REVISTA DE DIREITO | VIÇOSA | ISSN 2527-0389 | V.12 N.02 2020
DOI: doi.org/10.32361/2020120210597

DA EVOLUÇÃO DAS LEGISLAÇÕES SOBRE PROTEÇÃO DE DADOS: A NECESSIDADE DE REAVALIAÇÃO DO PAPEL DO CONSENTIMENTO COMO GARANTIDOR DA AUTODETERMINAÇÃO INFORMATIVA | EVOLUTION OF DATA PROTECTION LEGISLATION: THE NEED TO REASSESS THE ROLE OF CONSENT AS A GUARANTOR OF INFORMATIONAL SELF-DETERMINATION

LYS NUNES LUGATI
JULIANA EVANGELISTA DE ALMEIDA

RESUMO | A Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018) emerge em um contexto de disseminação massiva de dados na internet, com a chamada "datificação das coisas". Em uma eterna vigilância, o titular de dados vê diversos de seus direitos fundamentais violados. Isso faz com que haja a necessidade de legislações de proteção de dados que consagrem a participação do titular no processamento de dados. A LGPD conferiu importância visível ao requisito do consentimento e trouxe a ideia de que o consentimento do titular seria um passo rumo ao princípio da autodeterminação informativa. Todavia, é possível que o consentimento por si só assegure a autodeterminação informativa? Qual é a definição desse princípio e em que medida a LGPD o assegura? Para essa análise, será feita uma pesquisa jurídico dogmática, baseando-se em legislações de proteção de dados, comparações com legislações de outros países, estudos de doutrinas e materiais produzidos sobre o tema.

PALAVRAS-CHAVE | *Internet. Tratamento de dados. Lei Geral de Proteção de Dados.*

ABSTRACT | *The General Data Protection Law – LGPD (Law 13.709 /2018) emerges in a context of massive dissemination of data on the internet, with the so-called "datafication of things". In this eternal vigilance, the data holder sees several of his fundamental rights violated. This means that there is a need for data protection laws that establish the data holder's participation in data processing. The LGPD gave visible importance to the requirement for consent and brought the idea that the consent of the holder would be a step towards the principle of informative self-determination. However, is it possible that consent alone ensures informational self-determination? What is the definition of this principle and to what extent does the LGPD ensure it? For this analysis, a dogmatic legal research will be carried out, based on data protection laws, comparisons with laws of other countries, studies of doctrines and material produced about the theme.*

KEYWORDS | *Internet. Data processing. The General Data Protection Law.*

1. INTRODUÇÃO

Dentro do contexto do *Big Data,* a sociedade passa pela datificação das coisas. Isso implica dizer que a cada dia mais dados transitam pela internet em velocidades e números exponenciais. Como Bioni (2020) defende, visualiza-se uma vigilância descentralizada, com múltiplos atores envolvidos no processamento de dados, sem a separação da vida *on-line* e *off-line*. Nessa perspectiva é que crescem as violações a diversos direitos fundamentais do titular de dados que vê a sua privacidade sendo constantemente violada, como foi possível perceber, por exemplo, com o caso recente da empresa norte-americana Cambridge Analytica (ENTENDA.., 2020).

Todo esse contexto de acentuado uso de tecnologias fez emergir a necessidade de legislações de proteção de dados que realmente abordassem o direito à proteção de dados e colocassem o titular como participante do processamento de dados, tendo em vista que se encontra em uma posição (hiper)vulnerável, conforme Bioni (2020) mesmo defende, e que precisa estar ciente do que acontece com seus dados, consentindo com isso.

O assunto de proteção de dados já era indiretamente tratado em legislações esparsas como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Contudo, não existia regulamentação que abordasse especificamente a problemática da proteção de dados, o que colocou em destaque a importância de se ter uma legislação específica sobre isso.

Nessa linha do tempo, outros países também implementavam suas leis. Assim, a União Europeia, que já tinha históricos de legislações como a Convenção 108 e a Diretiva 95/46, implementou uma legislação de proteção de dados extensiva e que regulamentou o tratamento de dados pelos seus signatários, qual seja, a *General Data Protection Regulation* (GDPR). A criação dessa legislação serviu como catalisador para outros países e dessa forma, o Brasil cria, em 2018, a Lei Geral de Proteção de Dados (LGPD).

A LGPD vinha sendo desenvolvida desde 2010 e insere o Brasil entre

os países que têm legislações completas sobre proteção de dados. Seu texto, seguindo a linha das legislações de dados mais atuais, como a *GDPR,* denota a importância dada ao consentimento, tendo em vista que o instituto é apresentado diversas vezes ao longo do texto, além de ser agora adjetivado como “livre”, “informado” e “inequívoco” e servir como orientação para várias outras normas apresentadas pela legislação.

Não obstante, também é fundamental observar que a LGPD destaca o princípio da autodeterminação informativa que busca colocar o titular dos dados no controle e proteção de seus próprios dados. Com a necessidade do consentimento do usuário e consequentemente sua maior participação no tratamento de dados, é válido dizer que a LGPD se demonstra preocupada em garantir esse princípio.

Contudo, considerando o contexto atual: progresso tecnológico, com ampla circulação de dados e ampla gama de atores envolvidos o que dificulta o controle do conhecimento de informações sobre o tratamento de dados, é possível dizer que o consentimento seja obtido conforme as adjetivações que a Lei propõe? Além disso, é válido dizer que o consentimento é meio hábil a garantir a autodeterminação informativa?

Por isso, este artigo, através de uma pesquisa jurídico-dogmática, fará a análise de outras legislações de proteção de dados a fim de comparar o trajeto percorrido pelas legislações de proteção de dados até a promulgação da LGPD e se utilizará de revisão de literatura sobre o tema, que ainda carece de aprofundamento.

2. O TRAJETO DA PROTEÇÃO DE DADOS PESSOAIS ATÉ O IMPLEMENTO DA LGPD

A discussão sobre o que hoje se conceituaria como privacidade originou-se a partir do momento em que as tecnologias se tornaram invasivas, dando margem à divulgação de informações da esfera privada do indivíduo. Segundo Mendes (2014), um dos marcos para essa discussão foi o artigo “the right of privacy”, escrito por Warren e Brandeis. Para Cancelier (2017), a

concepção de privacidade, até aqui, era a assumida pelo jurista Thomas McIntyre que cunhou em 1888 a expressão "*right to be let alone*" (o direito a estar só).

O que se pode perceber é que o direito à privacidade tinha um cunho fortemente individualista e era visto como um direito negativo. Por isso, pode-se dizer que o direito à privacidade estaria sendo garantido desde que o Estado se abstivesse de adentrar na esfera individual de cada um. Essa perspectiva era condizente com a primeira geração de direitos fundamentais em que se inseria, vinculada diretamente com o direito à liberdade.

Essa conceituação começa a assumir novos delineados no fim do século XX, aproximadamente em 1960, com o avanço das tecnologias e frente a uma "capacidade técnica cada vez maior de recolher, processar e utilizar a informação." (DONEDA, 2006, p. 12). Junto a isso, cresce a democratização do interesse pela tutela de sua privacidade e de seu exercício.

Desde que o tratamento informatizado de dados surgiu e ganhou enfoque, houve a necessidade de que o conceito de direito à privacidade se modificasse a fim de abranger a proteção de dados pessoais. Segundo Mendes (2014), aproximadamente em 1970, são vistas decisões jurídicas e legislações que afirmam que os dados pessoais são uma projeção da personalidade do indivíduo e por isso são hábeis a receber tutela jurídica.

Adiante, as regulamentações sobre proteção de dados passam por diversas fases até chegar ao momento atual quando o direito à proteção de dados adquire o enfoque como um direito fundamental e passa a ter legislações específicas e completas como a LGPD e a *GDPR*.

As doutrinas defendem a visão de Viktor Mayer-Scönberger, que propõe que a regulamentação da proteção de dados pessoais percorreu quatro gerações distintas, que, de acordo com Doneda (2011, p. 96), são "leis que partem de um cerne mais técnico e restrito para, por fim, ampliar as disposições e as técnicas referentes às tecnologias modernas".

A primeira geração de leis se insere no contexto do Estado Moderno, onde o Estado se utilizava de grandes bancos de dados, pois o controle da

população se dava por meio de obtenções massivas de informações sobre os indivíduos. Dessa forma, segundo Doneda (2011, p. 96):

> O núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos. Essas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) dessas normas.

Nessa perspectiva, o Estado foi então centralizado como o destinatário desses regulamentos, que se direcionavam diretamente à própria tecnologia. Um exemplo das leis de primeira geração é o *Privacy Act,* norte-americano de 1974. A primeira geração se estende até o implemento da *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977. Várias leis acerca de proteção de dados foram implementadas na Alemanha nessa época e conforme explica Gasiola (2019):

> [...] são reações a projetos estatais para implementar bancos de dados centralizados sobre a população, em meio à euforia tecnológica que marcou o pós-guerra. O choque entre a recente lembrança (ou presença) dos governos autoritários e a iminência de tais projetos levou ao reconhecimento expresso da proteção de dados perante as pretensões públicas de aumentar seu poder informacional. O objetivo dessas leis era, acima de tudo, estabelecer limites e garantir a transparência na criação de bancos de dados.

Essa geração de leis baseada somente em autorizações tornou obsoleta, pois, frente ao avanço da tecnologia, o tratamento de dados passa a ser feito além do domínio governamental, sendo feito também por entes privados. Portanto, esse cenário ensejou a segunda geração de leis, em que, segundo Bioni (2020), o usuário, mediante o seu consentimento tem o poder de participar do processo de tratamento de dados, em fases como a coleta, uso e compartilhamento de seus dados pessoais.

A terceira geração de leis se preocupa mais com a tutela do direito à privacidade, indo além da liberdade de ceder ou não os dados, mas sim em garantir a efetividade deste direito. Nessa perspectiva, afirma Bioni (2020) que

se amplia a participação do indivíduo agora para todas as fases. Os regulamentos crescem até atingir o conceito central de “autodeterminação informativa”. Nas palavras de Doneda (2011, p. 97):

> A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes proporcionando o efetivo exercício da autodeterminação informativa.

Contudo, essa geração só abarcou uma parcela de indivíduos e isso fez com que a terceira geração se tornasse insuficiente, caminhando assim para a quarta geração, que prevalece até hoje.

Como forma de superar tais desvantagens do enfoque individual conferido pelas outras gerações, surge a quarta geração, vivenciada até os dias atuais, com leis que priorizam os titulares dos dados frente a terceiros que possam manipular suas informações pessoais. Nas palavras de Doneda (2011, p. 98):

> Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.

Consoante Bioni (2020), o consentimento continua sendo o traço marcante dos regulamentos, mas começa a sofrer limites e condições de forma a se adequar à autonomia do titular nesse contexto. Passa a ser, então, tomado como um consentimento “livre, informado, inequívoco, explícito e/ou específico”. Isso posto, pela grande importância dada ao consentimento nesses regulamentos, os próximos tópicos percorrerão a evolução do termo na União Europeia para, enfim, adentrar o assunto na legislação brasileira.

2.1 União Europeia

Conforme indica Krieger (2019), apesar de já existirem alguns regulamentos anteriores, é em 1980 que de fato a União Europeia se atenta ao assunto pelo qual passa a ter uma preocupação maior.

É regulamentada a Convenção 108, pelo Conselho Europeu, que por sua vez já inicialmente estabelece a relação entre dados pessoais e o livre fluxo informacional transfronteiriço (KRIEGER, 2019). Essa Convenção é grande influenciadora da Diretiva Europeia de Dados Pessoais (95/96 EC). Através dessa diretiva é estruturado o modelo europeu, que, conforme indica Doneda (2006), trata-se de “uma disciplina ampla e detalhada que é transposta para a legislação interna de cada estado-membro”. Serve, então, como uma uniformização legislativa.

A diretiva tem como uma de suas inovações a introdução de deveres àqueles que realizam o tratamento de dados (*data controllers),* além de trazer princípios regentes que devem permear a coleta, tratamento e utilização de dados. Além disso, definir práticas relacionadas com a tecnologia.

No artigo 2º, alínea h, pode-se ainda observar a conceituação do consentimento, sendo trazido 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 de tratamento”. Ademais, na alínea a do artigo 7º, vê-se que o consentimento é colocado como fundamental no tratamento de dados, excluídos os casos de dispensa, o que se assemelha inclusive com a disposição feita pela LGPD.

De acordo com Bioni (2020), a inovação trazida por essa regulamentação é hábil a enquadrá-la, inclusive, agora na quarta geração de leis de proteção de dados, pois vê-se que foco da Diretiva gira em torno do titular dos dados e dos *data controllers*.

Em relação às diretivas, cada país possui um determinado prazo para que faça a adaptação, o que ganha o nome de “transposição” e que pode incorrer à resposta pela mora do país diante da Corte Europeia de Justiça

(Doneda, 2006, p. 224).

Assim, em 27 de abril de 2016, é aprovado o novo Regulamento (EU) 2016/679, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation),* conhecido como GDPR, que revogou a Diretiva 95/46/CE, mas manteve seus princípios, conforme indica Malheiros (2017).

O consentimento aparece diversas vezes na lei, com adjetivações como “livre”, “específico”, “informado” e “inequívoco”. Apesar de o artigo 6º demonstrar outras hipóteses em que o consentimento é dispensado, vê-se que o consentimento ganha destaque através dessa regulamentação. Suas adjetivações aparecem no item 32 das considerações, assim como no item 11 de seu artigo 4º.

> (32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. [...] O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.
>
> Art. 4º
>
> (11) «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.

Conforme é possível visualizar pelos artigos que dispõem sobre o consentimento na GDPR, indica Bioni (2020) que o consentimento nesta lei parte de uma ação afirmativa ou declaração, que coloca a manifestação de vontade do titular com destaque.

Em seu item 42, o Regulamento indica a importância do consentimento informado, demonstrando a importância do conhecimento das finalidades do tratamento de dados pelo seu titular, consagrando o princípio da

autodeterminação informativa e a participação deste titular em todo o processo de tratamento de seus dados.

Isso também pode ser percebido através de outros artigos ao decorrer do Regulamento, como o item 60, que dispõe sobre a necessidade de que o titular seja informado dos perfis e riscos gerados por isso, além de quais seriam as consequências de não fornecer seu consentimento. Ademais, o item 61 indica a necessidade de que os responsáveis pelo tratamento de dados demonstrem que os dados serão utilizados para outros fins. Vejamos:

> (60) Os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deverá ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível uma útil perspetiva geral do tratamento previsto. Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.

> (61) As informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser a este fornecidas no momento da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias. Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deverá ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário. Sempre que o responsável pelo tratamento tiver a intenção de tratar os dados pessoais para outro fim que não aquele para o qual tenham sido recolhidos, antes desse tratamento o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias. Quando não for possível informar o titular dos dados da origem dos dados pessoais por se ter recorrido a várias fontes, deverão ser-lhe fornecidas informações genéricas.

Resta demonstrado no item 60, que as perspectivas do titular de dados devem ser levadas em consideração no momento da análise do tratamento de dados. Com isso, vê-se que, conforme indica Bioni (2020), além de o consentimento continuar sendo o cerne da GDPR, ele aparece como um dos

"fios condutores da recente reforma".

2.2 Brasil

Na perspectiva de Krieger (2019), ainda que apenas de maneira tácita, a proteção de dados começa a ser tratada, no Brasil, na Constituição Federal de 1988 (CF/88), como proteção ao direito de personalidade, à liberdade de expressão (art. 5º, IX) e pelo direito à informação (art. 5, XIV).

Ainda, é garantida a inviolabilidade da vida privada e intimidade (art. 5º, X), o habeas data (art. 5º, LXXII) e a interceptação das comunicações telefônicas, telegráficas ou de dados (art. 5º, LXXII).

Em linha cronológica, outras normas passam a dispor sobre proteção de dados, tal como o Código de Defesa do Consumidor, em 1990. O seu artigo 43 expõe a proteção dada ao titular dos dados frente a bancos de dados e cadastros. Há a exigência de cadastros e dados claros, objetivos e verdadeiros, com linguagem facilmente compreendida. Além disso, exige-se que o consumidor seja comunicado sobre a abertura de cadastros, ficha, registro e dados pessoais e de consumo.

Nas palavras de Doneda (2011) o legislador brasileiro teria se orientado no *Fair Information Principles*, e grande parte da doutrina elege a lei como um "marco normativo dos princípios de proteção de dados pessoais" no Brasil.

Contudo, conforme indicam Andrade e Moura (2019), a legislação consumerista ainda estava mais preocupada em regular os bancos de dados do que realmente se importarem com a necessidade do consentimento. Nas palavras dos autores:

> O presente artigo, entretanto, analisa a regra do CDC de forma mais crítica, pois se preocupa mais com a regulamentação dos Bancos de Dados do que com o consentimento prévio ao registro ou arquivamento dos mesmos (sic), estando mais próxima das normas de primeira geração do que as de terceira. Ademais, a suposta autodeterminação informacional do consumidor resta ainda mais fragilizada a partir da Súmula no 404, do STJ, que adverte: "É

> dispensável o aviso de recebimento (AR) na carta de comunicação ao consumidor sobre a negativação de seu nome em bancos de dados e cadastros.

Conforme também Bioni (2020) expõe, trata-se de uma legislação que busca abranger a todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor.

Surge no ano de 2011 a lei 12.414/2011, "Lei do Cadastro Positivo", estabelecendo regulamentação sobre os dados derivados de operações financeiras e adimplementos dos consumidores, que facilitam a concessão de crédito. (KRIEGER, 2019). Na perspectiva de Mendes (2014), é uma lei que consolida a evolução do conceito de autodeterminação informativa no ordenamento, na medida em que coloca o consentimento como necessário para o compartilhamento de dados ser lícito.

Também se pode perceber que, tal como indica Bioni (2020), a situação econômica do postulante de crédito não é vista só com informações negativas (como o não adimplemento de dívidas) mas também é conferido um olhar a outras informações que possam exprimir dados positivos de seu histórico de adimplemento.

Fundamental observar também que a Lei do Cadastro Positivo exige o consentimento do titular para que de fato ocorra o tratamento de dados, o que por sua vez não era visualizado no CDC, tendo em vista que havia apenas a exigência de uma mera notificação ao consumidor. Krieger (2019) defende que há a introdução do sistema *opt-in* no ordenamento jurídico brasileiro.

Aqui cabe a observação da implementação da Lei Complementar nº 166/2019, que regride ao sistema *opt-out*[1], tendo em vista a inclusão de consumidores no banco de dados de forma automática, como afirma Bioni (2020).

Seguindo a linha cronológica da legislação brasileira sobre dados, convém conferir especial destaque ao Marco Civil da Internet. Essa

1 De acordo com Davanzo (2015), "o sistema opt-out de envio é aquele onde o consumidor é inserido numa lista de "alvos" da empresa, recebe a publicidade eletronicamente e tem a possibilidade de ser excluído desse mailing list se assim requerer".

regulamentação ganhou proeminência e teve seu trâmite legislativo acelerado após um episódio escandaloso de espionagem revelado por um ex-analista, Edward Snowden, dentro da Agência Nacional de Segurança dos Estados Unidos. Foi demonstrado, inclusive, que houve repercussão dessa espionagem no âmbito brasileiro. Isso motivou o discurso da presidente Dilma em adotar o regimento de urgência da lei (APÓS ESPIONAGEM..., 2020), culminando na aprovação do Marco num evento de governança multisetorial da internet (NetMundial). (ARAGÃO, 2020).

Na explicação de Bioni (2020), o Marco Civil da Internet se constitui como uma reação à tentativa de regular o uso da internet por meio de leis penais, já que uma técnica prescritiva e restritiva para regular o uso da internet poderia resultar em um retardo da inovação tecnológica no país. Por isso, essa legislação se afasta dessa técnica e busca regular o uso da internet, conferindo direitos e garantias do cidadão nas relações travadas no meio virtual, de uma forma principiológica.

Nesta lei, já há menção expressa ao consentimento e sua adjetivação, tendo em vista que, principalmente após o escândalo, buscou-se conferir proteção especial ao titular dos dados, dando a ele participação no processo de tratamento de dados. Todavia, conforme explica Malheiros (2017), ainda não havia uma legislação que tratasse diretamente da proteção de dados em si, o que veio a ser efetivamente regulamentado por meio da LGPD em 2018.

Assim, naquele momento, o Brasil ainda carecia de uma legislação mais abrangente, que pudesse traçar normas especialmente referentes à proteção de dados, principalmente frente a influência que a GDPR gerou em outros países, ao traçar em seu artigo 46 que a transferência de dados só poderia ser feita a países que também tivesse leis que gerassem uma proteção adequada, vejamos:

> Artigo 46.º. Transferências sujeitas a garantias adequadas 1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.o, n.o 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

Conforme expõe Bioni (2020), desde 2010 existia o debate acerca de uma legislação de proteção de dados. Além disso, na primeira versão do anteprojeto da lei para proteção de dados colocada para consulta em 2010 (DISPÕE...,2020), o consentimento era colocado como a única hipótese em que poderia haver o tratamento de dados. Também, como afirma o autor, apesar de o artigo 7º da LGPD prever outras hipóteses em que poderá haver o tratamento de dados, isso não significa que o consentimento deixou de ser o seu vetor principal.

No decorrer da LGPD, o consentimento é tratado de forma exaustiva, aparecendo no texto 35 vezes. Nas palavras de Mendes (2014), a validade do consentimento se forma a partir dos pressupostos de que

> [..] o titular deve emitir consentimento por sua livre e espontânea vontade; ii) o consentimento deve ser voltado a uma finalidade específica; iii) deve haver informação ao usuário sobre os objetivos da coleta, processamento e uso de dados e consequências sobre não consentir com o tratamento.

Isso será mais bem tratado em tópico posterior.

Frente a importância que a LGPD confere ao consentimento, bem como às adjetivações trazidas para conferir ao indivíduo o seu direito de autodeterminação informativa, convém debater sobre ele e suas especificidades.

3. CONSENTIMENTO

Para entender a importância de se pensar acerca da figura do consentimento no cenário de proteção de dados, antes cabe uma análise sobre o contexto em que se insere a LGPD. Trata-se de uma sociedade em que, conforme indica Bioni (2020), os dados pessoais emergem com uma dupla função, qual seja, a de garantir direitos fundamentais e o direito à privacidade e, além disso, de fomentar o desenvolvimento econômico.

Logo, vê-se que os dados servem agora como uma moeda de troca

dentro do mercado, chegando a serem definidos até mesmo como uma *commodity*, conforme expõe Doneda (2006). Isso implica, também, a configuração de uma vigilância multifacetada, em que não há apenas uma relação de dois atores, mas de múltiplos, que compartilham as informações entre si. Trata-se, como ilustrado por Bauman (2011, p.25) de uma "modernidade líquida", em que há diluição das relações. Por isso, o controle do que é feito com tais dados torna-se cada vez mais complicado, o que gera a necessidade de regulamentações que possibilitem que os titulares de dados possam controlar suas informações frente ao que Bioni (2020) denomina de "morte da privacidade".

Nessa perspectiva, os países convencionam sobre a delimitação de princípios para reger o tratamento de dados, figurando dentre eles o princípio do consentimento. Nas palavras de Mendes (2014, p. 68):

> A convergência internacional estabelecida acerca dos princípios é marcante: mesmo os ordenamentos jurídicos mais diversos preveem praticamente os mesmos princípios de proteção de dados, com mínimas diferenças. Esse quadro comum de princípios é conhecido por "Fair Information Principles" e teve a sua origem na década de 70 de forma quase simultânea nos EUA, Inglaterra e Alemanha.

Mesmo em ordenamentos diversos, há basicamente um rol de princípios orientadores que é praticamente o mesmo, com diferenças mínimas. Dentre alguns princípios básicos listados, vejamos alguns que aparecem com mais frequência, conforme também listados por Malheiros (2017), quais sejam, o da publicidade, transparência, qualidade de dados, segurança, responsabilidade e o consentimento, cerne deste artigo.

O princípio da finalidade é um princípio constante em todas as atividades de processamentos de dados e envolve a adequação entre o uso e a finalidade pela qual o dado será tratado (MALHEIRO, 2017, p. 34). O princípio da transparência ou publicidade, por sua vez, veda a existência de bancos de dados sigilosos, conforme explica Doneda (2006), prezando que o banco de dados seja sempre de conhecimento público, a fim de coibir abusos.

Já o princípio da qualidade de dados denota que deve existir um tratamento adequado, lícito e pertinente dos dados, sem que as atividades ultrapassem ao necessário para obtenção da finalidade traçada. O princípio da segurança (física e lógica) demanda que haja proteção de qualquer banco de dados quanto a possíveis extravios, destruições e desvios (DONEDA, 2006, p. 217). Além disso, correlacionado estaria o princípio da responsabilidade, que, nas palavras de Malheiro (2017, p. 34), assegura a reparação de danos que possa ser gerado ao indivíduo pela violação de seus dados.

Nessa linha de pensamento, por fim, destaca-se o princípio do consentimento, pelo qual o usuário confere sua permissão, anuência, aprovação para determinada forma de tratamento de seus dados. (MALHEIRO, 2017, p. 34). O consentimento se configura como um meio para implemento do direito à autodeterminação informativa e, como afirma Doneda (2006, p. 212), age como uma “mola propulsora” na estrutura de proteção de dados.

Quando aplicado para o ambiente de proteção de dados pessoais, surge com a ideia de liberdade e autonomia para os usuários sobre a ciência dos procedimentos a serem feitos com seus atos e decidir se dará a sua anuência ou não. (CORRÊA, 2019, p.29). Nas palavras de Krieger (2019), o consentimento surge como um instrumento do indivíduo para exercício de sua autodeterminação informativa, conferindo a ele o poder de anuir ou não com a coleta e tratamento de suas informações.

Por isso, é válido dizer que o indivíduo assume, portanto, um papel central na legislação de proteção de dados, característica marcante já vista a partir da terceira geração de dados, cabendo a ele a participação em todo o processo de tratamento de dados, que vai desde a coleta até a exclusão do dado do sistema.

Nas palavras de Malheiro (2017), o consentimento adquiriu, no decorrer das gerações de leis de proteção de dados pessoais, um papel central, alterando apenas com o passar do tempo a sua carga participativa em autodeterminar suas informações pessoais.

Na LGPD o consentimento é determinado no artigo 5º, XII como uma

“manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. O intuito da lei em adjetivar o consentimento extensivamente, colocar o campo gravitacional dos princípios focado no indivíduo e conferir regramento específico ao instituto denota a importância dada ao consentimento na LGPD. (BIONI, 2020).

Assim, apesar de o consentimento não ser a única base legal em que pode ser fundado o tratamento de dados e também não se demonstrar como um princípio hierarquicamente superior aos outros expostos no artigo 7º da LGPD, este assume uma importante posição na Lei, motivo pelo qual é feito este estudo.

Com isso, é importante analisar sua natureza e os adjetivos que os acompanham, quais sejam: “livre”, “informado”, “inequívoco”, o que será feito nos próximos tópicos. Além disso, deve-se questionar se o consentimento efetivamente assume posição central e se assegura a autodeterminação informacional, nesse modelo de economia que é gerado a partir da troca de dados pessoais.

3.1 Consentimento “livre”

Apesar de a LGPD trazer a figura do consentimento no âmbito da proteção de dados, esse instituto já permeava o ordenamento jurídico brasileiro. A CF/88 já estabelece seu cerne em torno da pessoa, titular de direitos e garantias fundamentais que se refletem em todo o sistema jurídico. Essa é a tendência também seguida pelo Código Civil de 2002 (CC/02), que se desprende da visão patrimonialista e coloca em foco a pessoa e suas relações, de modo que, numa perspectiva Kantiana, o indivíduo é um fim em si mesmo e deve respeitar à comunidade em que se insere. Dessa perspectiva, emergem princípios como o de solidariedade e função social.

Um outro ponto importante é observar que o CC/02 trouxe o privilégio da autonomia privada em detrimento à autonomia da vontade, que, por mais que se pareçam sinônimos, apresentam diferenças notáveis, ao passo que a

autonomia da vontade se constitui como uma mera liberdade formal e a autonomia privada é pautada nos valores da CF/88, pensando nos interesses da sociedade em geral, não mais uma perspectiva individualista. Como explica Galvão (2015):

> A autonomia, hoje, não é mais um fim em si, essa era a autonomia da vontade. A autonomia privada é um instrumento que tem como finalidade a promoção de interesses que sejam úteis para a sociedade em geral, consolidando os fundamentos estabelecidos no preâmbulo da Constituição. Diante do exposto, resta claro que a autonomia da vontade e autonomia privada são lados opostos da mesma moeda, tendo em vista que a primeira é a vontade humana elevada à condição de base do liberalismo e a segunda representa a vontade humana adapta às necessidades e expectativas da sociedade em geral.

Na esfera contratualista, privilegia-se como um de seus elementos principais, então, a manifestação de vontade livre e de boa-fé, sem vícios do consentimento (erro, dolo, coação, lesão ou estado de perigo) ou vícios sociais (simulação e fraude contra credores).

Quando a vontade manifestada no mundo externo não corresponde àquela vontade gerada internamente, ou seja, quando essa não se dá de forma realmente livre e espontânea, diz-se que o negócio jurídico é viciado.

Sobre a definição clássica que privilegia o elemento volitivo, cabe a crítica trazida pela Teoria Preceptiva, defendida por alguns autores, como Fiuza (2007). A teoria propõe a ideia de que nem sempre será possível considerar a vontade interna, produzida no íntimo do agente, mas sim aquela vontade declarada, podendo ser expressa em comportamentos, por exemplo, como o clique no “eu aceito” de termos de adesão.

Na mesma perspectiva, a LGPD traz como elemento de validade do consentimento no âmbito da proteção de dados, a *manifestação livre.* De acordo com Bioni (2020), o instituto do consentimento é atrelado aos defeitos do negócio jurídico, tendo em vista que precisa ser livre e consciente.

Assim, pode-se dizer que, para traçar o que é o consentimento livre, cabe dizer que é aquele que, além de seguir as necessidades previstas na

LGPD, não contém em sua essência algum vício, que seriam os mesmos trazidos pelo CC/02, quais sejam: erro (arts. 138-144), dolo (arts. 145-150), coação (arts. 151-155), estado de perigo (art. 156), lesão (art. 157). Não obstante, o próprio artigo 8º, §3º já consagra a vedação de tratamento de dados pessoais mediante vício do consentimento.

Conforme ainda indica Souza (2018), é necessário entender que o consentimento se divide em duas etapas, devendo ser fornecido antes do processamento de dados e quando ocorre compartilhamento desses dados.

Bioni (2020) entende que, caso a caso, deve-se sempre observar se há algum tipo de subordinação na hora da emissão da manifestação de vontade.

Por isso, vê-se que o contexto em que o consentimento foi dado deve ser levado em consideração para verificar se, de fato, este foi livre, considerando caso a caso se houve subordinação que retirou a voluntariedade do consentimento.

3.2 Consentimento “informado”

O adjetivo “informado” traduz que o consentimento deverá ser dado pelo titular dos dados com a ciência deste sobre todas as informações acerca do tratamento. Ou seja, há a necessidade de que seja feito o repasse de tudo aquilo que irá permear o tratamento de dados de forma detalhada, verdadeira e transparente. Além disso, é necessário que as possíveis consequências de não consentir também sejam informadas.

Também trazendo o panorama de outras áreas do Direito, podemos ver que o consentimento informado é amplamente utilizado para tratamentos na área de saúde. Logo, o médico deve informar o paciente acerca de todas as informações sobre seu tratamento, conferindo ao paciente a participação em toda e qualquer decisão que atinja sua integridade psicofísica. Nesse sentido, destaca a necessidade de o paciente ser informado sobre todas ações que serão feitas durante seu tratamento médico, para que este tenha capacidade decisória sobre a sua submissão ou não ao tratamento. O consentimento

informado seria, ainda, uma extensão do princípio de boa-fé.

Na perspectiva da LGPD, essa participação do titular dos dados acontece em todo o seu tratamento de dados. Malheiro (2017) destaca o quão o consentimento informado está atrelado à autodeterminação informativa, pois os indivíduos estão no controle de suas informações e vidas, além de ser um dever de que ao indicar sua vontade, o titular deve estar completamente informado do que está consentindo, com as consequências e riscos da decisão.

Para melhor compreender esse adjetivo, é válido a observação dos artigos 9º e 6º, VI, da LGPD. É nítido o quão é importante o respeito ao princípio da transparência, tendo em vista que o titular deve ter acesso a todas informações do tratamento de dados, de forma simplificada e clara.

Assim, é perceptível que não basta que haja o repasse de informações àquele que têm seus dados tratados, mas esse repasse deve ocorrer de forma completa, transparente e simples, de modo que haja o entendimento do que irá ocorrer para que se saiba com o que se está anuindo.

Bioni (2020) defende que o consentimento informado passa por duas etapas, sendo: (i) o pedido através do controlador e (ii) a manifestação de vontade feita (ou não) pelo titular. Assim, vê-se a exigência de ações por parte dos interessados, ocorrendo em um primeiro prisma.

Sendo assim, conclui-se que o consentimento informado é a garantia de que o indivíduo tenha autonomia para decidir sobre o que acontecerá com os seus dados, mas, para que isso aconteça, deve ser ele empoderado com a verdadeira ciência de todas as informações e disposições sobre o tratamento, para que de fato essa autonomia seja preservada.

3.3 Consentimento “inequívoco”

O adjetivo “inequívoco” relaciona-se com a necessidade de que o titular tenha uma ação que indique a anuência do titular, não sendo considerado aquele consentimento feito de forma passiva. Poder-se-ia dizer então que se

estabelece uma vedação aos sistemas *opt-out*, E nesse mesmo passo, os extensos termos de privacidade que são utilizados na internet deveriam revisar suas práticas, tendo em vista que um mero “Eu aceito” no fim de longos textos talvez não seja hábil a expressar um consentimento inequívoco, que a LGPD traz.

Ainda poder-se-ia dizer que o consentimento trazido pela LGPD adota a forma “*click-wrap*”, modalidade em que, conforme Lima (2009), há uma ação por parte do usuário para demonstrar a sua anuência, através de expressões como “aceito”, “concordo”, “sim”.

No artigo 8º, é esclarecido que o consentimento deve ser dado de forma escrita ou de outro meio que demonstre sua vontade. Se por escrito, o §1º ainda traça que deverá ser dado de forma destacada das demais. Além disso, o §4º veda autorizações genéricas, devendo o consentimento se referir a fins determinados.

É fundamental perceber, então, que o consentimento deve ser atrelado em conjunto com o adjetivo da especificidade, se referindo a um processamento de dado específico. Ademais, que passa a fazer sentido a obtenção do consentimento “granular”, aquele dado aos poucos, em cada fluxo de dados e em cada tentativa de acesso aos dados pessoais.

Por isso, conforme explica Doneda (2006), o consentimento é voltado a um fim específico, retirando-se propósitos genéricos que poderiam implicar na emissão de um “cheque em branco” pelo titular aos coletores de dados, sem a possibilidade de interpretações extensivas, que vão além das que estariam previstas.

Logo, conforme apresenta Pinheiro (2018), é primordial para assegurar a liberdade e privacidade a garantia de que os usuários estejam cientes de que devem consentir o uso dos dados, assim como ter o direito de saber o fim da coleta e acesso ao seu conteúdo a qualquer momento.

3.4 Hipóteses de dispensa

Apesar de o consentimento ser um dos conceitos basilares que compõem a LGPD, Bioni (2020) defende que é necessário observar que, ao revés da primeira ideia de legislação apresentada em 2010, não é a única base legal para o tratamento de dados e, além disso, sua alocação foi feita no artigo 7º horizontalmente às outras hipóteses, sem relação de hierarquia.

A LGPD buscou, assim, estabelecer um equilíbrio entre as vontades do titular e as necessidades dos controladores de dados no momento que exercem suas atividades, tendo em vista serem alguns tratamentos de dados imprescindíveis ao cumprimento de obrigações em determinados setores de atuação. É o que se percebe quando se retira a necessidade do consentimento para cumprir leis e políticas públicas e para órgãos de pesquisa (com dados anonimizados, sempre que possível), por exemplo.

Ademais, importante perceber que há ponderação de direitos como o de tutela da saúde e proteção da vida, ao se analisar a hipóteses dos incisos VII e VIII, já que os direitos fundamentais não se revestem de caráter absoluto, mas sim relativos.

Também, dados referentes a pessoas públicas, sendo considerados de fácil acesso são uma hipótese de dispensa. Mas também o tratamento de dados deve se restringir à finalidade para qual eles foram disponibilizados.

Não obstante, há a dispensa do consentimento no que tange à necessidade de manipulação de dados para a execução de contratos ou exercício regular de direitos. Esse seria o caso de, por exemplo, uma empresa precisar se utilizar dos dados de seus empregados em eventuais ações judiciais.

Contudo, Bioni (2020) ainda defende que o consentimento não deixou de ser importante para a lei, considerando que o instituto é tratado de forma exaustiva ao decorrer do texto que o adjetiva, coloca princípios que centralizam o titular dos dados e confere ao consentimento regramento específico. Apesar

disso, no caso concreto, as outras hipóteses do artigo 7º também deverão ser analisadas, equitativamente à hipótese do consentimento.

3.5 Hipóteses de revogação

Como já trazido em outros tópicos, o tratamento de dados da LGPD é intrinsecamente ligado ao princípio da finalidade. O princípio é consagrado de forma principal no artigo 6, §1º e trazido ao longo de outros artigos pela Lei, o que reforça sua importância. Por isso, há a necessidade de que os fins que motivam o tratamento de dados e que foram informados ao usuário sejam mantidos e respeitados durante todo o processo.

As hipóteses de revogação dizem respeito principalmente a alterações que possam ocorrer durante o processo de tratamento de dados. Qualquer alteração feita em relação às informações fornecidas inicialmente importa na necessidade da obtenção de um novo consentimento, tendo em vista que houve mudança naquilo que foi passado ao titular quando este anuiu com o tratamento.

Consequentemente, as hipóteses dos artigos 8º, §6º e 9º, §2º demonstram a importância do resguardo da finalidade que motivou a anuência pelo titular e da ciência deste de todos os atos que permearão o processo de tratamento de dados. Caso não concorde com qualquer alteração ou modificação, poderá revogar o seu consentimento.

Mas é fundamental ressaltar, também, que o legislador se preocupou em assegurar que a revogação pudesse ser feita a qualquer momento, de forma gratuita e facilitada, por meio de uma manifestação pelo titular (artigo 8º, §5º e o artigo 18º, IX da LPGD)

Dessa forma, é visível a importância dada à vontade do titular para as ações feitas com suas informações, ao visualizar-se que este tanto permite ou não que o tratamento se inicie, mas também decide se o tratamento deve ser finalizado caso não concorde com os passos que serão dados por aqueles que manipulam suas informações.

4. DO PAPEL DO CONSENTIMENTO COMO GARANTIDOR DA AUTODETERMINAÇÃO INFORMATIVA

As legislações de proteção de dados de quarta geração têm a característica de conferir ao titular a participação em todas as etapas do processamento de dados, desde a coleta até ao compartilhamento. Colocando o consentimento como um requisito essencial do tratamento de dados, há a impressão de que a mera necessidade da obtenção do consentimento seria hábil a garantir a autodeterminação informativa do titular.

Discorre Doneda (2015) que o princípio da autodeterminação informativa surgiu como uma extensão das liberdades constantes nas leis de segunda geração, e a participação do titular não mais se restringe só a consentir no início do tratamento de dados, mas também participa de diversas fases sucessivas do tratamento, inclusive para decidir acerca do compartilhamento com terceiros ou não.

A doutrina afirma que o direito à autodeterminação informativa foi reconhecido primeiramente pelo Tribunal Constitucional Alemão, no julgamento da Lei do Censo Alemã, em 1983. A corte alemã afirmou que o direito à autodeterminação informativa “pressupõe que, mesmo sob as condições da moderna tecnologia de processamento de informações [...] o indivíduo exerça sua liberdade de decisão sobre as ações a serem precedidas ou omitidas em relação a seus dados”. (VIEIRA, 2007, p.88).

Portanto, o princípio visa garantir que o titular dos dados esteja no controle de suas informações ao participar do tratamento de dados, desde o consentimento para o início do tratamento até o compartilhamento com terceiros.

Como se afirma Krieger (2019), o consentimento surge como instrumento para possibilitar o exercício da autodeterminação informativa, ao passo que a ele cabe anuir (ou não) com a coleta e tratamento de suas informações.

Ainda, Malheiro (2017) diz que o consentimento é uma forma de

implementação do direito à autodeterminação informativa, com a participação do indivíduo, funcionando como uma “mola propulsora” da estrutura de proteção de dados.

Mas é nítido perceber que há uma certa “hipertrofia” do consentimento, conforme indica Bioni (2020), tendo em vista a tamanha importância que é conferida ao instituto. Como o autor defende, é necessário que se repense a autodeterminação informativa além da lógica binária, sendo fundamental que a tutela jurídica ultrapasse o raciocínio bifásico que se concentra na escolha do indivíduo consentir ou não com o tratamento de seus dados pessoais.

Por isso, é importante pensar que não só se deve observar o elemento volitivo, mas considerar o fluxo informacional em que está inserido, conferindo se o indivíduo realmente é empoderado a tomar as decisões acerca de seu tratamento de dados.

Primeiro porque se pode perceber que o consentimento enfrenta desafios e dificuldades diante da sua inserção na sociedade da informação. O que se deve observar é que vivemos em um contexto de massiva disseminação de dados, que circulam como moeda de troca. Na lógica do *Big Data,* prioriza-se o grande volume de dados e se descentraliza a vigilância. Os atores do fluxo informacional são muitos, sendo difícil até mesmo determiná-los.

Nesse grande progresso tecnológico, percebe-se quão difícil o consentimento cumprir de fato com os adjetivos que a Lei propõe. Como determinar que o consentimento é mesmo livre considerando, por exemplo, a massiva veiculação de propagandas que influenciam também a vontade do usuário? Ou o fato de que os termos de adesão não conferem escolha ao titular dos dados, pois, para se inserir na sociedade, deve consentir com os termos que são oferecidos?

Quanto aos termos de uso e políticas de privacidade de serviços oferecidos na Internet, é fácil perceber que são demasiadamente longos e o clique no “eu aceito” ao final no texto claramente não reflete a real manifestação de vontade do usuário. Isso porque, primeiramente, não há a

leitura de todo o texto, conforme Sansana (2018, p. 16), a Universidade de Stanford verificou em uma pesquisa que 97% dos entrevistados não liam os termos, contratos e políticas e passavam direto para o aceite.

Além disso, o que acontece sempre é a priorização de ganhos rápidos, tendo em vista que a sua não aceitação geraria a impossibilidade de uso daqueles serviços. Em suma, conforme defende Bioni (2020) a participação social é dependente do trânsito informacional. A não aceitação geraria, portanto, exclusão do usuário. Pode-se dizer, então, que há uma "falsa" escolha. Como elo mais fraco da relação, o usuário tende a se render ao mercado informacional; sequer o indivíduo é hábil a racionalizar uma decisão.

Nessa esteira de pensamento, o *European Data Protection Board* (EDPB), o órgão responsável pela aplicação da norma europeia, atualizou as diretrizes de consentimento que vigoravam desde 2018, reforçando o entendimento de que "um prestador de serviço não pode impedir um titular de dados de acessar um serviço em razão de este não ter dado seu consentimento" (EUROPEAN DATA PROTECTION BOARD, 2020). Ainda que essa disposição valha apenas para a União Europeia, as diretrizes já nos servem como um comparativo e talvez um forte indicativo de como a ANPD se posicionará, conforme analisa Moraes (2020).

Ademais, é difícil analisar apenas o elemento volitivo nesse contexto de massiva veiculação de publicidades que influenciam o usuário a todo tempo. Nas palavras de Fiuza (2007):

> Imaginar que os contratos seriam fruto de vontade livre e incondicionada, como queriam os liberais, nos séculos XVIII e XIX, é desdenhar todo o avanço das ciências que estudam a mente humana, como a psicologia e a psicanálise.

Isso porque a tamanha importância conferida ao elemento volitivo nos faz ignorar o contexto de veiculação de publicidades que influenciam a todo tempo a vontade dos usuários. Conforme indica Fiuza (2007), as convenções que originam os contratos vão além de um mero acordo de vontades, sendo calcadas numa verdadeira necessidade.

Não obstante, cabe repensar também o consentimento informado. O adjetivo “informado” diz respeito a um conhecimento adequado das ações que permearão o tratamento de dados para fornecer uma decisão adequada.

Contudo, cabe citar um exemplo trazido por Bioni (2020): em 2014, um artigo científico[2], produzido por um membro da equipe do Facebook, revelou que a rede social realizou uma pesquisa de cunho emocional com os usuários, demonstrando que os usuários eram influenciados pelo que viam nas *timelines.* Quando indagaram o Facebook sobre isso, foi alegado que o consentimento havia sido fornecido nos termos de uso do Facebook, na cláusula que informava a captação de informação para propósitos científicos. De acordo com a justificativa do Facebook, o titular então teria sido “informado” sobre a pesquisa.

Diante desses questionamentos e muitos outros, deve-se desvincular a ideia de uma autodeterminação informativa pautada apenas no consentimento. O que se vê na realidade, conforme Bioni (2020) diz é que há uma (hiper)vulnerabilidade do titular de dados, com uma clara “relação assimétrica que salta aos olhos”.

Autores como Malheiro (2017) chegam até mesmo a acreditar em um “mito do consentimento”, acreditando que seria um instrumento fictício e ilusório, pois seus efeitos se perdem e o usuário fica sem a autodeterminação que lhe era protegida.

Assim, mais importante do que apenas avaliar se o usuário anuiu ou não com as ações que permearão o tratamento de dados, Bioni (2020) propõe que a tecnologia pode ser útil também ao empoderamento do titular, que é (hiper)vulnerável.

Surge também a proposta de um consentimento “granular”, conforme explicita Bioni (2020), em que o titular tem a liberdade de decidir sobre: (i) quais serão seus dados coletados; (ii) por quais modalidades de tratamentos eles serão submetidos; (iii) por qual período de tempo e frequência; e (iv) a

2 KRAMERA, Adam D.I.; GUILLORYB, Jamie E.; HANCOCKB, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. PNAS Review, v.111, n.29, p. 8788-8790, Jul. 2014, Disponível em: <http://www.pnas.org/content/111/248788.full.pdf>. Acesso em: 12 jul. 2019

possibilidade de compartilhamento com terceiros.

Dessa forma, o consentimento granular permitiria que o titular dos dados tivesse uma entrada gradual em meio ao fluxo de dados, com a fragmentação de suas autorizações, como indica Corrêa (2019).

Nessa perspectiva, conclui-se que é um grande passo o indivíduo estar no controle de suas informações, mas é necessário analisar que implementar o consentimento é uma atividade complexa, repleta de desafios e dificuldades. Ainda há um longo caminho para se efetivar o princípio da autodeterminação informativa e conferir uma efetiva segurança ao titular de dados.

Olhando sob uma perspectiva positiva, é interessante analisar o recente julgamento da MP 954/2020[3], que dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Consultado e Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) durante a COVID-19, com o argumento de suporte à produção de estatísticas.

O julgamento, que determinou a suspensão da MP, foi considerado um marco histórico da proteção de dados no Brasil (VAINZOF, 2020) e demonstrou uma preocupação com o princípio da autodeterminação informativa e com o conteúdo da LGPD, ainda que a Lei não esteja ainda em vigor. É interessante observar que o caso que deu origem à autodeterminação informativa tratava-se de caso semelhante, em que o Tribunal Constitucional Alemão julgou parcialmente constitucional a Lei do Censo, que permitia a coleta e tratamento de dados para fins estatísticos, bem como a transmissão anonimizada desses dados para a execução de atividades públicas. Entre um dos motivos que motivou o julgamento, motivo esse que também permeou o julgamento no Brasil, o Tribunal afirmou que havia coleta excessiva de dados, além da finalidade adequada.

3 BRASIL. Medida provisória nº 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. **Diário oficial da União:** edição extra, Brasília, DF, 17 abr. 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 12 jul. 2020.

A decisão foi importante como um indicativo de relevância da LGPD para o ordenamento jurídico e nos traz a concepção de que, sim, há um longo caminho para que o titular dos dados esteja de fato seguro imerso na sociedade de informação em que vive, mas que as portas já estão abertas e a LGPD é um marco inicial para se efetivar a proteção de dados pessoais no Brasil.

5. CONCLUSÃO

Diante disso, conclui-se que a LGPD é um importante dispositivo que insere o Brasil como um dos países considerados seguros para tratamento de dados. Além disso, inova quanto às outras legislações brasileiras, visto que não se tinha um regulamento que tratasse especificamente sobre o tema de proteção de dados.

A LGPD se insere na quarta geração de legislações de proteção de dados, junto a legislações como a *General Data Protection Regulation* (GDPR), geração que insere o titular no processamento de dados, desde a coleta de dados até a decisão acerca do compartilhamento de terceiros.

Dentre as inovações trazidas pela LGPD, destaca-se a importância conferida ao consentimento, que aparece diversas vezes ao longo do texto, ganha adjetivações para que seja considerado válido e permeia diversas outras normas ao longo do texto. Esse destaque faz com que o consentimento seja considerado uma forma de garantir a autodeterminação informativa.

Tendo em vista o contexto de progresso tecnológico em que se insere, a dita sociedade da informação, não é possível conferir tamanha importância ao instituto sem adotar uma postura crítica e discorrer sobre os desafios e dificuldades que a implementação do consentimento enfrenta.

Dentro do processo de datificação das coisas, em que dados figuram como moedas de troca e os atores envolvidos no fluxo de dados são múltiplos, o consentimento esbarra em desafios para ser adjetivado como “livre, informado e inequívoco”.

Por consequência, é fundamental repensar a autodeterminação informativa como um princípio que vai muito além de obter o consentimento do titular ou não. As tecnologias devem, então, empoderar o titular de dados, que se encontra em posição de (hiper)vulnerabilidade, ao contrário do que se costuma afirmar. Só assim se poderá falar em uma autodeterminação informativa.

Logo, é imprescindível notar que a LGPD, apesar de sua importância, ainda enfrentará um longo caminho até efetivar a segurança do titular dos dados. De igual modo, o controle de informações por parte do titular é um passo extremamente importante e necessário, mas a implementação do consentimento enfrentará desafios para que seja hábil a empoderar o usuário cujos dados venham a ser tratados.

REFERÊNCIAS

ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. **Revista de Direito, Governança e Novas Tecnologias,** Goiânia, v.5, n.1, p.110-133, Jan/Jun de 2019.

APÓS ESPIONAGEM, Dilma pede urgência de votação do Marco Civil da Internet. **O Globo.** Disponível em: https://oglobo.globo.com/economia/apos-espionagem-dilma-pede-urgencia-de-votacao-do-marco-civil-da-internet-9912712. Acesso em: 20 mai. 2020.

ARAGÃO, Alexandre. Dilma sanciona Marco Civil na abertura do NETMundial. **Folha.** Disponível em: https://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml. Acesso em 01 mai. 2020.

BRASIL. Medida provisória nº 954, de 17 de abril de 2020**.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. **Diário oficial da União:** edição extra, Brasília, DF, 17 abr. 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 12 jul. 2020.

BAUMAN, Zygmunt. **44 cartas do mundo líquido moderno**. Rio de Janeiro:

Jorge Zahar, 2011.

BIONI, B. R. **Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 06 mar. 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

CANCELIER, Mikhail Vieira de Lorenzi; CRISTO, Camila Kohn de; MAFRA, Gabriela**.** Evasão de informações privadas: proteção à privacidade nos casos de pornografia de vingança. In: Anais do 4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. 2017, Santa Maria. **Anais** Santa Maria: UFSM, 2017. p.1. Disponível em: https://egov.ufsc.br/portal/conteudo/evas%C3%A3o-de-informa%C3%A7%C3%B5es-privadas-prote%C3%A7%C3%A3o-%C3%A0-privacidade-nos-casos-de-pornografia-de-vingan%C3%A7. Acesso em: 13 mar. 2020.

CORRÊA, Ana Carolina Mariano. **Análise do consentimento na Lei de Proteção de Dados Pessoais no Brasil e sua aplicação no mundo jurídico**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Presbiteriana Mackenzie, São Paulo, 2019.

DAVANZO, Danilo. E-mail marketing: sistema opt-in e opt-out de envio. **In: Revista JusBrasil.** 15 jul. 2015. Disponível em: https://danilodavanzo.jusbrasil.com.br/artigos/208357821/e-mail-marketing-sistema-opt-in-e-opt-out-de-envio. Acesso em 13 abr. 2020.

DISPÕE sobre a proteção de dados pessoais, a privacidade e dá outras providências". **Cultura Digital.** Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf. Acesso em: 20 mai. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. ed. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Princípios da proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coords.). ***Direito & Internet III*** – Tomo I: Marco Civil da Internet (Lei n.12.965/2014). São Paulo: Quartier Latin, 2015, p.373.

ENTENDA o escândalo de uso político de dados que derrubou o valor do Facebook e o colocou na mira de autoridades". **G1.** Disponível em:https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 20 mai. 2020.

EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2020 on consent under Regulation 2016/679. Disponível em: https://media-exp1.licdn.com/dms/document/C4D1FAQGHYcZLifl3AA/feedshare-document-pdf-analyzed/0?e=1589734800&v=beta&t=ChhNtAPlxfI1H0WTWK-X1MwPkxc1kpoQIEQVzm_Nr-c. Acesso em: 20 mai. 2020.

FIUZA, Cesar. Por uma redefinição da contratualidade**.** 31 mar. 2017 In: **Âmbito Jurídico**. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/por-uma-redefinicao-da-contratualidade/. Acesso em 10 abr. 2020.

GALVÃO, Camilla. Qual é a diferença entre autonomia privada e autonomia da vontade? **In: Revista Conjur,** 07 mai. 2015. Disponível em: https://galvaocamilla.jusbrasil.com.br/artigos/186333535/qual-e-a-diferenca-entre-autonomia-privada-e-autonomia-da-vontade. Acesso em 20 mar. 2020.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha.** Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em 10 mar. 2020.

KRAMERA, Adam D.I.; GUILLORYB, Jamie E.; HANCOCKB, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. **PNAS Review**, v.111, n.29, p. 8788-8790, Jul. 2014, Disponível em: http://www.pnas.org/content/111/248788.full.pdf. Acesso em: 12 jul. 2019

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18)**. Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019. Data da publicação: 05 dez. 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020.

LIMA, Cíntia Rosa Pereira de. ***Validade e obrigatoriedade dos contratos de adesão eletrônicos* (shrink-wrap e click-wrap) *e dos termos e condições de uso* (browse-wrap)**: um estudo comparado entre Brasil e Canadá. Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2009.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet:** uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (graduação) – Universidade de Brasília, Faculdade de Direito, 2017. Data da publicação: 8 jan. 2018. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em: 20 mar. 2020.

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

Saraiva, 2014.

MORAES, Henrique Fabretti. **EDPB atualiza diretrizes sobre consentimento.** Linkedin. Disponível em: https://www.linkedin.com/posts/opiceblum_edpb-atualiza-diretrizes-sobre-consentimento-activity-6667168373253644288-HwGT. Acesso em 20 mai. 2020.

PASCHOAL, Sandra Regina Remondi Introcaso. A evolução histórica da principiologia dos códigos civis brasileiros e suas repercussões na teoria da responsabilidade civil**.** 01 abr. 2010 In: **Âmbito Jurídico**. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/a-evolucao-historica-da-principiologia-dos-codigos-civis-brasileiros-e-suas-repercussoes-na-teoria-da-responsabilidade-civil/. Acesso em 20 de mar. 2020.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva, 2018.

SANSANA, Alexandre Gomes. **Privacidade, consentimento, legítimo interesse e a nova Lei Geral de Proteção de Dados Pessoais**. Trabalho de Conclusão de Curso (Pós-Graduação) - Instituto de Ensino e Pesquisa em Direito Societário, São Paulo, 2018.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal de Uberlândia, Minas Gerais, 2018.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Dissertação (Mestrado em Direito, Estado e Sociedade). Universidade de Brasília, Brasília, 2007.

WARREN, BRANDEIS. The Right to Privacy. In **Harvard Law Review**, Vol Iv, Dez. 1890. Diponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html acesso em: 07 de jun. de 2017.

Recebido em | 23/06/2020
Aprovado em | 30/07/2020

Revisão Português/Inglês | Maria Carolina Ferreira Reis

SOBRE AS AUTORAS | *ABOUT THE AUTHORS*

LYS NUNES LUGATI

Graduanda em Direito pela Universidade Federal de Ouro Preto. Pesquisadora em Direito Digital. E-mail: nuneslys@gmail.com.

JULIANA EVANGELISTA DE ALMEIDA

Doutora e Mestra em Direito Privado pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Direito Civil pela Pontifícia Universidade Católica de Minas Gerais. Bacharela em Direito pela Pontifícia Universidade Católica de Minas Gerais. Professora do curso de Direito da Universidade Federal de Ouro Preto. Pesquisadora em Direito Digital. E-mail: juliana.almeida@ufop.edu.br.