torna-se premente o debate a respeito do que seria um consentimento válido sob a ótica desta lei. Para isso, analisar-se-ão elementos tradicionais do direito civil, como a disciplina dos negócios jurídicos, bem como algumas questões mais modernas, trazidas à tona pelo texto da LGPD.

No direito privado brasileiro, a figura do consentimento está inserida – notadamente – no tema dos defeitos do negócio jurídico, mais especificamente no que toca aos vícios de consentimento, como o erro, o dolo, a coação, o estado de perigo e a lesão[199].

---

[195] Art. 8º, § 1º: "Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais".

[196] Art. 8º, § 4º: "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas".

[197] Art. 7º, § 6º: "A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular".

[198] Art. 18, § 2º: "O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei".

[199] Seções I a V do Capítulo IV do Livro III do Código Civil.

Como se sabe, a declaração de vontade é um dos elementos essenciais do negócio jurídico, sem a qual este não existiria. Tanto isso é verdade que se a vontade for inexistente, o negócio jurídico também o será[200]. No entanto, se houver a formação imperfeita desse elemento volitivo – isto é, se existir declaração de vontade por parte do agente, porém esta não encontrar correspondência com aquilo que ele quer exteriorizar – se está diante de um vício de consentimento, sendo anulável, portanto, o negócio jurídico decorrente[201].

Tendo em vista a menção expressa da LGPD à vedação do "tratamento de dados pessoais mediante vício de consentimento[202]", Bioni entende que deverá haver um diálogo entre a LGDP e o Código Civil para se interpretar a concepção de consentimento mencionada naquela sob a ótica dos defeitos do negócio jurídico[203].

Subsequentemente, no trajeto para a compreensão do que possa ser considerado um consentimento válido sob a perspectiva da LGPD, é de suma importância que se analise a adjetivação do consentimento feita por este regramento. Como já mencionado anteriormente, a nova lei brasileira de proteção de dados define consentimento da seguinte forma: "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[204]".

3.3.1. Livre

Como refere Bruno Bioni, o adjetivo livre nos remete à ideia de uma ação espontânea, que não é objeto de pressão, mas sim de livre-arbítrio. Uma decisão

---

[200] AZEVEDO, Antônio Junqueira de. Negócio jurídico: existência, validade e eficácia. 4. ed. São Paulo: Saraiva, 2002, p. 32-33. Neste ponto, o autor chama a atenção para que não se confundam os negócios jurídicos inexistentes (plano da existência) com os negócios jurídicos nulos ou anuláveis (plano da validade), pois estão situados em planos diferentes.

[201] Conforme o art. 171, II, do Código Civil: "Além dos casos expressamente declarados na lei, é anulável o negócio jurídico: [...] II - por vício resultante de erro, dolo, coação, estado de perigo, lesão ou fraude contra credores".

[202] Art. 8º, § 3º.

[203] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 190.

[204] Art. 5º, XII.

tomada livremente seria a realização de uma escolha em meio a tantas outras que poderiam ter sido feitas[205].

Segundo Rony Vainzof, um consentimento livre partiria da proposta de "conferir ao titular a oportunidade de dispor ou não de dados que não sejam fundamentais à prestação de um eventual serviço[206]". No mesmo sentido, o artigo 7º (4) do GDPR refere que ao se avaliar se o consentimento é dado livremente, deve-se verificar se a execução de um contrato ou prestação de um serviço está subordinada ao consentimento para o tratamento de dados pessoais que não sejam necessários para a execução desse contrato[207].

Em outras palavras, não se considera que o consentimento tenha sido dado livremente se o titular dos dados não dispuser de uma escolha verdadeira ou não puder recusar ou retirar o seu consentimento sem ser prejudicado[208]. De forma exemplificativa, cita-se um exemplo trazido pelo órgão consultivo *Article 29 Working Party*[209] (*Art. 29 WP*): um banco solicita aos clientes o consentimento para usar seus detalhes de pagamento para fins de marketing. Esse tratamento de dados não é necessário para a execução do contrato com o cliente e para o oferecimento de serviços bancários ordinários. Se a recusa do cliente em consentir com esse propósito levar à negação dos serviços bancários, ao encerramento da conta bancária ou ao aumento de taxas, haverá violação à liberdade de consentir[210].

---

[205] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 197.

[206] VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. São Paulo: Thomson Reuters Brasil, 2018, p. 72.

[207] Art. 7º (4), GDPR: "Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

[208] VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018, p. 72.

[209] O Article 29 Working Party foi um corpo consultivo europeu independente, responsável por lidar com questões ligadas à proteção de dados pessoais até o dia 25 de maio de 2018. Foi substituído pela European Data Protection Board, que recebeu poderes por meio do GDPR.

[210] Article 29 Working Party. Guidelines on Consent under Regulation 2016/679, p. 9. "A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given".

Além disso, é essencial que se analise o nível de assimetria de poder na relação entre o titular dos dados e o responsável pelo seu tratamento. Tomando como exemplo uma relação trabalhista, na qual há evidente assimetria de poder entre empregado e empregador, é altamente improvável que um empregado responda livremente, por exemplo, a um pedido de consentimento de seu empregador para a instalação de câmeras no ambiente de trabalho[211]. Isto é, o "poder de barganha[212]" do cidadão em relação ao tratamento de seus dados pessoais, a partir de uma análise casuística, é o que definirá se o consentimento pode ser adjetivado como livre ou não.

Vale destacar, por fim, que a LGPD considera que, quando o tratamento de dados pessoais for condição para o acesso a algum tipo de produto ou serviço, o titular dos dados deve ser informado sobre isso de forma destacada, além de ser cientificado sobre os meios pelos quais ele pode exercer os seus direitos[213], como a revogação do consentimento[214].

3.3.2. Informado

O requisito estabelecido pela LGPD de que o consentimento deve ser "informado" busca garantir ao cidadão que ele obtenha informações adequadas antes de tomar alguma decisão a respeito de seus dados. Como refere Bioni: "O fluxo dos seus dados precisa tomar forma (ser informado), sendo *pressuposto* para que haja qualquer tipo de processo de tomada de decisão por parte do titular dos dados[215]".

Como bem define o *Art. 29 WP*, o provimento de informações aos titulares dos dados de maneira prévia à obtenção de seu consentimento é essencial para que estes tomem decisões informadas, entendam com o que eles estão consentindo e

---

[211] Article 29 Working Party. Guidelines on Consent under Regulation 2016/679, p. 7.
[212] Expressão utilizada por BIONI (2019, p. 197).
[213] Art. 9º, § 3º: "§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei".
[214] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 198.
[215] Ibidem, p. 191.

compreendam quais são os seus direitos. Se o controlador dos dados não prover ao titular informações acessíveis e de fácil compreensão, a autodeterminação informacional torna-se uma ilusão e o consentimento perde a sua legitimidade como base legal para o processamento de dados[216].

Por esse ângulo, a LGPD estabelece uma forte relação entre o conceito de informação e o princípio da transparência[217], na medida em que define este 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[218]". Ademais, a lei prevê como nulo o consentimento concedido diante de informações de conteúdo enganoso ou abusivo, ou que não tenham sido apresentadas previamente com transparência[219].

Vale dizer, por outro lado, que a prestação de uma informação só se justifica se trouxer maior clareza e transparência ao fluxo de dados pessoais. Isso porque, diante da quantidade e complexidade de informações existentes na maioria das relações de tratamento de dados, o excesso de informações pode vir a desinformar o indivíduo. A informação, portanto, deve ser prestada em uma quantidade suficiente para que o cidadão possa compreender com o que ele está consentindo e quais seriam as consequências caso ele não fornecesse seu consentimento[220].

Nesse sentido, a LGPD refere que as informações disponibilizadas ao titular devem ser claras, adequadas e ostensivas[221], bem como define, de forma exemplificativa, quais devem ser essas informações. Entre elas, destaca-se a

---

[216] Article 29 Working Party. Guidelines on Consent under Regulation 2016/679, pp. 12-13. "Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing".

[217] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 196.

[218] Art. 6º, VI.

[219] Art. 9º, § 1º: "Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca".

[220] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 192-196.

[221] Art. 9º, caput: "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso".

finalidade específica do tratamento, a identificação do controlador e os direitos do titular[222].

O fornecimento de informações claras, adequadas e suficientes, portanto, é o elemento que capacita o cidadão para que ele possa exercer o controle sobre seus dados pessoais.

3.3.3. Inequívoco e para uma finalidade determinada

A ideia de que o consentimento seja dado para uma finalidade determinada é essencial à própria lógica da LGPD. Como refere Bioni, "qualquer declaração de vontade dever ter um direcionamento, já que não se consente no vazio e de forma genérica. Seria o equivalente a emitir um cheque em branco que esvaziaria qualquer esfera de controle do cidadão sobre seus dados[223]". Pode-se dizer, em outros termos, que a especificação do motivo pelo qual se fará o uso de determinados dados pessoais é elemento indispensável à validade do consentimento emitido pelo usuário (este que é, justamente, o fundamento legal para o tratamento desses dados).

De forma a corroborar essa visão, a lei brasileira de proteção de dados estabeleceu o princípio da finalidade, o qual determina que toda atividade de tratamento de dados deve possuir um propósito legítimo, específico, explícito e informado ao titular[224].

A definição de um propósito, além disso, permite que se verifique se o titular foi previamente bem informado para iniciar um processo de tomada de decisão

---

[222] Art. 9º: "I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei".

[223] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 198.

[224] Art. 6º, 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".

livre[225]. Afinal, o cidadão deve estar ciente a respeito de quem irá processar os seus dados e com o que ele está consentindo para, só então, conseguir visualizar a finalidade do tratamento de seus dados.

Essa manifestação de vontade livre, informada e com uma finalidade determinada deve ser acrescida de uma declaração de vontade inequívoca por parte do titular dos dados, tendo em vista que o consentimento requer uma ação afirmativa que não deixe dúvidas sobre a intenção do indivíduo. Isto é, deve ser óbvio que o titular consentiu com o tratamento de seus dados.

Assim, visando definir o que seria um consentimento inequívoco, o *Art. 29 WP* refere que uma ação afirmativa clara é aquela em que o indivíduo toma uma ação deliberada para consentir com determinado processamento de seus dados. Sob essa lógica, caixas pré-selecionadas, por exemplo, não implicariam em um consentimento inequívoco, ao passo que isso se enquadraria como uma omissão por parte do indivíduo e não uma ação afirmativa[226].

Embora não haja definição expressa na LGDP sobre o que configuraria uma declaração de vontade inequívoca, Bioni entende que o *design* do ambiente virtual (ou físico), apresentado pelo controlador ao titular dos dados, deve proporcionar uma ampla margem de controle a este, em vez de manipular as suas escolhas. Trata-se de algo diretamente relacionado ao princípio da boa-fé[227].

Um consentimento válido no âmbito da LGPD, portanto, é aquele fornecido por um titular amplamente informado, de modo livre, visando a uma finalidade determinada, por meio de uma ação deliberada e inequívoca.

Destaca-se, por fim, que essa extensa adjetivação do consentimento demonstra a preocupação da LGDP em estabelecer parâmetros que definam a carga participativa do indivíduo no fluxo de seus dados pessoais. A lei claramente buscou inserir o indivíduo ao máximo na dinâmica da proteção de dados pessoais, a partir da ideia de que ele deveria acompanhar as suas informações de perto durante todo o processo de tratamento.

---

[225] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 198.
[226] Article 29 Working Party. Guidelines on Consent under Regulation 2016/679, pp. 15-18.
[227] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 200.

CONCLUSÃO

A disciplina de proteção de dados pessoais percorreu um longo caminho. Desde os primeiros passos dados pelo direito à privacidade, num contexto de fotografias instantâneas e tabloides, até os dias de hoje, nos quais a informação e a tecnologia permeiam praticamente todos os aspectos das nossas vidas, esse tema vem evoluindo de forma gradual e constante.

Como demonstrado, o titular dos dados pessoais passou a ser tratado como protagonista a partir da segunda geração de leis de proteção de dados[228]. Naquele momento, optou-se por uma estratégia regulatória que depositava nele a responsabilidade de proteger as suas próprias informações pessoais. Essa estratégia foi concebida a partir da ideia de que o indivíduo deveria poder controlar os seus próprios dados pessoais, de forma que se recorreu a um instituto jurídico mediante o qual a vontade do indivíduo pudesse ser manifestada: o consentimento.

Desde então, o consentimento tornou-se a principal ferramenta utilizada pelas leis de proteção de dados como meio de legitimar (ou deslegitimar) o tratamento de dados pessoais. Nesse sentido, as *privacy guidelines* da OCDE[229] delinearam um modelo legislativo cujo centro gravitacional girava em torno de princípios e direitos que visavam a fortalecer essa diretriz normativa de que o indivíduo deveria autodeterminar as suas informações pessoais[230].

Embora a importância do consentimento no âmbito da proteção de dados tenha passado por movimentos refratários – com o surgimento, por exemplo, de autoridades independentes para a implementação e aplicação das leis sobre a matéria e com o surgimento de leis que retiraram da esfera de controle do indivíduo a escolha sobre o tratamento de certos tipos de dados, como os sensíveis – tal instituto jurídico permaneceu sendo o elemento central de toda e qualquer legislação sobre o assunto[231]. Isso pode ser verificado, por exemplo, na extensa adjetivação sofrida pelo consentimento, tanto no contexto europeu, com a Diretiva Europeia

[228] Vide subcapítulo 1.3.
[229] Vide subcapítulo 2.3.
[230] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, pp. 136-137.
[231] Ibidem, p. 137.

sobre proteção de dados de 1995 ou mais recentemente com o GDPR[232], quanto no contexto brasileiro, com o Marco Civil da Internet[233] e a Lei Geral de Proteção de Dados[234]. O consentimento, compreendido como devendo ser livre, informado, inequívoco e referente a uma finalidade determinada, confirma esse prestígio atribuído à vontade do indivíduo.

Assim, verifica-se que o papel do consentimento no âmbito da proteção de dados pessoais passou por várias transformações desde a sua introdução ao assunto, na década de 1980. De um instituto jurídico visto como a solução para todas as questões envolvendo proteção de dados, assumindo um caráter quase que canônico, passou a ser questionado por sua fragilidade ao enfrentar questões práticas, o que acabou por mitigar sua influência. Foi, então, submetido a um processo de reestruturação, recebendo qualificadores que o trouxeram novamente à linha de frente do debate. O consentimento, portanto, percorreu um caminho pelo qual ele surgiu, foi questionado e se reafirmou como sendo o elemento principal da disciplina.

No mais, é inegável que as atuais normas de proteção de dados pessoais, baseadas fundamentalmente no instituto jurídico do consentimento, apresentam problemas relacionados à sua efetividade diante de situações concretas. A ubiquidade da tecnologia e a propagação em massa de informações pessoais tornaram-se questões inseparáveis da vida cotidiana, apresentado novos desafios a essas leis, as quais, por sua vez, devem apresentar uma resposta à altura. Afinal, como pôde ser observado durante toda a construção teórica deste trabalho, um dos componentes mais importantes da disciplina de proteção de dados pessoais é a constante busca pela evolução, de modo a não ficar obsoleta diante das permanentes mudanças provocadas pelo homem e pela tecnologia.

[232] Vide subcapítulo 2.4.
[233] Vide subcapítulo 3.1.4.
[234] Vide subcapítulo 3.2.

REFERÊNCIAS

ARTICLE 29 WORKING PARTY. *Guidelines on Consent under Regulation 2016/679*. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Data de acesso: 10/05/2019.

AZEVEDO, Antônio Junqueira de. *Negócio jurídico: existência, validade e eficácia*. 4. ed. São Paulo: Saraiva, 2002.

BARRAL, Welber Oliveira. *Metodologia da Pesquisa Jurídica*. Florianópolis: Fundação Boiteux, 2003.

BELTRÃO, Silvio Romero. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2014.

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

BOFF, S.O.; FORTES, V.B.; FREITAS, C.O.A. *Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação*. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988.* Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Data de acesso: 03/04/2019.

_____. Lei nº 8.078, de 11 de setembro de 1990. *Código de Defesa do Consumidor*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Data de acesso: 01/06/2019.

_____. Lei nº 9.507, de 12 de novembro de 1997. *Lei do Habeas Data*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>. Data de acesso: 31/05/2019.

_____. Lei nº 10.406, de 10 de janeiro de 2002. *Código Civil*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Data de acesso: 31/05/2019.

_____. Lei nº 12.414, de 9 de junho de 2011. *Lei do Cadastro Positivo*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Data de acesso: 02/06/2019.

_____. Lei nº 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Data de acesso: 03/06/2019.

_____. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Data de acesso: 15/04/2019.

CATE, Fred H. The failure of Fair Information Practice Principles. In: WINN, Jane K. (ed.). *Consumer Protection in the Age of the 'Information Economy'*. Hampshire: Ashgate Publish, 2006.

CONSELHO DA EUROPA. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Estrasburgo, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Data de acesso: 23/05/2019.

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

_____. *A proteção de dados pessoais como um direito fundamental*. Espaço Jurídico Journal of Law. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

EUROPEAN DATA PROTECTION BOARD. *Article 29 Working Party*. Disponível em: <https://edpb.europa.eu/our-work-tools/article-29-working-party_en>. Data de acesso: 10/05/2019.

_____. *Europe's new data protection rules and the EDPB: giving individuals greater control*. Disponível em: <https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en>. Data de acesso: 10/05/2019.

FERRAZ JÚNIOR, T. S. (1993). *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista Da Faculdade De Direito, Universidade De São Paulo, 88, 439-459. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Data de acesso: 14/04/2019.

GALLAGHER, Susan E. *Introduction to "The Right to Privacy" by Louis D. Brandeis and Samuel Warren: A Digital Critical Edition*. University of Massachusetts Press. Disponível em: <http://faculty.uml.edu/sgallagher/harvard__law_review.htm>. Data de acesso: 05/05/2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice, coord. *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. São Paulo: Thomson Reuters Brasil, 2018.

MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Federal Alemão*. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Konrad-Adenauer-Stiftung E.V., 2005.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy: the new landscape*. Cambridge: The MIT Press, 2001, pp. 219-242.

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

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito

alemão. In: MENDES, G.F.; SARLET, I.W.; COELHO, A.Z.P., coord. *Direito, inovação e tecnologia*. São Paulo: Saraiva, 2015, pp. 205-230.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publications Service, 2001.

_____. *OECD Privacy Guidelines*. Disponível em: <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>. Data de acesso: 17/05/2019.

_____. *The OECD Privacy Framework*, 2013. Disponível em: <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Data de acesso: 17/05/2019.

ORWELL, George. *1984*. Trad. Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)*. São Paulo: Saraiva Educação, 2018.

SILVA, Daniel Pereira Militão da. *Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação*. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo. São Paulo, 2009.

SOLOVE, Daniel J. *Introduction: privacy self-management and the consent dilemma*. Cambridge: Harvard Law Review, v. 126, 2013.

UNIÃO EUROPEIA. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Data de acesso: 05/05/2019.

_____. *Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas)*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2002.201.01.0037.01.POR>. Data de acesso: 06/05/2019.

_____. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Data de acesso: 09/05/2019.

WARREN, Samuel; BRANDEIS, Louis. *The right to privacy*. Cambridge: Harvard Law Review, v. 4, n. 5, 1890.

OUTRAS FONTES EM MEIOS ELETRÔNICOS

BENTO, Beatrice Helena Silveira Bento. *A nova lei de proteção de dados no Brasil e o general data protection regulation da União Europeia*. Artigo publicado no site Migalhas, em 23 de outubro de 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI289555,11049-A+nova+lei+de+protecao+de+dados+no+Brasil+e+o+general+data+protection>. Data de acesso: 12/04/2019.

BIONI, Bruno Ricardo. *Proteção de dados, Fluxo Transnacional, GDPR e novos padrões*. 2018. Palestra realizada no III Seminário de Governança das Redes – Políticas, Internet e Sociedade, promovido pelo Programa de Pós-Graduação em Direito da UFMG, em parceria com o Instituto de Referência em Internet e Sociedade – IRIS, nos dias 24 e 25 de setembro de 2018. Disponível em: <https://www.youtube.com/watch?v=jzCM2ya2ho4>. Data de acesso: 10/04/2019.

PINHEIRO, Patrícia Peck. *Como o Direito Digital está transformando a atuação dos advogados*. 2017. Palestra realizada no Aurum Summit 2017. Disponível em: <https://www.youtube.com/watch?v=ZeGShfvThYw>. Data de acesso: 28/03/2019.

SOUZA, Carlos Affonso; FORMICA, Piero; BLUM, Renato Opice. *Especialistas abordam aspectos e desafios da Lei Geral de Proteção de Dados*. Artigo publicado no site Migalhas, em 25 de março de 2019. Disponível em: <https://www.migalhas.com.br/Quentes/17,MI298789,31047-Especialistas+abordam+aspectos+e+desafios+da+Lei+Geral+de+Protecao+de>. Data de acesso:12/04/2019.

US-LEGAL.COM. *No-Fault Compensation Law and Legal Definition*. Disponível em: <https://definitions.uslegal.com/n/no-fault-compensation/>. Data de acesso: 15/05/2019.