UNIVERSIDADE NOVE DE JULHO
FACULDADE DE DIREITO
MESTRADO EM DIREITO

ALEXANDRE MULTINI MIHICH

O CONSENTIMENTO E O DIREITO À PRIVACIDADE SOB A ÓTICA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

São Paulo
2021

ALEXANDRE MULTINI MIHICH

O CONSENTIMENTO E O DIREITO À PRIVACIDADE SOB A ÓTICA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Nove de Julho - UNINOVE, como requisito parcial para a obtenção do grau de Mestre em Direito.

Orientador: Prof. Dr. Bruno Dantas Nascimento

São Paulo
2021

Mihich, Alexandre Multini.
Consentimento e o direito à privacidade sob a ótica da lei geral de proteção de dados pessoais. / Alexandre Multini Mihich. 2021.
113 f.
Dissertação (Mestrado) - Universidade Nove de Julho – UNINOVE, São Paulo, 2021.
Orientador (a): Prof. Dr. Bruno Dantas Nascimento.
1. Dados pessoais. 2. Direito à privacidade. 3. Proteção de dados. 4. Lei geral de proteção de dados.
I. Nascimento, Bruno Dantas. II. Titulo.

CDU 34

ALEXANDRE MULTINI MIHICH

O CONSENTIMENTO E O DIREITO à PRIVACIDADE SOB A ÓTICA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Mestrado em Direito da Universidade Nove de Julho como parte das exigências para a obtenção do título de Mestre em Direito

São Paulo, 09 de abril de 2021.

BANCA EXAMINADORA

Prof. Dr. Bruno Dantas Nascimento
Orientador
UNINOVE

pp

Prof. Dr. Newton. De Lucca
Examinador Interno
UNINOVE

pp

Prof. Dr. Adalberto Simão Filho
Examinador Externo
UNAERP

RESUMO

Nos dias atuais, a regulação da proteção de dados torna-se necessária, haja vista a massificação da coleta de informações. Inúmeras ações cotidianas compreendem transações envolvendo dados pessoais, tais como a relação do empregado e seu empregador ou a relação entre consumidor e fornecedor nas plataformas de *streaming*, e colocam o cidadão em situações de desvantagem e até mesmo de vulnerabilidade. Assim, a presente dissertação pretende proporcionar uma análise crítica da Lei Geral de Proteção de Dados, em especial buscando investigar se o direito à privacidade está salvaguardado pela lei e, ainda, se o consentimento do titular de dados está bem contemplado. Outro objetivo traçado para este estudo é esclarecer a importância e o impacto da Lei Geral de Proteção de Dados Pessoais, que se entende ser superior ao Código de Defesa do Consumidor. Não resta dúvida que a lei consumerista modificou os paradigmas das relações entre as empresas e as pessoas naturais. A metodologia adotada neste trabalho foi a dedutiva, ao partir de argumentos gerais para argumentos particulares, tendo sido apresentados os fundamentos que se consideram verdadeiros, em balizada doutrina, para, em seguida, chegar a conclusões formais particulares, com a modesta ousadia de tentar estabelecer pontes entre ideias, pensamentos e conceitos a fim de tentar uma nova abordagem sobre o tema. A pesquisa também realiza considerações críticas sobre o próprio texto da Lei Geral de Proteção de Dados Pessoais de forma indutiva, buscando explicar conceitos e as nuances normativas de determinados dispositivos que guardam pertinência com o objeto da pesquisa. Por fim, o presente trabalho buscou demonstrar que o consentimento perdeu seu núcleo central de protagonismo, seja pela dinâmica da sociedade ou mesmo pela massificação no tratamento de dados, devendo o aplicador do direito revisitar seus conceitos, em especial o paradigma do consentimento, para que utilize as outras bases legais de tratamento de dados pessoais previstas na Lei Geral de Proteção de Dados Pessoais, como o legítimo interesse ou o cumprimento de obrigação legal.

Palavras-chave: Dados pessoais. Direito à privacidade. Proteção de dados. Lei Geral de Proteção de Dados.

ABSTRACT

Nowadays, the regulation of data protection becomes necessary, in view of the widespread collection of information. Countless daily actions include transactions involving personal data, such as the relationship between the employee and his employer or the relationship between the consumer and the supplier on the streaming platforms, and put the citizen at a disadvantage and even vulnerability. Thus, this dissertation intends to provide a critical analysis of the General Data Protection Law, in particular seeking to investigate whether the right to privacy is safeguarded by the law and, also, whether the consent of the data subject is well contemplated. Another objective outlined for this study is to clarify the importance and impact of the General Law for the Protection of Personal Data, which is understood to be superior to the Consumer Protection Code. There is no doubt that consumer law has changed the paradigms of relations between companies and natural persons. The methodology adopted in this work was the deductive one, starting from general arguments for particular arguments, having been presented the foundations that are considered true, in marked doctrine, to, then, arrive at particular formal conclusions, with the modest boldness of trying to establish bridges between ideas, thoughts and concepts in order to try a new approach on the topic. The research also makes critical considerations about the text of the General Law for the Protection of Personal Data in an inductive way, seeking to explain concepts and the normative nuances of certain devices that are relevant to the object of the research. Finally, the present study sought to demonstrate that consent has lost its central nucleus of protagonism, whether due to the dynamics of society or even the massification of data processing, and the enforcer of the law should revisit its concepts, especially the consent paradigm, so that use the other legal bases for processing personal data provided for in the General Personal Data Protection Law, such as legitimate interest or compliance with legal obligations.

Keywords: Personal data. Right to privacy. Data protection. General Data Protection Law.

LISTA DE SIGLAS

ANPD	Agência Nacional de Proteção de Dados
CONAR	Código Brasileiro de Autorregulamentação Publicitária
CGI.br	Comitê Gestor da Internet no Brasil
DNPDP	*Dirección Nacional de Protección de Datos Personales*
FTC	*Federal Trade Commission*
IMDB	*Internet Movies Databases*
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
OCDE	Organização para a Cooperação e Desenvolvimento
PLPIP	Projeto de Lei de Proteção de Informações Pessoais
RJET	Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado
RGPD	Regulamento Geral sobre a Proteção de Dados

SUMÁRIO

INTRODUÇÃO

As normas jurídicas de proteção de dados vêm sendo discutidas há mais de cinquenta anos, considerando-se que a Lei de Proteção de Dados do *Land* alemão de Hesse foi promulgada em 30 de setembro de 1970.

Denota-se que a Alemanha, há muito vislumbrou a necessidade de proteção dos dados das pessoas naturais, pois identificou que a existência de meios automatizados para o tratamento da informação pessoal poderia proporcionar uma redistribuição de poderes na sociedade, de forma a conceder mais poder a quem tivesse mais dados pessoais em relação aos cidadãos ou titulares de dados, vale dizer, quem detivesse mais informações poderia realizar mais escolhas e análises, conforme seus próprios critérios e parâmetros; este poder, por decorrência, poderia causar prejuízos ao cidadão, na medida em que seus dados poderiam ser classificados de uma forma dissonante da sua realidade.

Em descompasso com a celeridade da nação alemã, apenas em 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD) pátria desabrochou sob o nº 13.709, contudo, sem vigência imediata, pois há uma nítida diferença entre ‘vigorar’ e ‘existir’, o que no Brasil é mister demonstrar, haja vista que a lei nacional passou a ter eficácia parcial somente em setembro de 2020, além do mais, de forma acidental, o que posteriormente será melhor esclarecido em capítulo apropriado.

O pensamento para regular a proteção de dados, por vários motivos, foi se tornando cada vez mais importante, pois até mesmo os fatos relacionados ao cotidiano estão mais ou menos impregnados em uma transação que envolve dados pessoais, tais como a relação do empregado e seu empregador ou a relação entre consumidor e fornecedor nas plataformas de *streaming*.

A proteção de dados pessoais se propõe, basicamente, a delimitar uma série de regras que vão governar o tratamento dos dados, pois reconhece que o cidadão está em uma relação de desvantagem, de até vulnerabilidade, sob certo ponto de vista, do tratamento de seus dados, no sentido de que ele não tem, em regra, o menor grau de conhecimento de quantas empresas e órgãos tratam seus dados pessoais, quais informações eles detêm, o que é feito com as informações, quais efeitos essas informações podem gerar sobre a pessoa natural.

É possível obter uma resposta concreta para todas estas indagações? Certamente, não. Atualmente as possibilidades de tratamento de dados são muito amplas, de formas diversas e, inclusive, sem que a pessoa natural se dê conta ou queira fornecê-los, como nas situações de ingresso na portaria de um edifício, em que o cidadão, além de ser monitorado por câmeras, ainda deve fornecer seus dados pessoais.

A massificação da coleta de informações não caracteriza propriamente uma distopia, mas o fato de que há um desequilíbrio conjuntural, já que os cidadãos têm necessidade de um rol serviços e novos produtos disponibilizados ou proporcionados pela sociedade da informação.

Desta maneira, mostra-se essencial a existência de um encadeamento de regras que definam, com clareza, como os dados devem ser tratados e quais os direitos do cidadão para insurgir-se contra eventuais abusos e contra o uso indevido da informação pessoal.

Em última análise, o cidadão não pode ser prejudicado em prol dos detentores da informação, dos grandes centros de processamento, sejam empresas privadas ou o próprio Estado, os quais detêm poder de vigilância, controle social e econômico e, ainda, realizam decisões que influenciam a vida do indivíduo, sem que este possa ter participação na tomada destas decisões.

Não se pode olvidar que a proteção de dados pessoais está ligada à noção de privacidade, que evoluiu a partir do direito à privacidade, mas com o decorrer do tempo se deslocou deste direito para se tornar um direito autônomo e, inclusive, mais amplo que o próprio direito à privacidade.

Para se compreender a dimensão do direito à proteção de dados, a lei pátria utiliza o substantivo geral, que é sinônimo do adjetivo universal, em sua redação, ou seja, se opõe à ideia de uma lei setorial, o que acarreta que toda informação relacionada à pessoa natural, identificada ou identificável, está abrangida por este direito.

Pretende-se, assim, com a presente dissertação, proporcionar uma análise crítica da Lei Geral de Proteção de Dados, em especial se o direito à privacidade está

salvaguardado pela lei e, ainda, se o consentimento do titular de dados está bem contemplado.

Outro objetivo traçado para este estudo é esclarecer a importância e o impacto da Lei Geral de Proteção de Dados Pessoais, que se entende ser superior ao Código de Defesa do Consumidor. Não resta dúvida que a lei consumerista modificou os paradigmas das relações entre as empresas e as pessoas naturais. Neste sentido, o viés de ser um consumidor está englobado na Lei Geral de Proteção de Dados, em razão da exigência de que a pessoa natural consumidora, para ser atendida, ou para que o serviço seja prestado, forneça suas informações pessoais.

Deve-se relembrar que o direito à privacidade, em apertada síntese, consiste no poder que a pessoa natural tem de controlar o conhecimento de terceiros, mas de forma negativa, excluindo-os do conhecimento de fatos a seu respeito. Portanto, o paradigma da privacidade é a exclusão, ou seja, deixar de fora o outro, pois aquilo que é privado seria exclusivo do titular de dados, cabendo apenas a ele escolher com quem compartilhar.

No entanto, o direito à privacidade não é vocacionado a ser aplicado na sociedade atual com o mesmo rigor de antigamente, pois há, hoje, um volume massificado de tratamento de dados pessoais por sistemas sofisticados de computadores; ademais, a privacidade é algo muito íntimo, visto que aquilo que é privado para um, pode não o ser para o outro, em razão da especificidade de pensamento de cada pessoa natural.

Em decorrência deste complexo quadro, surge a proteção de dados como uma solução adequada, no sentido de que a Lei Geral de Proteção de Dados não indaga, em artigo algum, se a privacidade foi violada, haja vista que não adentra em questões de ordem subjetiva, acerca do que seria na esfera pessoal de cada cidadão o significado de privacidade ou intimidade.

Inclusive, não se pode deixar de mencionar que a Lei Geral de Proteção de Dados tem o intuito de trazer proteção para circunstâncias em que a mera indenização não resolveria, em decorrência do problema conjuntural de assimetria de informações, razão pela qual prescreve uma sequência de regras objetivas sobre a informação pessoal, enfatizando com clareza o que se pode ou não fazer com os dados.

Para a organização que trabalha os dados, como para o controlador ou operador, a LGPD proporciona um elemento de segurança, pois esclarece quais são os requisitos a cumprir para o tratamento de dados pessoais. De outro lado, para o cidadão, determina quais são seus direitos, para que ele possa exercer não propriamente o direito à privacidade, pois não é este o propósito da lei, mas para que possa exercer o direito de controle sobre seus próprios atos.

Como se nota, os paradigmas da proteção de dados não são propriamente a exclusão, o segredo, o recato, a solidão, mas sim o controle, o conhecimento, a fiscalização, permitindo que a pessoa natural tenha instrumentos para fiscalizar e direcionar o que é feito com suas informações pessoais.

O cidadão, com os instrumentos que a lei de proteção de dados lhe proporciona, pode escolher com quem compartilhar seus dados pessoais, com qual finalidade e para quais empresas.

No atual cenário de evolução da sociedade, em que as pessoas estão constantemente sendo demandadas para fornecer dados, o direito à privacidade não conseguiria obter uma resposta regulatória segura, o que, inclusive, impediria o fluxo de transferência de dados, motivo pelo qual a lei direcionou o foco para o controle.

As leis de proteção de dados procuram proteger os dados, mas sem impedir sua utilização, na medida em que proporcionam ao cidadão segurança quanto ao uso, permitindo-lhe compartilhá-los com maior serenidade, pois tem ele ciência que poderá contestar e cancelar qualquer utilização indevida.

Hoje em dia o cidadão deve enxergar a Lei Geral de Proteção de Dados como um elemento indispensável para que exista confiança na utilização de seus dados, mesmo que, em determinadas circunstâncias, sua utilização indevida possa gerar consequências tremendamente nocivas e prejudiciais.

Outro ponto que não pode deixar de ser mencionado é a técnica pela qual a proteção dos dados exerce a sua proteção, que ocorre sobre os dados pessoais, e não sobre o direito à privacidade.

Em razão desta arquitetura, a Lei Geral de Proteção de Dados retira do centro da tutela a pessoa em si, e passa a exercer a tutela nos dados das pessoas naturais, o que, a princípio, pode parecer algo externo. Em outras palavras, na medida em que

as organizações coletam os dados, estes não estão mais física ou digitalmente com o seu titular, pois passam a estar em um sistema informatizado, como os servidores; neste sentido, a lei dedica sua atenção não propriamente nos dados, mas na forma pela qual o mau uso destes dados pode implicar danos em seu titular.

A finalidade última da lei de proteção de dados não é a proteção dos dados em si, pois os dados não são sujeitos de direitos, mas, ao invés, são objetos da lei e somente têm algum valor jurídico na proteção dos dados enquanto refletirem algo sobre o seu titular.

Portanto, pode-se concluir: a lei de proteção de dados é uma lei cujo alicerce é voltado para a proteção da pessoa humana, embora esta proteção seja realizada por via oblíqua, pois protegem-se os dados pessoais e não o direito à privacidade da pessoa natural. Ainda: estes dados pessoais são protegidos pela forma como são utilizados, pois os dados não são sujeitos de direto, mas são objetos da lei somente enquanto refletirem algo de seu titular.

Um ponto relevante que precisa ser mencionado é o substantivo ‘proteção’, constante no nome da lei e em outras 61 (sessenta e uma) oportunidades em seu inteiro teor, o qual direciona toda a orientação interpretativa da lei.

A ideia de proteção, como base interpretativa, não deixa esquecer que a razão de ser da lei somente se justifica quando a pessoa natural é protegida, pois o objetivo da lei não é regular dados, mas permitir interpretações hermenêuticas que proporcionem garantias à pessoa humana.

Outro ponto de construção da lei que precisa ser ventilado, refere-se ao fato de que os dados pessoais são regulados de forma objetiva (finalidade, consentimento, bases legais etc.), o que permite a construção de computadores, sistemas, modelos de negócios etc., que levem em conta, somente, as regras legítimas para o tratamento dos dados, sem a necessidade de questionar se a pessoa natural foi ofendida em sua personalidade ou se houve violação ao direito à privacidade.

As organizações, ao implementarem a Lei Geral de Proteção de Dados por meio de critérios objetivos de verificação e conformidade, proporcionam maior segurança à pessoa natural. Não haveria meio de proporcionar proteção de forma massificada sem um vetor objetivo ao tratamento de dados.

Além disso, o fato de as regras serem objetivas, permite que o alcance da proteção atinja a todas as pessoas naturais, independente de terem ciência ou condições de se preocupar com a proteção de seus dados, pois seriam poucas as pessoas naturais - se levar em conta o universo de pessoas - que teriam condições de postular pessoalmente seus próprios interesses em juízo, para requerer indenizações ou qualquer coisa do gênero.

Em razão da publicação da Lei Geral de Proteção de Dados, houve uma mudança conjuntural, pois apesar de os dados pessoais estarem presentes em quase todas as relações negociais e serem economicamente relevantes, a pessoa natural não recebia proteção estrutural e, inclusive, não tinha condições de ter controle sobre os seus dados.

Neste sentido, a lei não fez distinção entre um dado e outro, vale dizer, não há dado que possa ser mais relevante que outro, pois todo dado é protegido pela lei, sendo esta a forma encontrada pela legislação de proporcionar maior segurança e controle ao cidadão com relação aos seus dados pessoais.

Inclusive, o dado pessoal sensível previsto no artigo 5º, II, que trata de questões relativas à personalidade, tais como origem racial ou étnica, opinião política, convicção religiosa etc., não caracteriza maior proteção com relação ao dado em si, mas, tão somente, um regime mais estruturado para a sua utilização (art.11).

Para a lei, até mesmo um dado público é considerado dado pessoal, e há para o titular direito de exigir o devido tratamento, como na hipótese de o tratamento empregado atender ou não o princípio da finalidade.

O substantivo ‘tratamento’ foi empregado para transmitir a impressão de guarda-sol, pois ao ser maior que um guarda-chuva, propaga a ideia de envolver qualquer tipo de ação que seja feita com o dado, desde a coleta, armazenamento, transmissão, difusão etc., sendo, portanto, uma lei muito difícil de se evitar; assim, praticamente todas as atividades com um mínimo grau de complexidade vão envolver dados pessoais em alguma medida.

Não se pode deixar de mencionar as bases legais para o tratamento, previstas no artigo 7º, as quais devem ser verificadas *a priori*, pois sem estas o tratamento de dados pessoais não pode ser realizado. A lei transmite o entendimento de que não

existe tratamento de dados insignificante, que não precise ser justificado, ou seja, para ser legítimo, o tratamento deve estar previsto em um dos requisitos legais.

As bases ou requisitos legais para o setor privado são: consentimento, cumprimento de obrigação legal ou regulatória, execução de contrato ou de procedimentos preliminares, legítimo interesse e proteção do crédito.

Desta maneira, no setor privado, se o tratamento de dados não for enquadrado em uma destas cinco hipóteses, por consequência, não poderá ser realizado e deverá cessar.

O princípio da adequação, previsto no artigo 6º, II, da Lei Geral de Proteção de Dados, é descrito como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" e tem o fim de provocar no aplicador da lei, no mínimo, reflexões antes de tratar os dados pessoais para a organização, pois este deverá indagar: onde se usam dados pessoais? Para qual finalidade? A atividade é legítima? A atividade se enquadra em qual base legal de tratamento? Em outras palavras, o aplicador deve primeiramente documentar, a fim de evitar a ilegitimidade no tratamento dos dados.

As sanções previstas na lei estão dispostas nos artigos 52 a 54 e somente poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados, que é um órgão integrante da Presidência da República com a função de fiscalizar a aplicação da Lei.

Apesar de as sanções previstas somente poderem ser aplicadas a partir de agosto de 2021, devido a *vacatio legis*, isto não significa que não existam consequências potenciais para eventual descumprimento da lei, pois, uma vez em vigor, há possibilidade de serem propostas reclamações perante órgãos de defesa do consumidor, bem como ocorrer atuação do Ministério Público como fiscal da lei, ainda que a capacidade sancionatória da lei não esteja em vigor.

No artigo 6º, a lei prescreve dez princípios com relação à proteção de dados, sendo que, tivesse o legislador optado por fazer uma lei sintética, estes princípios, associados à boa-fé prevista no *caput* do artigo, seriam praticamente suficientes para proporcionar uma satisfatória proteção de dados, pois, na verdade, todo o restante da lei é uma tentativa analítica de tentar concretizar estes princípios.

No entanto, há de se ressaltar que a boa-fé não está classificada explicitamente como um princípio, sendo um fator de extrema importância em várias circunstâncias da aplicação, na leitura e nos modelos de utilização dos dados pessoais, principalmente, com relação a situações negociais contratuais.

A boa-fé é instituto já muito estudado no Direito Civil e no Direito do Consumidor e, por consequência, muito conhecido e utilizado pelo magistrado brasileiro, o que permite considerar sua aplicação como um princípio.

A Lei Geral de Proteção de Dados procura trazer ao tratamento de dados uma situação de legitimidade, que envolve, inclusive, lisura, no sentido de que os atos sejam praticados com o intuito de não lesar a outra parte (o titular de dados); neste sentido, importante considerar a boa-fé como um princípio, por toda a sua amplitude e por estar em perfeita harmonia com todo o restante da lei.

Além da lei tratar de prevenção, de obrigação de anotar, de fazer registro no tratamento de dados, de fazer análise e procurar minimizar riscos, a ideia da boa-fé entrelaça todos os demais princípios, e pode servir de fundamentação para todos os demais fundamentos, de forma a constatar se os demais instrumentos foram bem ou mal interpretados.

No entanto, o princípio mais característico da proteção de dados é o princípio da finalidade, pois determina que os dados pessoais somente podem ser tratados para as finalidades que forem autorizadas e que forem levadas ao conhecimento do titular de dados no momento da coleta.

De outro lado, nem todo tratamento começa junto com o titular de dados, pois o tratamento no setor público começa quando o órgão público tem acesso ao dado, por compartilhamento; porém, o fato de o acesso ao dado ter sido justificado, implica sempre em uma finalidade.

O princípio da finalidade impede que um dado seja vendido, eis que não existe finalidade genérica, pois a lei prevê que o consentimento genérico é nulo, evocando, aliás, uma regra da personalidade, de que ninguém pode abrir mão de nenhum aspecto da personalidade sem reter o mínimo essencial necessário para manter a sua própria autonomia.

Portanto, o princípio da finalidade é típico da proteção de dados, sendo que os princípios do acesso, transparência e segurança dos dados, a título de exemplo, podem ser encontrados na Lei de Acesso à Informação.

Pelo exposto, pode-se inferir que os princípios da proteção de dados são a energia ou o motor da proteção pretendida pelo legislador.

A metodologia adotada neste trabalho foi a dedutiva, ao partir de argumentos gerais para argumentos particulares, tendo sido apresentados os fundamentos que se consideram verdadeiros, em balizada doutrina, para, em seguida, chegar a conclusões formais particulares, com a modesta ousadia de tentar estabelecer pontes entre ideias, pensamentos e conceitos a fim de tentar uma nova abordagem sobre o tema.

A pesquisa também realiza considerações críticas sobre o próprio texto da Lei Geral de Proteção de Dados Pessoais de forma indutiva, buscando explicar conceitos e as nuances normativas de determinados dispositivos que guardam pertinência com o objeto da pesquisa.

A dissertação encontra-se estruturada da seguinte forma: o primeiro capítulo traz uma síntese do desenvolvimento do direito à privacidade, a evolução legislativa e o significado da privacidade para a jurisprudência; o segundo capítulo aborda o que se entende por dados pessoais, os conceitos adotados pela lei (reducionista *versus* expansionista), a crença no dado anônimo; o terceiro capítulo esboça o caos regulatório da Lei Geral de Proteção de Dados, o caminhar da legislação, as ponderações sobre a vigência, os princípios gerais que formam a estrutura dorsal da lei, em conjunto com os direitos básicos, e as bases legais para o tratamento; já o quarto capítulo trata do consentimento, vale dizer, questiona-se o que se entende por consentimento perante a Lei Geral de Proteção de Dados, o problema da antinomia do consentimento inequívoco *versus* o consentimento expresso, se o consentimento seria uma utopia e o problema da revogação do consentimento.

Com a problematização do consentimento, a dissertação objetivou verificar se o direito à privacidade do titular de dados pessoais está resguardado pelo fornecimento do consentimento de seu titular.

Como se verá, a Lei Geral de Proteção de Dados está estruturada a partir de uma relevância dos dados pessoais, de uma base legal necessária para o tratamento, e da necessidade da observância de inúmeros princípios. A lei tem um encadeamento de medidas de natureza preventiva, desde a promoção de política de governança de dados até o incentivo direito para que empresas e organizações adotem iniciativas proativas preventivas para minimizar riscos e evitar inconformidade no tratamento dos dados pessoais. De outro lado, a lei proporciona um rol de direitos sobre os seus dados (artigos 17 a 22), tais como continuação do tratamento, acesso, retificação, oposição, portabilidade, revogação do consentimento; assim, a Lei Geral de Proteção de Dados é bastante prolixa, de modo que o presente trabalho irá trazer algumas reflexões sobre o consentimento e o direito à privacidade sob a ótica da lei de dados.

1 DA PRIVACIDADE

1.1 DO DIREITO À PRIVACIDADE – DO DIREITO NEGATIVO AO POSITIVO – A PROVÁVEL PREVISÃO CONSTITUCIONAL

Com a evolução das relações sociais, econômicas e políticas, a sociedade torna-se cada vez mais complexa, despontando novos vínculos em razão do desenvolvimento tecnológico e científico, o que, em um olhar a um passado próximo, sequer poderia ser imaginado. O progresso é um motor que impulsiona o desenvolvimento da sociedade e do direito, sendo que este vem na rabeira, ou seja, após surgirem os conflitos, serão eles prescritos e regulados a fim de pacificar as relações decorrentes da evolução, em um ciclo sem fim.

A cada ciclo de evolução surgem novos direitos, a partir de uma nova forma de pensar existente. De tal maneira como a revolução industrial provocou a corrida pela tecnologia, obrigando o direito a regular a propriedade industrial, a inovação tecnológica atual obriga a sociedade a regular a informação, ou melhor, os dados das pessoas naturais, que são o novo motor da sociedade.

Nas palavras de Podestá, “é conhecida a velha lição de que os fatos jurígenos sempre antecedem a normatização, daí porque a compatibilização entre o texto legal e o avanço desenfreado da tecnologia seja o maior desafio.”[1]

Inovações tecnológicas, além de seus atributos intrínsecos que proporcionam um novo vetor para a sociedade, também são dotadas de atributos extrínsecos que transformam o direito. Com a invenção do filme fotográfico em rolo e a fundação da Kodak, George Eastman[2], além de popularizar a fotografia, proporcionou que as pessoas utilizassem sua invenção para os mais variados fins, entre eles, o de registrar a privacidade de terceiras pessoas. A invasão da privacidade, que sequer era considerada um direito a ser protegido, foi o fato gerador do artigo escrito pelos

[1] PODESTÁ, Fabio Henrique. A Privacidade e o Consentimento (Informado) em Face da Nova Lei de Proteção de Dados. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 83.

[2] Em 1874, Eastman ficou intrigado com o jeito de fotografar, considerou o processo complicado e após três anos de experimentação com emulsões de gelatina desenvolveu uma chapa fotográfica seca (cf. INTERNATIONAL PHOTOGRAPHY HALL OF FAME AND MUSEUM. George Eastman: 1854-1932. **IPHF**. Disponível em: https://iphf.org/inductees/george-eastman/. Acesso em: 21 jul. 2020.

advogados estadunidenses Samuel Warren e Louis Brandeis, intitulado *the right to privacy*, no qual defendem o direito de ser deixado em paz (*the right to be let alone*).

No mencionado artigo, os advogados esclarecem que fotografias instantâneas e empresas de jornais invadiram o sagrado ambiente da vida privada e doméstica, sendo que numerosos dispositivos mecânicos ameaçam fazer cumprir a previsão de que "o que é sussurrado no armário deve ser proclamado no telhado"[3], ou seja, conforme o artigo escrito no século XIX, a privacidade começou a ser desrespeitada com o advento da tecnologia.

O artigo de Warren Samuel e Brandeis Louis foi o marco inaugural sobre o direito de privacidade, sendo compreendido, inicialmente, como o direito de ficar sozinho ou *zero relationship*, no qual as pessoas teriam o direito à absoluta ausência de comunicação. Esse direito foi moderado com o passar do tempo, pois a privacidade seria um aspecto fundamental da evolução da pessoa e do desenvolvimento de sua personalidade[4].

Não obstante ter sido concebido como um direito negativo, com caráter formalmente individualista, já que propagava o ideal de ser deixado só, como condição absoluta do Estado não interferir na esfera privada das pessoas naturais, o aludido direito continha ressalvas que permitiriam a divulgação de informações, entre elas: a) o direito à privacidade não seria invadido por nenhuma publicação feita em um tribunal, órgãos legislativos, assembleias municipais, como em qualquer outro órgão de interesse geral; b) não seria exigível reparação se a intromissão não causasse danos e; c) o direito à privacidade cessaria com a publicação dos fatos pelo indivíduo ou com o seu consentimento[5]. Além destas ressalvas que não impediam a divulgação de informações, o artigo destacava que a alegação da veracidade dos fatos não isentaria o agressor da violação, bem como, a ausência de dolo, igualmente, não excluiria a transgressão do direito[6].

---

[3] WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, Dec.15, 1890, Boston. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 21 jul. 2020, p. 2.
[4] DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, ano 4, n. 16, out./dez., 2003, p. 30.
[5] WARREN; BRANDEIS, *op. Cit,* p. 10.
[6] *Ibidem*, p. 11.

Utilizando este fato como parâmetro para o desenvolvimento do raciocínio, a exposição das pessoas aos fatos e a divulgação “boca a boca” sempre existiu, mas, de outro lado, lucrar com a exposição e tornar a amplitude da exposição indefinida a um sem número de pessoas fez exsurgir o direito à proteção da privacidade nos modelos hoje compreendidos, buscando-se estabelecer um equilíbrio entre o que pode ou não ser propagado.

De um direito negativo no século XIX, este direito sofreu uma mutação no decorrer do século XX para ser considerado um direito positivo, devido à alteração da função do Estado, associado à evolução da tecnologia que contribuiu para modificar o conteúdo e o sentido do direito à privacidade[7].

No ordenamento brasileiro não encontra-se propriamente proteção à privacidade, em vez disso, está prescrita a proteção à vida privada, tendo a Constituição Federal disposto que “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” (art. 5°, X) e, de outra forma, o Código Civil prescreve que “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” (art. 21). Como se nota, trata-se de prescrições relevantes, a uma, por explicitar a proteção de um dos contornos da personalidade e, a duas, por constituir um embrião do que viria a ser a proteção do direito à privacidade.

Mendes sintetiza que o direito à privacidade “transformou-se para fazer emergir a dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado de dados.”[8]

Apesar de consagrada a expressão “proteção de dados pessoais”, faz-se necessário tecer importante esclarecimento no sentido de que esta expressão revela-se claramente equivocada, haja vista que a proteção normativa deve recair, na verdade, sobre a pessoa titular dos dados e não, obviamente, sobre estes[9].

---

[7] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 29.
[8] MENDES, *loc. Cit.*
[9] DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, ano 4, n. 16, out./dez.2003, p. 118.

Por entender que o direito à proteção dos dados pessoais recai sobre o seu titular, mostra-se oportuno questionar sobre qual princípio encontra-se ele relacionado; assim, estaria este princípio vinculado à dignidade da pessoa humana ou se poderia entender como um desdobramento do direito à privacidade, como uma autônoma categoria.

De Lucca e Maciel entendem que a promoção de dados pessoais se acha intrinsecamente ligada ao princípio da dignidade humana:

> [...] e, como tal, inserida inquestionavelmente entre os direitos da personalidade, como vem sendo oportunamente assinalado por significativa parte da doutrina - , parecem de pouca serventia os *rios de tinta* que poderiam ser gastos sobre serem tais direitos da personalidade oriundos de uma cláusula geral de proteção da tutela e promoção da pessoa humana ou na mesma linha de raciocínio, decorrentes de um sistema geral de tutela à pessoa humana, ou, numa outra vertente doutrinária, se esses direitos da personalidade são efetivamente constituídos por intermédio de suas diferentes espécies e não a partir de uma cláusula geral de proteção ou de um sistema geral da tutela e promoção da pessoa humana.[10] (grifo do autor).

Ademais, devido a enorme importância do princípio da dignidade da pessoa humana, muito mais que um princípio, este pode ser lançado à categoria de um "meta-princípio", em razão de que "na eventual colisão de princípios constitucionais, inexiste a possibilidade de algum deles prevalecer sobre ele".[11]

Vinculada a proteção de dados pessoais, por irrefutável doutrina, ao princípio da dignidade da pessoa humana, cumpre esclarecer o significado de tão vaga expressão. Nas palavras de Barroso[12], utilizada tanto para "conflitos de vizinhança à proibição de brigas de galo, a dignidade é utilizada como uma varinha de condão que resolve problemas, sem maior esforço argumentativo".

Para solucionar a questão, vale-se mais uma vez da lição de Barroso[13]:

> A dignidade, portanto, é um princípio jurídico de *status* constitucional. Como valor e como princípio, a dignidade humana funciona tanto como justificação moral quanto como fundamento normativo para os direitos fundamentais. Na verdade, ela constitui parte do conteúdo dos direitos fundamentais. Os

---

[10] DE LUCCA, Newton; MACIEL, Renata Mota. A Lei n° 13.709, de 14 de Agosto de 2018: a Disciplina Normativa que Faltava. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 22.
[11] *Ibidem,* p. 25.
[12] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: Os conceitos fundamentais e a construção do novo modelo. 8. ed. São Paulo: Saraiva, 2018, p. 245.
[13] *Ibidem,* p. 246.

> princípios constitucionais desempenham diferentes papéis no sistema jurídico. Destacam-se aqui dois deles: a) o de fonte direta de direitos e deveres; e b) o interpretativo. Os princípios operam como fonte direta de direitos e deveres quando do seu núcleo essencial de sentido se extraem regras que incidirão sobre situações concretas.

De toda sorte, importante considerar que o princípio da dignidade da pessoa humana está prescrito no art. 1°, III, da Constituição Federal, assim localizado no elenco dos princípios fundamentais do Estado Democrático de Direito, tendo sido opção do constituinte de 1988, não incluí-lo no rol dos direitos e garantias fundamentais.

Desta forma, nas palavras de Sarlet, Marinoni e Mitidiero[14]:

> No momento em que a dignidade é guinada à condição de princípio estruturante e fundamento do Estado Democrático de Direito, é o Estado que passa a servir como instrumento para a garantia e promoção da dignidade das pessoas individual e coletivamente consideradas.

Não se pode olvidar que o aludido princípio também é integrante dos princípios gerais da atividade econômica, pois no *caput* do art. 170 há menção que a ordem econômica é fundada na valorização do trabalho humano a fim de assegurar a todos existência digna.

Neste papel de fonte direta de direitos e deveres, pode-se trazer lição de Jabur[15], que assim esclarece:

> O direito constitucional à livre concorrência, arrimo inavegável da ordem econômica nacional (CF, art. 170, V), não abona a obtenção ilícita de dados pessoais nem a entrega de produtos ou serviços que dela ordinariamente decorre sob a invocação de *oferta comercial*. A oferta saudável e revestida de liceidade não se serve de subterfúgios que a preparam (obtenção de dados pessoais à revelia ou à sorrelfa) nem de métodos que a introjetam no domicílio ou ambiente alheio. A privacidade é zona de reserva, é santuário que reclama isolamento, é, numa expressão, círculo do qual participam somente aqueles a quem se quer dar a revelar.

Por outro lado, não se pode deixar de mencionar que o Senado Federal elaborou proposta de Emenda Constitucional de n° 17/2019, na qual o Senador

---

[14] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 4. ed. São Paulo: Saraiva, 2015, p. 257.

[15] JABUR, Gilberto Haddad. A Dignidade e o Rompimento de Privacidade. *In:* MARTINS, Ives Gandra da Silva; PEREIRA JR, Antonio Jorge. **Direito à Privacidade**. 1. ed. Aparecida: Editora Ideias & Letras, 2005, p. 98.

Eduardo Gomes (MDB/TO) sugeriu a inclusão do inciso XII-A, ao art. 5°, e o inciso XXX, ao art. 22, da Constituição Federal, para fazer constar a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Aludida proposta foi aprovada no Senado Federal, por unanimidade, e remetida à Câmara dos Deputados, em 03 de julho de 2019.

Na hipótese desta Emenda Constitucional entrar em vigor, os dados pessoais passarão a ser classificados como um direito fundamental autônomo, sendo desnecessária sua classificação como um direito vinculado ao princípio da dignidade da pessoa humana.

Levando-se em consideração que (i) a proteção dos dados pessoais constitui um direito positivo e recai sobre a pessoa titular dos dados, e não logicamente nos dados; (ii) o ordenamento positivo brasileiro está vinculado ao princípio da dignidade da pessoa humana, o qual se insere entre os princípios fundamentais do Estado Democrático de Direito; (iii) o Estado serve como instrumento para a garantia e a promoção das pessoas individual e coletivamente consideradas; é mister concluir que, entre estas proteções estatais, está inserida a proteção dos dados pessoais.

Desta forma, o modelo jurídico brasileiro de proteção de dados pessoais consiste em uma proteção constitucional, que hoje se encontra lastreada no princípio da dignidade da pessoa humana. Entretanto, caso ocorra a aprovação na Câmara dos Deputados do projeto do Senador Eduardo Gomes (MDB/TO), a Constituição Federal passará a prescrever que os dados pessoais são integrantes do rol de direitos e garantias individuais e coletivos.

1.2 EVOLUÇÃO LEGISLATIVA DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS

A evolução tecnológica permitiu que pessoas tivessem acesso cada vez mais facilitado à telecomunicação e aos microcomputadores. As informações foram no mesmo passo sendo coletadas e transmitidas, o que exigiu a regulamentação da portabilidade de transmissão de tais informações.

Não se pode olvidar que as pessoas têm proteção física e psíquica garantidas pelo ordenamento, mas uma parcela de seus direitos, que são suas informações, não

foram objeto de proteção da mesma maneira, pois sequer eram vistas como bens jurídicos a serem tutelados.

No entender de Mendes[16]:

> [...] as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Por se constituírem uma parcela da personalidade de uma pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade.

Para tanto, não se deve pensar em regular a tecnologia e, tampouco, o seu desenvolvimento, que não pode ser freado e, sequer, imaginado, mas urge regular como será realizada a tradição das informações a fim de preservar a privacidade.

A tecnologia é como um veículo sem freio que atravessa qualquer forma de pensar e rompe qualquer barreira; assim, o foco do ordenamento não deve ser sobre ela, mas sobre o que ela pode ensejar e, a partir deste ponto, regular.

Desta forma, os dados pessoais devem ser entendidos como um direito a ser resguardado, pois figuram como uma parcela da personalidade da pessoa natural, devendo ser resguardado ao cidadão o direito de suas escolhas.

Para Mendes[17], as leis de proteção dos dados pessoais são divididas em quatro gerações, a seguir mencionadas.

A primeira geração teve a Alemanha como país precursor sobre proteção de dados de seus cidadãos, pois desde o ano de 1970 há legislação sobre a matéria no estado de Hesse, tendo a Suécia editado sua lei a partir de 1973, para proteger a pessoa natural contra o abuso no armazenamento, transmissão e exclusão no processamento de dados eletrônicos nas Administrações Públicas e nas empresas privadas.

Oportuno mencionar que as primeiras gerações de leis tinham por intenção tentar regular os bancos de dados de forma *ex ante*, na tentativa de condicionar o seu funcionamento à licença prévia ou a registro nos órgãos competentes, o que deixava

---

[16] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 33.
[17] *Ibidem,* p. 39.

para trás a garantia do direito à privacidade. Portanto, estas legislações buscavam regular procedimentos em vez de garantir direitos.

Devido à incapacidade de proporcionar garantia à privacidade dos cidadãos, a segunda geração de leis buscou normas de proteção de dados pessoais que tratavam prioritariamente sobre o direito à privacidade, em detrimento dos procedimentos. Com a evolução da tecnologia, o temor pelo banco de dados único transmutou diante da existência de inúmeros bancos de dados, o que fez com que as legislações se voltassem a direitos fortes[18].

A grande questão desta segunda geração de direitos é que, ao proporcionar a efetividade do consentimento e o real exercício de sua liberdade de escolha, ocasionava um efeito colateral, qual seja, com a opção pela não disponibilização dos dados, haveria a consequente exclusão social.

Devido a dicotomia existente nas legislações de segunda geração, a nova leva de legislações (terceira geração) buscou solucionar este impasse ao proporcionar discricionariedade do cidadão em todo o processamento de seus dados, promovendo um envolvimento escalonado em todo o processo. Desde a coleta dos dados, passando pelo armazenamento e após a transmissão, a cada degrau era determinada uma autorização, e não apenas com uma única opção de sim ou não[19].

Interessante que, ao ofertar aos indivíduos o direito de participar de todo o processo, a solução não vingou, pois os custos sociais e monetários decorrentes não eram factíveis de serem suportados.

Por último, a quarta geração tentou resolver os problemas das gerações anteriores por meio de duas soluções: a primeira foi a edição de normas que visavam proteger a posição dos indivíduos, tornando mais seguro o controle sobre seus dados pessoais e, a segunda, foi a edição de normas setoriais, de modo que a legislação pudesse contemplar as diversas especificidades setoriais[20].

---

[18] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 40.
[19] *Ibidem,* p. 42.
[20] *Ibidem,* p. 43.

Por se tratar de um tema de interesse quase mundial, a matéria evolui a cada edição de nova lei, sendo de fácil acesso a qualquer estudioso a obtenção de legislação estrangeira.

A título de ilustração, em outubro de 2020, a República Popular da China publicou o seu Projeto de Lei de Proteção de Informações Pessoais (PLPIP)[21], tendo, inclusive, permitido a participação social no debate legislativo de uma lei que se assemelha com a estrutura da Lei 13.709/2018 e com o Regulamento nº 2016/679 (Regulamento Geral Europeu sobre a Proteção de Dados).

Neste sentido, pode-se perceber que as legislações forasteiras caminham para conceder controle aos indivíduos, ou melhor, que os indivíduos tenham maior domínio e possam moderar a informação coletada, armazenada, processada e disseminada[22].

Pelo exposto, pode-se entender que o resguardo da privacidade deve integrar os controles individuais e coletivos de proteção dos direitos fundamentais, sendo que nas palavras de Tepedino e Teffé[23]:

> Quando se controla o tratamento de dados, não se resguarda apenas o indivíduo cujo dados estão relacionados, mas também o grupo social do qual ele faz parte, interesses coletivos e as futuras gerações. Nesse sentido, entende-se que também às coletividades devem ser garantidos meios jurídicos, técnicos e sociais que aumentem seu poder e controle sobre os dados.

---

[21] O projeto de lei da China é composto por 08 (oito) capítulos, 70 (setenta) artigos, e de forma semelhante ao ordenamento jurídico brasileiro e europeu, tratam dos conceitos de: i) informações pessoais, no “Artigo 4: Informações pessoais são todos os tipos de informações registradas por meio eletrônico ou outro meio relacionado a pessoas físicas identificadas ou identificáveis, não incluindo informações após o tratamento de anonimato”; ii) o tratamento “ Artigo 4: O tratamento de informações pessoais inclui a coleta, armazenamento, uso, processamento, transmissão, fornecimento, publicação e outras atividades de informações pessoais”; iii) informações pessoais sensíveis “Artigo 29: Os manipuladores de informações pessoais podem lidar com informações pessoais confidenciais apenas para fins específicos e quando suficientemente necessário. Informações pessoais confidenciais significam informações pessoais que, uma vez vazadas ou usadas ilegalmente, podem causar discriminação contra indivíduos ou graves danos à segurança pessoal ou patrimonial, incluindo informações sobre raça, etnia, crenças religiosas, características biométricas individuais, saúde médica, contas financeiras, localização individual rastreamento etc., entre outras disposições semelhantes. CREEMERS, Rogier *et al.* China's Draft 'Personal Information Protection Law' (Full Translation). **New America,** 2020. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/. Acesso em: 06 fev. 2021.

[22] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 46.

[23] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters. Revista dos Tribunais, 2019, p. 297.

O vetor da liberdade de controle de dados pessoais fundamenta-se no consentimento do titular, que entende-se ser o núcleo duro de todo o sistema de proteção de dados pessoais. Como consequência, para que haja validade no consentimento, há necessidade de que exista liberdade, transparência e especificidade.

1.3 O SIGNIFICADO DA PRIVACIDADE DE ACORDO COM A JURISPRUDÊNCIA

As cortes superiores, mesmo antes do reconhecimento do direito à proteção de dados, já vinham se manifestando no sentido de relacionar o *habeas data* à tutela dos direitos da personalidade, ao direito à intimidade e à autonomia individual, a fim de garantir ao cidadão o direito a obter a informação a ele referente.

O Supremo Tribunal Federal, no julgamento do RHD 22/DF[24], no voto do Min. Sepúlveda Pertence, reconhece o direito material à proteção de dados pessoais, pois segundo seu voto:

> Penso que tudo isso é de transplantar-se para o *habeas data*, que, a rigor, na modalidade do art. 5°, LXXII, *a*, CF/1988 – isto é, para obter ordem à autoridade para fornecer ao impetrante as informações que sobre ele detenha, efetivamente é, no mínimo, remédio perfeitamente análogo ao mandado de segurança, cuja novidade não está no perfil processual do instituto, mas, *sim, no direito substancial ao conhecimento dos dados reclamados* (grifos nossos).

Perante o mesmo recurso[25], cumpre colacionar voto de lavra do Min. Celso de Mello, que descreve sobre os direitos da personalidade:

> Esse tema tem suscitado grande discussão, especialmente porque envolve um dos aspectos mais expressivos da tutela jurídica dos direitos da personalidade.
> A garantia de acesso a informações de caráter pessoal, registradas em órgãos do estado, constitui um natural consectário do dever estatal de

[24] BRASIL. Supremo Tribunal Federal. **Recurso em Habeas-Data: RHD 22 DF**. Relator: Min. Marco Aurélio. Voto do Min. Sepúlveda Pertence. Data de Julgamento: 19/09/1991. Data de Publicação: DJ 01-09-1995, p. 16.
[25] BRASIL. Supremo Tribunal Federal. **Recurso em Habeas-Data: RHD 22 DF**. Relator: Min. Marco Aurélio. Voto do Min. Celso de Mello. Data de Julgamento: 19/09/1991. Data de Publicação: DJ 01-09-1995, p. 3. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=362613. Acesso em: 28 jan. 2021.

> respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade.

Desta maneira, o Supremo Tribunal Federal garantiu, por meio do *habeas data*, a obtenção de um direito material à privacidade, como também a uma ordem democrática mais transparente[26].

No sentido de proporcionar inovações no conceito de privacidade, o Superior Tribunal de Justiça, no julgamento do REsp 22.337-8/RS[27], em voto de lavra do Ministro Ruy Rosado de Aguiar, extraiu constatações da norma sobre banco de dados de proteção ao crédito prevista no art. 43 do Código de Defesa do Consumidor:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com plenos conhecimentos de causa, também pode servir, ao Estado ou ao particular para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, algumas providências já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível das garantias fundamentais, com o direito de autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do ombudsman, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação (Hassemer, "Proteção de Dados", palestra proferida na Faculdade de Direito da UFRGS, 22.11.93). No Brasil, a regra do art. 5~, inc. X, da Constituição de 1988, é um avanço significativo: "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".

---

[26] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 130.

[27] BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Extraordinário 22.337-8/RS**. Data do Julgamento 13/02/1995. Publicado no DJ de 20/03/1995, p. 6119, RSTJ vol. 77, p. 205, Registro nº 92.0011446-6, Relator Ministro Ruy Rosado de Aguiar. Disponível em https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=199200114466. Acesso em: 30 jan. 2021.

Em leitura do aludido voto, pode-se constatar que o foco do Ministro Ruy Rosado de Aguiar foi de alertar que os bancos de dados, por meio de seu gestor, permitem um controle das situações da vida dos indivíduos, sendo que estas informações podem ser usadas de maneira lícita ou ilícita, colocando os cidadãos em situação de vulnerabilidade.

O voto é muito feliz ao prescrever que “o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo”; desta maneira, o voto trouxe luz sobre: a) a ausência de informação sobre o processamento de dados; b) falta de conhecimento que os dados são armazenados e c) impossibilidade de correção e cancelamento dos dados.

2 DOS DADOS PESSOAIS

2.1 O QUE SE PODE ENTENDER POR DADOS PESSOAIS

O significado de dado pessoal é fundamental e determinante para a compreensão do que está dentro ou fora do escopo da lei, razão pela qual afigura-se importante discorrer sobre o seu exato significado e a origem da palavra empenhada na lei.

O legislador brasileiro, em nítida inspiração no Regulamento Geral sobre a Proteção de Dados (RGPD) da comunidade europeia, utiliza a palavra “dado” para designar toda a informação pessoal relacionada a pessoa natural identificada ou identificável (art. 5º, I, Lei 13.709/2018), proporcionando, a princípio, uma certa inquietude ao leitor que tem contato pela primeira vez com o termo.

Como substantivo masculino, “dado” remete, ao cidadão comum, o significado de um pequeno cubo de faces marcadas com pontos e, como adjetivo, ao que não se precisa pagar, por ser gratuito; desta maneira, a expressão “dado pessoal” não estaria de pronto a prestar o devido entendimento de seu real significado.

No entanto, em leitura aprofundada da legislação, o substantivo “dado”, no sentido de conhecimento, demonstra ser a palavra adequada a ser utilizada, em vez do substantivo feminino “informação”, pois, apesar de ambas as palavras possuírem sentidos que se sobrepõem, cada uma possui distinções a serem consideradas.

Expostas tais premissas, cumpre transcrever o entendimento de Doneda[28] sobre o significado de “dado”, veja-se:

> [...] “dado” apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de “pré-informação”, anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza.

[28] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 136.

Portanto, o substantivo “dado” carrega um significado de informação em potencial, que ainda não se desenvolveu completamente, que aguarda uma possível utilização ou trabalho para ser decifrado, ou seja, transmite a amplitude de proteção para uma informação latente, que não se manifesta, que não está aparente, que está oculta, mas mesmo assim é alvo de proteção legislativa.

Por outro lado, o substantivo feminino “informação” remete a algo que está exposto ou revelado, ou seja, com percepção aflorada, com o conhecimento depurado, o que pressupõe uma redução no estado de dúvida.

Pode-se sintetizar que o substantivo “dado” remete a uma proteção de um conhecimento que estaria em estado cru, áspero ou bruto, que não proporcionaria, em uma análise superficial, qualquer significado ou correlação; de outro lado, o substantivo “informação” já ulula a transmissão de um conhecimento, no entanto, não impede que ambos sejam utilizados como sinônimos para uma melhor compreensão da matéria.

Semelhante entendimento é fornecido por Bioni[29], pois o autor compreende que:

> De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação.

Ademais, a palavra “dado” demonstra ser a mais adequada, haja vista que a proteção legislativa abarca a proteção, mesmo que o titular dos dados pessoais não seja identificado, como nos casos em que o controlador ou operador atribuem um identificador eletrônico a uma pessoa natural, sem nenhuma relação com a real identidade da pessoa natural, pois basta que um dispositivo esteja conectado para que se molde toda a navegação do usuário e se forme um perfil de suas atividades.

Inclusive, para a Lei Geral de Proteção de Dados, tem-se por princípio que não existe dado insignificante, razão de ter adotado “o conceito amplo de dado pessoal:

---

[29] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2020a, p. 31-32.

informação relacionada a pessoa natural identificada ou identificável”[30], como a seguir será esclarecido.

2.2 CONCEITO REDUCIONISTA *VERSUS* EXPANSIONISTA DOS DADOS PESSOAIS

Conforme mencionado em tópico anterior, o processo legislativo da atual Lei foi proveniente de anteprojetos de Lei do Executivo, do Ministério da Justiça (PL 5.276/16), do Senado Federal (PL 330/2013, 181/2014 e 131/2014) e da Câmara dos Deputados (PL 4060/2012), os quais, após muito debate, em especial sobre o conceito reducionista ou expansionista de dado pessoal, delimitou seu atual conceito, como mostra-se a seguir.

O artigo 7°, inciso I, da Câmara dos Deputados, definia que dado pessoal era qualquer informação que permita a “identificação exata e precisa” de uma pessoa determinada; desta forma, por esta redação, somente a vinculação direta e imediata com o titular dos dados pessoais estaria debaixo do guarda-chuva da lei.

De outro lado, o projeto de lei do Senado Federal prescrevia no art. 3°, inciso I, que dado pessoal era qualquer informação sobre pessoa natural “identificável” ou “identificada”, da mesma forma que o projeto de lei do Ministério da Justiça, que estabelecia no art. 5°, inciso I, que dado pessoal era o dado relacionado à pessoa natural “identificada” ou “identificável”, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa. Assim, por este entendimento flexível, há uma desconsideração à vinculação exata e precisa, para abranger qualquer tipo de identificação/reconhecimento, ainda que o dado de uma pessoa natural não seja estabelecido de imediato, como nos casos em que os controladores/operadores criam um identificador eletrônico, mas que sejam passíveis de identificação de forma mediata ou indireta.

A importância do conceito reducionista ou expansionista se observa quando da análise do processo de anonimização prescrito no inciso XI, art. 5°, do atual

[30] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters. Revista dos Tribunais, 2019, p. 294.

ordenamento, pois se fosse adotado o critério reducionista, não haveria incidência da lei após o dado ser anonimizado, haja vista que supostamente não haveria identificação exata e precisa da pessoa natural.

Importante esclarecer, por ora, que dados anônimos são a outra face da moeda dos dados pessoais e estabelecem uma falácia, na medida em que discorrem sobre a impossibilidade de reversão de seu processo, proibindo a impossibilidade de associação, direta ou indireta, a um indivíduo. Oportunamente será estudado o processo de anonimização e as suas consequências.

Portanto, o conceito expansionista trabalha com a ideia de pessoa identificável, indeterminada, com vínculo mediato, indireto, impreciso, inexato, em um verdadeiro alargamento da qualificação de dado pessoal. De outro lado, o conceito reducionista trabalha com a ideia de pessoa identificada, específica, determinada, com vínculo imediato, direto, preciso e exato, em um recuo à qualificação de dado pessoal.

Se a lei tivesse adotado o critério reducionista de dado pessoal, somente dados diretos, tais como o número do CPF e do RG, além dos dados biométricos, estariam passíveis de proteção, haja vista que se exigiria uma vinculação imediata, direta e precisa com a pessoa natural.

Neste sentido, a previsão do adjetivo identificável na lei permite que a proteção dos dados pessoais se dê a partir de uma agregação de informação, pela qual as informações esparsas, e a princípio desconexas, são protegidas, pois, a partir do momento em que são tratadas, permitem a identificação exata de uma pessoa natural.

Desta maneira, entende-se acertada a atual legislação que adotou o critério expansionista de dado pessoal, sendo este determinado no artigo 5°, I, como a informação relacionada a pessoa natural “identificada” ou “identificável”.

Para melhor verificar esta afirmação, pode-se sugerir um exemplo hipotético (Tabela 1), no qual as linhas são compostas por dados, e as colunas por atributos, sendo esta uma demonstração de como os dados podem ser organizados de maneira inteligível.

Tabela 1 – Base de dados relacionais[31]

A	B	C	D
Nome	CPF	Idade	Segmentação
Antônio da Silva	123.456.789-00	60	Empresário
Antônio da Silva	987.654.321-00	60	Desempregado

Fonte: Adaptado de Bioni (2015).

A indicação de homônimo, sem que houvesse o apontamento de outros dados personalíssimos, como o CPF, não permitiria identificar qual Antônio da Silva teria a ocupação de empresário ou de desempregado, haja vista que ambos têm a mesma idade. Desta maneira, pelo critério reducionista, haveria a proteção dos dados dos Antônios, pois seus dados são identificados, específicos, precisos e exatos.

Agora, na hipótese de haver a supressão da coluna B, diante da igualdade dos nomes, não haveria a proteção dos dados pessoais de ambos os Antônios, em razão de a pessoa não ser de forma imediata ou diretamente identificável.

Desta maneira, dado pessoal deve ser compreendido dentro de um contexto, pois nem todas as bases de dados podem exprimir exatamente, de forma específica, a que pessoa natural se relaciona, mas diante de uma análise mais apurada, ou diante do cruzamento de banco de dados, estes dados podem ser correlacionados a uma pessoa natural específica, razão do acerto da lei ao determinar a proteção dos dados, mesmo que estes estejam relacionados a pessoa identificável, pessoa indeterminada ou tenham vínculo mediato, indireto, impreciso ou inexato.

No entanto, apesar do acerto da lei em adotar o critério expansionista de dados pessoais, a fim de proporcionar adequada proteção à pessoa natural titular dos dados pessoais, cabe uma crítica à sua redação, haja vista que na redação final não constou o rol exemplificativo, que estava presente no Projeto de Lei do Executivo e explicitava a proteção para os “números indicativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa”.

[31] Bruno Ricardo Bioni utiliza semelhante tabela e o título base de dados relacionais para discorrer sobre o conceito reducionista e expansionista dos dados. BIONI, Bruno Ricardo. **Xeque-Mate**. O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI, USP, 2015. Disponível em: https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 31 ago. 2020.

No ordenamento atual, por ser posterior e, ainda, por ter sido inspirado no Regulamento Geral sobre a Proteção de Dados da comunidade europeia, deveria ter tido mais cuidado a fim de evitar dúvidas, o que poderia ter sido proporcionado com a inclusão de um rol exemplificativo.

O Tribunal de Justiça da União Europeia[32], em 19 de outubro de 2016, foi instado a se manifestar se os protocolos de internet dinâmicos se incluem como dados pessoais, a fim de o usuário ter direito à proteção de seus dados. A decisão do Tribunal foi no sentido de que o protocolo de internet dinâmico de um visitante constitui dados pessoais, no que diz respeito ao operador do site, se esse operador tiver os meios legais que lhe permitam identificar o visitante, ou seja, se houve a ratificação de que os dados identificáveis são passíveis de proteção.

Ademais, se tivesse sido incluído o rol exemplificativo, não haveria necessidade de se utilizar o Decreto do Marco Civil da Internet (MCI) (art. 14, I) a fim de preencher a lacuna observada, haja vista que o objetivo da lei foi o de trazer esclarecimentos e não dúvidas sobre a amplitude de proteção dos dados pessoais.

2.3 A CRENÇA NA EXISTÊNCIA DO DADO ANÔNIMO E O NECESSÁRIO CONTRAPONTO COM A TÉCNICA DA ENTROPIA

O adjetivo “anônimo” pode ser entendido como aquilo que é desprovido de autoria ou o que não leva a assinatura de seu autor, bem como aquilo que não tem nome, sendo esta a intenção da Lei Geral de Proteção de Dados, vale dizer, a de qualificar um dado passível de não ter a guarida da lei, em face de sua impossibilidade de vinculação a uma determinada pessoa natural.

Neste sentido, dado anonimizado é prescrito na lei (art. 5, III) como sendo um “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”; desta forma, este dado não será considerado dado pessoal para fins desta lei (art. 12), salvo

[32] EUROPEAN UNION. **Judgment in Case C-582/14**. Court of Justice of the European Union. “The dynamic internet protocol address of a visitor constitutes personal data, with respect to the operator of the website, if that operator has the legal means allowing it to identify the visitor concerned with additional information about him which is held by the internet access provider”. Luxembourg, 19 oct. 2016. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.pdf. Acesso em: 05 set. 2020.

“quando o processo de anonimização ao qual foram submetidos for revertido, utilizando meios próprios, ou quando, com esforços razoáveis, puder ser revertido”.

A própria lei entende que, para ser considerado anonimizado, um dado deve ser preparado por meio de um processo no qual se retiram informações que tornavam uma pessoa identificada ou identificável.

No entanto, a retirada destes elementos de identificação dos dados passa somente a adjetivar uma informação como anonimizada, sendo que a informação continuará a ser um ativo ao controlador, que poderá utilizar da melhor maneira que sua atividade empresarial necessite, mas sem que seja considerado um dado pessoal passível das proteções da lei geral de proteção de dados.

Neste sentido, o processo de anonimização é um procedimento de boa-fé, que mantém o dado utilizável, mas sem identificar a pessoa natural detentora do dado; assim, o controlador poderá utilizar ferramentas de *business intelligence*[33] sem o risco da exposição de dados.

No entanto, devido ao avanço da tecnologia, a qualificação de um dado como anônimo deve ser visto com ressalvas, pois, devido a capacidade de processamento de informação, tanto do ponto de vista quantitativo, como qualitativo, estes dados podem ser revertidos a partir do cruzamento de dados, razão de a lei ter feito a combinação de duas ressalvas, quais sejam, meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Desta forma, entende-se que a lei exige do controlador que este comprove que o dado anonimizado não seja passível de identificação com a utilização dos meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Nesta esteira, na hipótese de o dado deixar de ser anonimizado, o controlador deverá comprovar que o meio técnico utilizado para sua exposição está além do razoável e, ainda, que o mesmo não estava disponível no período de seu tratamento.

[33] Entende-se necessário utilizar a expressão em inglês para que fosse transmitida a ideia correta do processo de coleta, organização, análise, compartilhamento e monitoramento de informações que oferecem suporte ao negócio, sendo estas ferramentas comercializadas por diversas empresas de tecnologia, em vez da tradução do português (inteligência de negócios), por não exprimir em uma única expressão o significado desejado.

Entende-se que o artigo 5°, III, deverá ser sempre interpretado em conjunto com o artigo 6°, *caput*, que prevê a necessidade da observância da boa-fé para o tratamento de dados, haja vista que o adjetivo “razoável”, previsto para qualificar os métodos de anonimização, é por demais aberto e pode suscitar as mais variadas interpretações acerca do que pode ou não ser considerado como razoável.

Para ilustrar este entendimento, cumpre mencionar o caso da provedora de *streaming* de filmes Netflix, que criou um concurso chamado *Netflix Prize*, segundo o qual os competidores deveriam criar um algoritmo que melhorasse substancialmente a precisão das previsões sobre o quanto alguma pessoa vai gostar de um filme, com base em suas preferências, sendo que o vencedor melhorou o algoritmo em 10% (dez) por cento (Patel).

Para tanto, a Netflix disponibilizou a sua base de dados com as avaliações de seus usuários dos anos de 1998 a 2005, mas os anominizando, pois não forneceu o nome de seus usuários, mantendo somente a data e a nota de avaliação, além de randomizar os dados. A princípio, os dados estavam anonimizados, mas os pesquisadores Narayana & Shmatikov cruzaram estas informações com as de outro sítio da internet (*Internet Movies Databases*/IMDB), o que possibilitou a descoberta da identidade dos usuários do site da Netflix[34].

Neste exemplo de anonimização, acredita-se que a Netflix agiu com boa-fé e tentou se cercar de cautelas a fim de anonimizar os dados, ao retirar o nome dos seus usuários e randomizar os dados de avaliação, mas, pergunta-se: primeiro, este processo de anonimização utilizou métodos razoáveis? E, segundo, este método estava disponível na ocasião do tratamento?

Que o método estava disponível na ocasião do tratamento dos dados de anonimização parece inquestionável, haja vista que foram os próprios participantes do concurso que conseguiram, durante a vigência do concurso, pelo método da

[34] BIONI, Bruno Ricardo. **Xeque-Mate**. O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI, USP, 2015. Disponível em: https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 31 ago. 2020, p. 27-8.

entropia[35] da informação, a vinculação dos supostos dados anônimos às respectivas pessoas naturais.

No entanto, resta resolver a definição do conceito indeterminado de razoabilidade, que para o artigo 12, §1°, se “deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios”, ou seja, para a lei, devem-se considerar fatores como o custo, o tempo e o estado da arte, haja vista que o processo de reversão, em última análise, será sempre possível.

Pela lei, o emprego exacerbado de custo e tempo são fatores objetivos que tornam o dado anonimizado, bem como o emprego de tecnologia de ponta, disponível a somente pouquíssimas empresas no mundo.

Cumpre ressaltar que, ao adotar o critério do razoável, parametrizado por custo, tempo e tecnologia, o legislador deixou a lei atemporal, pois o que é razoável hoje, não o será amanhã, sendo que estes critérios deverão ser calibrados com a tecnologia disponível no tempo de sua análise.

Portanto, com relação à indagação do critério do razoável proposto no exemplo da Netflix, não há critérios seguros para responder na hipótese de análogo problema no Brasil, sob a atual legislação, por não existirem respostas sobre o fator custo, tempo e estado da arte empregados.

De qualquer forma, sintetiza-se o acerto do legislador ao estabelecer um critério objetivo, que utiliza a avaliação do padrão médio da sociedade/empresa, com os parâmetros de custo, tempo e tecnologia, para definir o que pode ou não ser considerado como dado anonimizado.

Por último, não se pode deixar de mencionar que, além dos critérios objetivos, a LGPD, no *caput* do artigo 12, prescreve que o dado poderá ser considerado pessoal, se quem os trata, utilizando meios próprios exclusivos, tem condições de reverter o

[35] A fim de esclarecer, para Bioni, o processo de entropia de uma informação consiste na utilização de uma informação auxiliar para a reversão do processo de anonimização. *Ibidem,* p.28.

processo de anonimização sem a necessidade de esforços ou aportes financeiros em tecnologia.

3 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

3.1 DO CAOS REGULATÓRIO À LEI GERAL DE PROTEÇÃO DE DADOS: HAVIA NO BRASIL UM VAZIO REGULATÓRIO COM RELAÇÃO À PROTEÇÃO DE DADOS?

Antes da promulgação da Lei Geral de Proteção de Dados, havia no Brasil um verdadeiro caos regulatório, em vez de um imaginário vazio, sendo que o excesso de normas esparsas sobre proteção de dados pessoais dificultava em muito a aplicação e os conceitos que deveriam ser considerados.

Entre as principais leis que tratavam do tema proteção de dados, pode-se elencar o Código de Defesa do Consumidor (Lei n° 8.072/90), o Marco Civil da Internet (Lei n° 12.965/14), o Decreto do Marco Civil da Internet (n°8.771/16), a Lei do Cadastro Positivo (Lei Complementar n° 166/19), a Lei de Acesso à Informação (Lei n° 12.527/11), o Decreto da Lei de Acesso à Informação (n° 7.724/12), a Lei do Sigilo das Instituições Financeiras (Lei Complementar n° 105/11), a Resolução do Conselho Monetário Nacional (nº 4.658/2018)[36], o Estatuto da Criança e do Adolescente (Lei 8.609/90) e o Código Brasileiro de Autorregulamentação Publicitária (CONAR), entre outras disciplinas normativas.

Esta estrutura legislativa, nas palavras de Tepedino e Teffé[37], “mostrava-se pouco preciso e não oferecia garantias adequadas às partes, o que, além de gerar insegurança jurídica, acabava tornando o País menos competitivo no contexto de uma sociedade cada vez mais movida a dados”.

---

[36] O Banco Central do Brasil, na forma do art. 9º da Lei nº 4.595, de 31 de dezembro de 1964, torna público as sessões do Conselho Monetário Nacional, com base nos arts. 4º, inciso VIII, da referida Lei, 9º da Lei nº 4.728, de 14 de julho de 1965, 7º e 23, alínea "a", da Lei nº 6.099, de 12 de setembro de 1974, 1º, inciso II, da Lei nº 10.194, de 14 de fevereiro de 2001, e 1º, § 1º, da Lei Complementar nº 130, de 17 de abril de 2009, razão pela qual a sessão do Conselho Monetário Nacional, realizada no dia 26 de abril de 2018, passa a vigorar com o número nº 4.658. BRASIL. **Resolução n. 4658**. Banco Central do Brasil, 26 abr. 2018. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 30 jan. 2021.

[37] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters. Revista dos Tribunais, 2019, p. 290.

A fim de facilitar a compreensão do caos legislativo, colaciona-se a seguir um quadro comparativo de alguns princípios e conceitos que eram tratados em mais de um dispositivo legislativo (Quadro 1)[38].

Quadro 1 - Comparação entre conceitos x Leis ou Decretos

TEMA	CDC	Marco Civil Internet	Decreto MCI	Lei do Cadatro Positivo	Lei Acesso à Informação
Conceito de dados Pessoal			Art. 14, I		Art.4, IV
Banco de dados				Art. 2, I	
Tratamento de dados			Art. 14, II		Art.4, V
Princípio da finalidade		Art. 7,VIII, "c"	Art 13, § 2° , I	Art. 5, VII	
Princípio da minimização		Art. 7,VIII, "a"	Art 13, § 2°	Art. 3, §3°, I	
Princípio da Transparência	Art. 4, caput				Art. 6, I
Informação	Art 43, § 2°	Art. 7,VIII, caput		Art. 3, §2, I	
Princípio da Qualidade	Art 43, §2 1°			Art. 3, §2, III	Art.4, VIII
Consentimento		Art. 7,VII e IX		Art. 4, caput	Art 31, § 2°, I

Fonte: Adaptado de Bioni (2020).

O conceito de dado pessoal é prescrito tanto no Decreto do Marco Civil da Internet (artigo14, I), como na Lei de Acesso à Informação (art. 4°, IV), sendo assim definido por ambos:

> Art. 14, I, dado pessoal – dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;
> Art. 4, IV, informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

Apesar de ambas as leis utilizarem o conceito expansionista de dados pessoais, o Decreto do Marco Civil da Internet amplia ainda mais o conceito para incluir os números identificativos, locacionais ou identificadores eletrônicos, quando relacionados a uma pessoa natural.

De outro lado, o conceito de consentimento utilizado no Marco Civil da Internet é divergente do consentimento exigido na Lei do Cadastro Positivo, pois na primeira exige-se o consentimento volitivo, ao invés da presunção do consentimento existente na segunda. Veja-se:

[38] Adaptado de BIONI, Bruno Ricardo. **LGPD: O Essencial**. Data Privacy Brasil, 2020b. Curso on-line, Módulo II, Parte 2, Cenário prévio: um quebra-cabeça regulatório denominado. Disponível em: < https://dataprivacy.com.br/curso/curso-online-protecao-de-dados-pessoais-muito-alem-da-lgpd/>. Acesso em: 04 set. 2020.

> Art. 7°, VII - 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. 7°, IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> Art. 4º Até 90 (noventa) dias após a data de publicação desta Lei Complementar, os gestores de bancos de dados deverão realizar ampla divulgação das normas que disciplinam a inclusão no cadastro positivo, bem como da possibilidade e formas de cancelamento prévio previsto no § 7º do art. 5º da Lei nº 12.414, de 9 de junho de 2011.
> § 7º O gestor deve proceder automaticamente ao cancelamento de pessoa natural ou jurídica que tenha manifestado previamente, por meio telefônico, físico ou eletrônico, a vontade de não ter aberto seu cadastro.

Com a publicação da Lei Geral de Proteção de Dados, em 14 de agosto de 2018, o vetor de interpretação dos princípios e conceitos deverá ser o de uma lei que fomenta o desenvolvimento econômico e tecnológico, de um lado, e de outro, que visa proteger os direitos e liberdades fundamentais das pessoas naturais, o que por consequência proporciona segurança jurídica.

No entanto, importante mencionar que a LGPD não regula proteção aos dados: (i) das pessoas jurídicas, sendo resguardada a proteção dos dados de seus colaboradores; (ii) das pessoas naturais, quando tratados por pessoas físicas, para fins particulares e não econômicos; (iii) nas hipóteses de tratamento de dados para fins jornalísticos ou acadêmicos; e (iv) para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

3.2 O CAMINHAR DA LEI GERAL DE PROTEÇÃO DE DADOS

As leis de proteção de dados vêm sendo debatidas na Europa e Estados Unidos desde o século passado, sendo que na Alemanha em 30 de setembro de 1970, a primeira Lei de Proteção de Dados do *Land* alemão de Hesse foi promulgada, estando hoje essa disciplina presente de forma objetiva em mais de 140 (cento e quarenta) países, conforme esclarece Doneda[39].

[39] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz; BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2020, p. 3.

Inspirada no direito europeu, a Deputada Federal Cristina Tavares (PMDB-PE) protocolou o projeto de lei nº 2.796, em 05 de maio de 1980[40], para que fosse tratado o tema da proteção de dados no Brasil, com o seguinte título: “Assegura aos cidadãos acesso às informações sobre sua pessoa constantes de bancos de dados e dá outras providências”.

No entanto, o embrião não vingou e o projeto de lei foi arquivado ao final da legislatura, apesar de necessário e conter interessantes previsões que hoje são adotadas, tais como: “Art. 1º É direito de todos os cidadãos conhecer e contestar as informações e as razões utilizadas nos bancos de dados sobre sua pessoa” e “§ 2º do Art. 3º. Para efeito desta lei, considera-se tratamento automatizado de informações nominativas, todo o conjunto de operações realizadas pelos meios automáticos e que permitem, sob qualquer forma, a identificação das pessoas físicas às quais elas se aplicam”.

Não restam dúvidas que o projeto de lei da Deputada pernambucana estava à frente de seu tempo no Brasil, pois utilizou como justificativa à Comissão de Constituição – Comissão Especial Código Civil, temas relevantes, sem parâmetro legislativo no ordenamento jurídico da época, veja-se:

> A informática deve estar a serviço de cada cidadão; não deve constituir ameaça nem à identidade humana, nem aos direitos de cada um, nem à vida privada, nem às liberdades individuais ou públicas.
> Importa que a informática respeite quatro séries de valores, dois tradicionais: os direitos do homem e as liberdades individuais ou públicas e dos mais propalados atualmente: a vida privada e a identidade humana.
> [...]
> A noção de “identidade humana”, primeiro objetivo citado pela nova lei, é o mais novo nos textos. A expressão é hoje utilizada em sociologia, em psicologia e os estudos sobre a cultura e o saber. Identidade se junta à personalidade sem entretanto se confundirem entre si. Refere-se ao que é essencial e singular em cada ser humano de acordo com seu tipo e seu meio. Em relação à informática, a palavra significa que a máquina deve respeitar o nome de cada um e não pode reduzir seus direitos a números anônimos.
> [...]
> A iniciativa não pretende ser a primeira e provavelmente não será a última, mas cremos que o momento é chegado de dar a nosso povo o direito de se precaver contra eventuais ofensas a sua integridade.

[40] BRASIL. **Projeto de Lei 2.796**, Câmara dos Deputados, 1980. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD557906FEB1829EFEA68AED.proposicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 05 fev. 2021.

A brilhante justificativa da Deputada Cristina Tavares, talvez, tenha ressoado no Congresso Nacional de 1980 como o heliocentrismo de Galileu Galilei, haja vista que estavam sendo apresentados conceitos precursores sobre a informática, tratamento de dados e a sua correlação com o direito à privacidade.

Do projeto de lei precursor, transcorreram mais de 20 anos, para somente, a partir da metade do ano 2000, o grupo de trabalho do Mercosul iniciar a discussão sobre a necessidade de uma lei de proteção de dados, ano em que a Argentina promulgou sua lei de proteção de dados[41], tendo sido o primeiro país da "América Latina a adotar uma legislação sobre proteção de dados e criar um órgão responsável pelo controle e pela fiscalização do cumprimento da lei, a denominada *Dirección Nacional de Protección de Datos Personales* (DNPDP)"[42], o que provocou a necessidade de haver um regulamento comum para a proteção de dados.

O Uruguai[43] caminhava para a regulamentação da proteção de dados e o Brasil não tinha uma lei específica que tratasse do tema, sendo este um problema a ser resolvido, em razão da necessária reciprocidade que se exige em blocos econômicos.

No ano de 2009, o Comitê Gestor da Internet no Brasil (CGI.br) publicou o Decálogo da Internet (Resolução CGI.br/RES/2009/003/P), que continha dez princípios que deveriam sinalizar o uso da rede, sendo que seu artigo 1º prescrevia os princípios de liberdade, privacidade e direitos humanos, para que a *internet* fosse guiada pelos "princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática".

No entanto, a discussão se aprofundou no dia 30 de novembro de 2010[44], data em que o Ministério da Justiça abriu a primeira consulta pública sobre o Anteprojeto

---

[41] A Argentina promulgou a *Ley de Protecion de Los Datos Personales* 25.326 em 30 de outubro de 2000, tendo sido sancionada em 4 de outubro de mesmo ano. ARGENTINA**. Proteccion de los datos personales, Ley 25.326**. Buenos Aires: Congreso Argentino, 30 out. 2000. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf. Acesso em: 30 jan. 2021.

[42] LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados Pessoais e a Efetividade da Lei Geral de Proteção de Dados**. São Paulo: Ed. Almedina, 2020, p. 165.

[43] O Uruguai promulgou a *Ley 18.331 – Protección de Datos Personales y acción de Habeas Data* em 11/08/2008, tendo sido sancionada em 18/08/2008. URUGUAI. *Ley 18.331 – Protección de Datos Personales y acción de Habeas Data.* Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 30 jan. 2021.

[44] No sítio eletrônico do Ministério da Justiça é possível consultar as disposições originais, os comentários elaborados em cada artigo, bem como contribuições em artigos .pdf de diversas

de Lei de Proteção de Dados Pessoais, tendo este trabalho sido realizado a quatro mãos por Laura Shertel Mendes e Danilo Doneda.

Em 13 de junho de 2012, o Deputado Federal Milton Monti apresenta um projeto de lei de proteção de dados pessoais (PL 4060/12), mas em julho de 2013 houve um acontecimento mundial de extrema relevância, que foi o escândalo de espionagem revelado por Edward Snowden[45], trazendo à tona que os Estados Unidos, em conjunto com outros países, tinham a capacidade de espionar e vigiar todas e quaisquer pessoas do mundo por meio de comunicações eletrônicas, principalmente através de plataformas de internet, tendo inclusive a Presidente Dilma Rousseff[46] sido espionada.

A partir de outubro de 2013 até abril de 2014, ocorreu uma aceleração do Marco Civil da Internet, que culminou com a sua aprovação, criando um microssistema de proteção de dados pessoais, no âmbito on-line, o que ainda se mostrava tímido, considerando-se que o uso de dados pessoais não se restringe à internet.

Outro fator relevante a acrescentar deu-se no âmbito do Superior Tribunal de Justiça, em voto do Ministro Paulo de Tarso Sanseverino[47], em 12 de novembro de 2014, ocasião em que foi reconhecida a legalidade do *credit scoring*[48].

---

instituições e pessoas naturais. BRASIL. Ministério da Justiça. **Anteprojeto de Lei para a Proteção de Dados Pessoais**. Pensando o Direito. Disponível em: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em: 05 set. 2020.

[45] O analista de sistemas e ex-administrador de sistemas da CIA, tornou público detalhes de vários programas que constituem o programa de vigilância global da NSA. A revelação deu-se através dos jornais *The Guardian* e *The Washington Post*. G1 GLOBO. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA, **Portal G1,** 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 29 ago. 2020.

[46] A Presidente da República Dilma Rousseff, por ocasião do Debate Geral da 68° Assembleia Geral das Nações Unidas, no dia 24 de setembro de 2013, manifestou sua indignação e repúdio ao caso de espionagem sofrido. BRASIL. **Discurso da Presidenta da República, Dilma Rousseff**, por ocasião do Debate Geral da 68ª Assembleia Geral das Nações Unidas. Brasília: Ministério das Relações Exteriores, 2013. Disponível em: https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/presidente-da-republica/presidente-da-republica-federativa-do-brasil-discursos/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas. Acesso em: 28 ago. 2020.

[47] SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp: 1457199 RS 2014/0126130-2**, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 12/11/2014, S2 – Segunda Seção, Data de Publicação: DJe 17/12/2014. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/158643665/recurso-especial-resp-1457199-rs-2014-0126130-2/certidao-de-julgamento-158643667?ref=juris-tabs>. Acesso em: 28 ago. 2020.

[48] Trata-se de uma pontuação de crédito, ou melhor, uma expressão numérica baseada em uma análise de nível dos arquivos de crédito de uma pessoa, para representar a qualidade de crédito de um indivíduo. ESTADO DE MINAS. STJ confirma legalidade de sistema de score de crédito. **Jornal Estado de Minas**, 2014. Disponível em:

De 2014 a 2015, sucedeu o reinício das discussões da Lei Geral de Proteção de Dados pessoais, o que carreou no ano 2015 em nova consulta pública (28/01/2015), que culminou em 20 de outubro de 2015 com um novo anteprojeto. Em 2016, foi levado à Câmara dos Deputados um anteprojeto de lei, sendo este um dos últimos atos da Presidente Dilma Rousseff, que foi aglutinado a outros projetos de lei que discutiam sobre a mesma matéria: PL 4060/2012 e PL 5276/2016 (Câmara dos Deputados) e o PLS 330/2013 (Senado Federal). Entre 2016 e 2018, houve mais de 13 audiências públicas.

Devido a 04 (quatro) fatores que reputam-se relevantes, a lei de proteção de dados foi sancionada em 14 de agosto de 2018, com data prevista para entrar em vigor após 18 (dezoito meses) de sua publicação oficial (art. 65 – redação original), ainda sem ter a atual denominação de Lei Geral de Proteção de Dados, designação esta obtida somente por meio da Lei n° 13.853, de 8 de julho de 2019.

O primeiro fator externo a contribuir com a promulgação da lei brasileira de proteção de dados foi a entrada em vigor do Regulamento Geral sobre a Proteção de Dados da União Europeia, em 25 de agosto de 2018, haja vista que esta lei tem aplicação extraterritorial, o que levou inúmeras empresas brasileiras a se adequarem.

O segundo fator extrínseco a contribuir com a promulgação da referida lei foi a revelação de outro escândalo, mas este da empresa privada de mineração e análise de dados Cambridge Analytica[49], que coletou dados pessoais nas plataformas de rede social do mundo, sendo que inicialmente estes dados coletados tinham fins triviais, para análise da personalidade, mas que acabaram sendo utilizados para finalidades completamente diferentes. Nos Estados Unidos, foram coletados dados de mais de 70 milhões de pessoas, sendo estes dados utilizados para o envio de publicidade direcionada, que ficou conhecido como *microtargeting*[50]. No Reino Unido, suspeita-se

---

https://www.em.com.br/app/noticia/economia/2014/11/12/internas_economia,589362/stj-confirma-legalidade-de-sistema-de-score-de-credito.shtml. Acesso em: 13 set. 2020.

[49] Esta empresa foi criada em 2013 para participar de campanhas políticas nos Estados Unidos, tendo participado em 44 pleitos eleitorais. No ano de 2016 trabalhou na campanha presidencial de Donald Trump e também para o Brexit, visando a saída do Reino Unida da União Europeia. INGRAM, David. Factbox: Who is Cambridge Analytica and what did it do? **Reuters**, 2018. Disponível em: https://www.reuters.com/article/idUSKBN1GW07F. Acesso em: 29 ago. 2020.

[50] Técnica usada frequentemente por partidos políticos e campanhas eleitorais que inclui marketing direto, que envolve segmentação de mercado para rastrear eleitores individuais e identificar possíveis apoiadores. ISSENBERG, Sasha. How Obama's Team Used Big Data to Rally Voters. **MIT, Technology Review,** 2012. Disponível em:

que a utilização do *microtargeting* tenha sido responsável pela saída do país da União Europeia, e nos Estados Unidos, tenha resultado na eleição do presidente Donald Trump. Essa empresa supostamente estava preparada para prestar seus serviços para a eleição presidencial no Brasil, sendo que, após estas revelações, vários parlamentares se manifestaram sobre a necessidade de ter uma lei que regulasse os dados pessoais.

O terceiro fator a influenciar foi intrínseco, pois refere-se a tentativa de o Brasil ingressar para a Organização para a Cooperação e Desenvolvimento (OCDE), haja vista que esta exige, desde o ano de 1980, *guidelines* para a transferência de dados pessoais e uso apropriado a esses dados. Para ingressar na OCDE, o país membro tem que se adequar e garantir que irá seguir as orientações. O fato de não ter a proteção de dados dificultava muito o ingresso na OCDE.

Por último, o quarto fator, também interno, refere-se às tentativas de alterações da lei do cadastro positivo. A lei do cadastro positivo, quando aprovada em 2011 (Lei n° 12.414, de 9 de junho de 2011), determinava a necessidade de consentimento expresso do titular, para que seus dados de adimplência pudessem ser alocados em uma base de dados (art. 2°, III, redação original[51]). Devido a esta imposição legal, a adesão ao cadastro positivo, por meio do consentimento expresso, era muito baixa, inferior ao desejado pelas instituições financeiras, o que levou a uma discussão sobre a desnecessidade do consentimento prévio, bastando uma adesão automática ao cadastro positivo, mas com o direito de oposição (art. 5°, I, Lei n° 12.414, de 9 de junho de 2011), o que implicaria imediata transferência de mais de 100 (cem) milhões de dados dos brasileiros economicamente ativos. Em uma discussão de fundo de vários agentes, chegou-se à conclusão de que antes de colocar automaticamente todos os dados dos brasileiros no cadastro positivo, deveriam ser discutidas primeiro regras e direitos adequados aos titulares, no âmbito de uma lei de proteção de dados pessoais, para depois se discutir o cadastro positivo. Esta alteração, no entanto, só ocorreu quase 8 (oito) anos depois, com a promulgação da Lei Complementar n° 166, de 8 de abril de 2019.

---

https://www.technologyreview.com/2012/12/19/114510/how-obamas-team-used-big-data-to-rally-voters/. Acesso em: 29 ago. 2020.

[51] BRASIL**. Lei 12.414, de 9 de junho de 2011**. Art. 2°, III, cadastro: pessoa natural ou jurídica que tenha autorizado inclusão de suas informações no banco de dados (redação revogada pela Lei Complementar n° 166, de 2019);

3.3 PONDERAÇÕES SOBRE A DATA DE VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

Feitos estes esclarecimentos sobre a necessidade de uma lei de proteção de dados pessoais, cumpre ainda indicar os fatores intrínsecos e extrínsecos que levaram à prorrogação da vigência da lei, os quais lembram a odisseia vivida pelo grego Ulisses, no poema escrito por Homero.

No entanto, Ulisses era um personagem da mitologia grega que narrava personagens ou seres que incorporavam as forças da natureza e as características humanas, em teor fantástico e simbólico, do qual o Brasil não consegue se desvincular.

Barroso, em primorosa síntese[52], esclarece, com base no desenvolvimento da nação brasileira, a razão de perdurar até os dias de hoje a confusão legislativa, o descaso e a falta de seriedade no emprego das diretrizes de governo:

> Começamos tarde. Somente em 1808 – trezentos anos após o descobrimento -, com a chegada da família real, teve início verdadeiramente o Brasil. Até então os portos eram fechados ao comércio com qualquer país, salvo Portugal. A fabricação de produtos era proibida na colônia, assim como a abertura de estradas. Inexistia qualquer instituição de ensino médio ou superior: a educação resumia-se ao nível básico, ministrada por religiosos. Mais de 98% da população era analfabeta. Não havia dinheiro e as trocas eram feitas por escambo. O regime escravocrata subjugava um em cada três brasileiros e ainda duraria mais oitenta anos, como uma chaga moral e uma bomba-relógio social. Pior que tudo: éramos colônia de uma metrópole que atravessava vertiginosa decadência, onde a ciência e a medicina eram tolhidas por injunções religiosas e a economia permaneceu extrativista e mercantilista quando já ia avançada a Revolução Industrial. Portugal foi o último país da Europa a abolir a inquisição, o tráfico de escravos e o absolutismo. Um império conservador e autoritário, avesso às ideias libertárias que vicejavam na América e na Europa.
> Começamos mal. Em 12 de novembro de 1823, D. Pedro I dissolveu a Assembleia Geral Constituinte e Legislativa que havia sido convocada para elaborar a primeira Constituição do Brasil. Já na abertura dos trabalhos constituintes, o Imperador procurava estabelecer sua supremacia, na célebre "Fala" de 3 de maio de 1823. Nela manifestou sua expectativa de que se elaborasse uma Constituição que fosse digna e merecesse sua imperial aceitação. Não mereceu. O Projeto relatado por Antônio Carlos de Andrada, de corte moderadamente liberal, limitava os poderes do rei, restringindo seu direito de veto, vedando-lhe a dissolução da Câmara e subordinando as Forças Armadas ao Parlamento. A constituinte foi dissolvida pelo Imperador

[52] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: Os conceitos fundamentais e a construção do novo modelo. 8. ed. São Paulo: Saraiva, 2018, p. 373-374.

> em momento de refluxo do movimento liberal na Europa e de restauração da monarquia absoluta em Portugal. Embora no decreto se previsse a convocação de uma nova constituinte, isso não aconteceu. A primeira Constituição brasileira – a Carta Imperial de 1824 – viria a ser elaborada pelo Conselho de Estados, tendo sido outorgada em 25 de março de 1824.
> Percorremos um longo caminho. Pouco mais de duzentos anos separam a vinda da família real para o Brasil e a comemoração do vigésimo quinto aniversário da Constituição de 1988.

E apesar deste longo percurso, tendo começado tarde e começado mal, vem o pior, vale dizer, ainda permanece-se mal.

A presente dissertação está sendo escrita nos anos de 2020 e 2021, período em que estão sendo sentidos os efeitos do "cometa" que caiu no planeta Terra, chamado COVID-19, que abalou as estruturas da economia de muitos países, o que permite perceber o quão estruturado está um Estado, em razão dos tremores que as mudanças de paradigmas proporcionaram.

Este simples protesto demonstra o quanto o Brasil permanece confuso, sem diretrizes, com ações atabalhoadas e que acarretam prejuízos incalculáveis para todos os seus cidadãos. Em pesquisa do Lowy Institute[53], que compilou um estudo com as respostas de 98 (noventa e oito) países à Covid-19, avaliou-se que o Brasil teve o pior desempenho entre todas as nações do grupo, tendo sido levados em conta dados do total de casos e mortes em cada nação, a oferta de testes e o percentual da população afetada pela pandemia. A título de ilustração, na América do Sul, inclusive o Brasil ficou atrás do Paraguai e da Bolívia, sendo que estes tiveram média no estudo de 40,9 e 18,9, respectivamente, e o Brasil no incrível último lugar com 4,3.

Para não creditar razão, somente sob uma perspectiva, das ações de descaso do governo em face do cidadão, a OCDE[54] elaborou um estudo e constatou que o Brasil é dos países com mais tempo sem aula por causa da pandemia, o que irá acarretar uma defasagem educacional a ser sentida em décadas. Em leitura ao estudo, é possível constatar que "a perda do aprendizado reflete em perdas de habilidades, isso reflete na produtividade. O impacto relativo sobre o PIB pode ser de 1,5% em média até o final do século."

---

[53] LOWY INSTITUTE. Covid Performance Index. Deconstructing Pandemic Responses. **Lowy Institute,** 2021. Disponível em: https://interactives.lowyinstitute.org/features/covid-performance/. Acesso em: 03 fev. 2021.

[54] OECD. Education at a Glance 2020. **OCDE**, 2020, on-line. Disponível em: https://www.oecd.org/education/education-at-a-glance/. Acesso em: 03 fev. 2021.

Toda esta introdução se justifica para que se possa afirmar que, no tocante ao objeto de estudo desta dissertação, o *modus operandi* não foi diferente, ou seja, começou-se tarde e começou-se mal.

Como já mencionado, a Lei Geral de Proteção de Dados foi publicada no dia 14 de agosto de 2018, sendo prescrito no artigo 65 (redação original) o prazo de vacância de 18 (dezoito) meses, o que acarretaria seu início de vigência para o dia 14 de fevereiro de 2020.

No entanto, em 27 de dezembro de 2018, o Presidente Michel Temer, ao criar a Agência Nacional de Proteção de Dados (ANPD), por meio da Medida Provisória nº 869, alterou parcialmente o início de vigência da lei, ou seja, quanto à ANPD, o início dar-se-ia em 28 de dezembro de 2018 e, quanto aos demais artigos, decidiu-se postergar sua vigência por mais 06 (seis) meses, devido à complexidade que a lei exige para sua adequação, ou seja, uma mudança intrínseca que tornou o prazo semelhante ao da *vacatio legis* da RGPD.

Importante constar que a Medida Provisória nº 869 foi convertida na Lei nº 13.853, de 8 de julho de 2019, mas este processo de conversão da Medida Provisória em Lei não alterou, por mais surpreendente que possa parecer, a data de vigência da lei, que em seu artigo 65 manteve a data de vigência da Medida Provisória, ao assim prescrever[55]:

> Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019) I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019) (grifos nossos).

Nas palavras de Newton De Lucca, o legislador cometeu um *lapsus calami*, já que poderia ter tido a intenção de prescrever 2019 ou 2020, mas nunca 2018, haja vista que a lei é de 2019. Inclusive, este erro poderia ter sido reparado na lei 14.010/20, mas também não o foi.

Entretanto, o ano de 2020 apresentou à população mundial as consequências de uma pandemia jamais vista, pois o COVID-19 acarretou o afastamento social e,

[55] Arguta observação feita pelo Prof. Dr. Newton De Lucca, em banca de qualificação deste mestrando, realizada em 16/11/2020, que contou com a participação do Prof. Dr. Bruno Dantas Nascimento e do Prof. Dr. Guilherme Amorim Campos da Silva.

por consequência, a necessidade de se pensar na prorrogação da entrada em vigor da LGPD, haja vista que a lei, além dos custos de sua implantação, exige o treinamento de pessoas, as quais estavam em situação de isolamento.

Esse fator extrínseco de extrema relevância foi o fato gerador de 02 (duas) propostas legislativas que tramitaram paralelamente no Congresso Nacional, objetivando a alteração da data de vigência da lei.

De iniciativa do Poder Executivo, a Medida Provisória 959, de 29 de abril de 2020[56], prorrogava a vigência da lei para o dia 03 de maio de 2021, por entender que as consequências econômicas da pandemia iriam prejudicar o cumprimento e adequação das empresas às exigências da lei de proteção de dados.

A outra proposta, de autoria do Senador Antonio Anastasia (PSD/MG), que tramitou no Congresso Nacional, sugeriu a criação do Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado (RJET), ou seja, o Projeto de Lei n° 1.179/2020, que prorrogava a vigência da Lei Geral de Proteção de Dados por mais 18 (dezoito) meses[57], "de modo a não onerar as empresas em face das enormes dificuldades técnicas econômicas advindas da pandemia".

Portanto, tanto o Poder Executivo, como o Poder Legislativo, este por meio do Senado Federal, estavam uníssonos quanto à necessidade de prorrogação da vigência da Lei, por entenderem que as consequências da pandemia afetariam o atendimento dos requisitos legais.

No entanto, conquanto os Poderes da República concordassem com a necessidade de uma prorrogação, isto não significa que esta tenha ocorrido nos moldes propostos, haja vista que "o Brasil não é para principiantes", conforme popular frase do maestro Tom Jobim.

Entre os meses de abril e maio de 2020, o Congresso Nacional apreciou o RJET (Projeto de Lei n° 1.179/20), que foi convertido na Lei 14.010, de 10 de junho de 2020, que assim prescreveu: Art. 65, I-A – dia 1° de agosto de 2021, quanto aos arts. 52, 53

---

[56] A exposição de motivos da Medida Provisória 959, assinada pelo Ministro Paulo Roberto Nunes Guedes, em seu artigo 10, prescreve que "o adiamento da entrada em vigor dos dispositivos previstos na Lei Geral de Proteção de Dados em consequência de uma possível incapacidade de parcela da sociedade em razão dos impactos econômicos e sociais da crise provocada pela pandemia do Coronavírus".

[57] SENADO FEDERAL, **Projeto de Lei n° 1179/2020**, Justificação, inciso x.

e 54 (dispositivos que regulam as sanções) e, ii) quanto a vigência dos demais artigos decidiu-se por manter o prazo da Medida Provisória n° 869.

Com a conversão em Lei do Projeto do Senado Federal, ainda tramitava a Medida Provisória n° 959 de iniciativa do Poder Executivo; desta forma, a Câmara dos Deputados, em 25 de agosto de 2020, aprovou o projeto com uma alteração em seu artigo 4°, para que o início de vigência da LGPD se desse no dia 31 de dezembro de 2020.

Interessante observar: i) no dia 10 de junho de 2020 entra em vigor a lei 14.010/20, que determina o prazo de vigência da LGPD para o dia 16 de agosto de 2020, sendo que ainda há no Congresso uma Media Provisória que pode prorrogar a sua vigência e, ii) no dia 25 de agosto, precisamente, 11 (onze) dias após a suposta vigência determinada pela Lei 14.010/20, vota-se na Câmara dos Deputados a prorrogação para o dia 31 de dezembro de 2020.

A princípio, tudo caminhava para a prorrogação da vigência para o dia 31 de dezembro de 2020; no entanto, o Senado Federal, ao apreciar a matéria no dia 26 de agosto de 2020, último dia antes de caducar a Medida Provisória n° 959, aplicou o artigo 334, II[58], de seu Regimento Interno, que classifica a matéria como prejudicada, em virtude de seu prejulgamento pelo Plenário em outra deliberação.

Em outras palavras: como o Senado Federal já havia decidido sobre a matéria na votação do RJET (Projeto de Lei n° 1.179/20), este tema não poderia ser objeto de apreciação, o que acarretou no dia 26 de agosto de 2020 a sua não apreciação e, por consequência, a previsão de entrada em vigor da LGPD para o dia 16 de agosto de 2020.

Neste sentido, com a impossibilidade de se apreciar a prorrogação da lei para o dia 31 de dezembro de 2020, o imbróglio surgiu, pois se questionou, primeiro, se a lei já estava em vigor, e, segundo, com a sanção ou veto presidencial, a lei teria a sua vigência retroagida?

---

[58] BRASIL. Senado Federal. **Regimento Interno**, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/regimento-interno. Acesso em: 20 set. 2020.

Devido à ambiguidade de interpretações, a assessoria de imprensa do Senado Federal publicou uma nota de esclarecimento[59] segundo a qual a LGPD entraria em vigor apenas após a apreciação do projeto de lei de conversão do Presidente da República, com fundamento no artigo 62, § 12 da Constituição Federal, o que poderia levar 15 (quinze) dias úteis.

Neste sentido, em 18 de setembro de 2020 entrou em vigor a lei 14.058, que converteu a Medida Provisória n° 959 e, por consequência, iniciou a vigência da Lei Geral de Proteção de Dados Pessoais.

3.4 DOS PRINCÍPIOS GERAIS – O ESPÍRITO DA LEI E OS VERDADEIROS FUNDAMENTOS

A Lei Geral de Proteção de Dados prescreve no art. 6°que “as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios”, sem, contudo, explicitar se a boa-fé configuraria mais um princípio a ser observado e, ainda, se a boa-fé teria natureza subjetiva ou objetiva.

A boa-fé ainda está presente em mais duas oportunidades na lei: a primeira, quando regula tratamento de dados pessoais cujo acesso é público (art. 7°, §3°); e a segunda, como critério de gradação de sanção (art. 52, §1°, II), sem, contudo, esclarecer a sua natureza jurídica.

Ademais, não se pode olvidar que na atual sociedade da informação, o compartilhamento de dados, apesar de inevitável, precisa ser delimitado, sendo a boa-fé uma importante ferramenta para este exercício.

De ordem constitucional, pode-se dizer que a privacidade é garantida pelo artigo 5°, X, isto sem mencionar o art. 12 da Declaração Universal dos Direitos Humanos e o art. 21 do Código Civil, que classificam a vida privada da pessoa natural como inviolável.

De outro lado, como proteção do interesse coletivo, a liberdade de acesso à informação é garantida pelo art. 5°, XIV, da Constituição Federal, já que assegura a

---

[59] BRASIL. Senado Federal. **Assessoria de Imprensa**, 2020. Disponível em https://www12.senado.leg.br/assessoria-de-imprensa/notas/nota-de-esclarecimento-vigencia-da-lgpd. Acesso em: 20 set. 2020.

todos o acesso à informação, sendo resguardado o sigilo da fonte, quando necessário ao exercício profissional.

Portanto, de um lado tem-se o direito à privacidade, que confere abrigo à proteção individual da privacidade e, de outro, a liberdade de acesso à informação, como garantia de manutenção das relações sociais; assim, neste contexto, insere-se a Lei Geral de Proteção de Dados para regular o conflito entre estes interesses, aparentemente, antagônicos.

Não se pode negar que "tal como a luz, os dados são um recurso renovável e não-rival. O uso correto de dados fomenta a inovação em todos os setores da economia"[60], razão pela qual estes podem ser classificados como remuneráveis, sendo legítimo o interesse, nesta "troca cambial", entre a pessoa natural e a entidade controladora dos dados.

Neste ponto, importante trazer lição de Senise Lisboa[61] sobre o tema:

> Muito embora o compartilhamento de dados seja uma das diretrizes da sociedade da informação, razões de ordem pública e de interesse social justificam a delimitação dessa atividade, proporcionando-se ao intérprete a análise da regra implícita de conduta (boa-fé objetiva) que as partes deverão ter a respeito do uso e tratamento de dados, levando-se em consideração as circunstâncias do caso.

Desta maneira, vale mencionar o artigo 113 do Código Civil, que prescreve o princípio da boa-fé como aplicável ao negócio jurídico, incluindo-se o contrato (art. 422).

Para tanto, cabe aqui invocar, mais uma vez, o diálogo das fontes e utilizar o entendimento já consolidado sobre a boa-fé no Código de Defesa do Consumidor - lei de natureza principiológica, constitucional, de tutela dos vulneráveis[62] - em razão da assimetria de forças existente entre os contratantes, em semelhança com a disparidade de poderio entre a pessoa natural e controlador de dados, em regra.

---

[60] LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 328.

[61] LISBOA, Roberto Senise. Boa-fé e Confiança na Lei Geral de Proteção de Dados Brasileira. **Revista do Advogado**. AASP. São Paulo, n°144, nov.2019, p. 76-77.

[62] MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman de Vasconcellos; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor.** 2. ed. Porto Alegre: Editora Revista dos Tribunais, 2006, p. 30-36.

A natureza objetiva da boa-fé pode ser entendida como a exigência de um comportamento de lealdade dos participantes negociais, em todas as fases do tratamento de dados, ou seja, fase pré-tratamento, fase do tratamento e fase pós-tratamento, haja vista que os princípios abarcam todas estas fases negociais[63].

A boa-fé objetiva, inclusive, está relacionada com os deveres laterais ou anexos de conduta, que são deveres inerentes a qualquer contrato, sem a necessidade de previsão no instrumento; entre eles, estão: dever de cuidado, respeito, informação, colaboração ou cooperação, transparência, confiança e o de agir com razoabilidade[64].

Pela amplitude da boa-fé, que versa sobre o comportamento dos participantes da relação jurídica, em todas as fases do tratamento de dados e, ainda, abarca os deveres laterais de conduta, esta deve ser tratada como mais um princípio a ser cumprido por todas as partes envolvidas, devendo ser classificada como de natureza objetiva, por ser a probidade dos participantes uma exigência a ser observada.

Devido a amplitude da boa-fé, por sua relação de complementariedade, deve ser entendido que a Lei Geral de Proteção de Dados possui onze, em vez de dez princípios a serem cumpridos, sob pena de os dados serem tratados em desconformidade.

Por abarcar uma relação de complementariedade, a boa-fé deve ser analisada nas circunstâncias concretas, para que se possa verificar se a entidade controladora dos dados atuou de forma a atender as legítimas expectativas da pessoa natural, haja vista que não existe uma equação simples em que se possa formatar o cumprimento da boa-fé.

De outro lado, não se pode olvidar que os demais princípios representam o espírito da lei e todos atuam em sinergia, em ação simultânea e coletiva de cooperação, para que o titular dos dados pessoais tenha controle sobre as suas informações, e que sua legítima expectativa não seja frustrada quando do tratamento de dados pelo agente de tratamento.

---

[63] GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil**. Contratos: Teoria Geral. v. IV, t. 1, 5. ed. São Paulo: Editora Saraiva, 2009, p. 64-66.
[64] TARTUCE, Flávio. **Direito Civil:** Teoria Geral dos Contratos e Contratos em Espécie. 4. ed., v. 3. São Paulo: Editora Método, 2009, p. 115-131.

Desta maneira, entende-se que a ausência de cumprimento de um único princípio, além da boa-fé prescrita no *caput*, não legitimaria o tratamento dos dados, pois todos atuam em consonância, acarretando um tratamento de dados em desconformidade com a lei.

Diante do exposto, cumpre mencionar que são 10 (dez) os princípios expressos da Lei Geral de Proteção de Dados, que serão a seguir tratados.

O princípio da finalidade (art. 6°, I) é previsto no ordenamento como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;" e por isso pode-se entender que os propósitos do tratamento precisam ser bem especificados, ou delimitados ou delineados, não sendo admitida a usual expressão de que os dados serão tratados para "melhorar a experiência".

Neste sentido, é preciso envolver o tratamento de dados ao propósito específico para o qual foi autorizado, limitando a finalidade do tratamento e impossibilitando-a de ser desviada.

De outro lado, o princípio da adequação (art. 6°, II) é descrito como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;"

Consonante ao princípio da adequação, está o princípio da necessidade (art. 6°, III), definido como a "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;"

Pelo princípio da adequação e da necessidade, é de se questionar a relação da pessoa natural com a funcionalidade do tratamento de dados; vale dizer, analisar se o aplicativo ou programa que irá tratar os dados está coletando a menor quantidade de dados possível e, mais, se esta coleta é adequada para justificar o tratamento, o propósito que se visa buscar.

A título de ilustração, um aplicativo de bússola, para um aparelho de celular, não poderia solicitar autorização para acessar a lista de contatos do titular do aparelho, pois, primeiro, não seria adequado ao tratamento e, segundo, não haveria necessidade pelo propósito da função que se busca obter.

Outro princípio prescrito é o do livre acesso (art. 6°, IV), que determina a "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"; assim, por este princípio, o titular dos dados tem o direito de requisitá-los e verificar se os dados estão sendo tratados de maneira adequada.

Pelo princípio da qualidade dos dados (art. 6°, V), que estipula a "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", em conjunto com o princípio da transparência (art. 6°, VI), que garante 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;" deve ser compreendido, por parte do controlador ou operador (titular dos dados), que há uma obrigação de informar com qualidade, e de forma facilitada, como irá conseguir exercer este tipo de controle.

Outro princípio extremamente relevante é o da segurança (art. 6°, VII), definido como a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;"

Este princípio destina-se a proteger a segurança da informação, ou seja, o local em que os dados serão armazenados, guardados, para serem manipulados com segurança. Apesar da legislação brasileira ser nova, e ter acabado de entrar em vigor, não foi objeto de preocupação do legislador a exigência de armazenamento dos dados território pátrio, principalmente pelo fato de a legislação europeia, igualmente, não prever referida obrigação.

Devido à diária evolução da tecnologia, o aplicativo de vídeo TikTok, da controladora ByteDance Ltd., entrou no radar do governo americano, que o acusa de transferência indevida de dados para o Governo Chinês.

Em decorrência do alerta do governo americano, o Reino Unido, igualmente, se mobilizou e questionou a TikTok, por meio de seu diretor de relações políticas e governamentais, Theo Bertram, se o *data center* que está sendo construído na Irlanda, ao custo de €420 milhões de euros, irá abrigar inclusive os dados retroativos, haja

vista que até a sua implantação, os dados dos europeus estão alocados nos Estados Unidos e Cingapura[65].

Referida preocupação é legítima, pois cada país deve zelar pelos dados de seus cidadãos, sendo que estes dados devem estar armazenados sob sua jurisdição, para que possa ser conferida a segurança prescrita neste princípio.

Sob esta ótica, em 25 de setembro de 2020, o Deputado Federal Luiz Philippe de Orleans e Bragança (PSL-SP), autor do Projeto de Lei 4.723/2020[66], propõe a alteração do artigo 3°, da Lei 13.709/2018, para que seja acrescido o inciso IV, que irá determinar: "os dados de que trata esta lei sejam armazenados e mantidos fisicamente em repositório situado em território nacional".

Como justificativa[67] do projeto, é mencionada a necessidade "de preservação dos direitos fundamentais de seu titular e os princípios da soberania e segurança nacional", em razão da Lei 13.709/2018 ter deixado "implícito o local de guarda e armazenamento físico ou virtual (nuvem) do objeto em questão".

Outro princípio que não pode deixar de ser mencionado é o da prevenção (art. 6°, VIII), que determina a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

Com este princípio, "foram incorporados e positivados, aqui, assim como ocorreu no Regulamento europeu, os pilares da chamada proteção da privacidade e dos dados pessoais por design e por padrão"[68], motivo pelo qual se pretende antever os riscos à violação da privacidade, com os objetivos de evitar os danos à pessoa natural, o tratamento abusivo de informações e o vazamento dos dados.

---

[65] STOLTON, Samuel. **TikTok unclear on how old EU data will be transferred to new Irish data centre**. Euractiv.com, 23 set. 2020. Disponível em: https://iapp.org/news/a/tiktok-clarifies-plans-for-eu-info-when-irish-data-center-launches/. Acesso em: 07 out. 2020.

[66] CÂMARA DOS DEPUTADOS. **Projeto de Lei 4723/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2263413. Acesso em: 07 out. 2020.

[67] CÂMARA DOS DEPUTADOS. **Projeto de Lei 4723/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=8DC96910BEB329A6F823902348BE5879.proposicoesWebExterno1?codteor=1932527&filename=PL+4723/2020. Acesso em: 07 out. 2020.

[68] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 294.

Por este princípio, pode-se entender que os algoritmos não podem reforçar práticas discriminatórias, em uma lógica de prevenção de danos; portanto, em oposição à correção de danos, pois o "ecossistema" da lei gira em torno da precaução.

Outro princípio elucidativo é o da não discriminação (art. 6°, IX), que propaga a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos".

Por último, a lei prescreve o princípio da responsabilização e prestação de contas (art. 6°, X), pelo qual deve haver a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Princípio novo no ordenamento jurídico, segundo o qual a entidade que irá tratar os dados pessoais deverá adotar medidas e práticas eficientes para estar em conformidade com a lei.

O vetor deste princípio é a ética, ou seja, que a relação da pessoa natural com a entidade controladora dos dados deve ser sincera e autêntica, a fim de que os dados sejam tratados com transparência.

3.5 DIREITOS BÁSICOS DOS TITULARES DE DADOS PESSOAIS

Para Pasquale[69] "os controladores de dados criaram um sistema projetado para maximizar seus próprios lucros, para não tratar os titulares de dados decentemente"[70], razão pela qual da Lei Geral de Proteção de Dados busca a proteção da pessoa natural, nos mais variados campos, como o direito à privacidade, da autodeterminação informativa, dos direitos humanos, dos direitos do consumidor, entre outros.

---

[69] PASQUALE, Frank. **The Black Box Society**. The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015. Disponível em: https://www.semanticscholar.org/paper/The-Black-Box-Society%3A-The-Secret-Algorithms-That-Pasquale/16d48c78afb6a9880486ce1b2111a611b4007557. Acesso em: 22 out. 2020, p. 146.

[70] Esta afirmação consta da mais importante obra de Frank Pasquale, que discute o papel dos algoritmos nos sistemas de reputação da sociedade da informação e para os rumos da economia mundial. A versão original, em inglês, é descrita da seguinte forma no livro "*Data controllers have created a system designed merely to maximize their own profi ts, not to treat data subjects decently*".

Desta forma, além da proteção de dados, a LGPD pretende “a proteção da pessoa humana e de suas situações existenciais relevantes, o que deve ser levado em consideração para a interpretação de todas as suas demais disposições[71]”.

Pelo entendimento colacionado, além da proteção de dados, o objetivo da LGPD é proporcionar a dignidade dos titulares de dados (pessoa natural), bem como todos os direitos correlacionados e, ainda, a autodeterminação informativa, podendo funcionar como “um freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância[72]”.

Desta forma, cumpre analisar os direitos básicos prescritos no Capítulo III, Dos Direitos do Titular, da Lei Geral de Proteção de Dados, que elenca diversos direitos que detém a pessoa natural em face do controlador.

Perante o art. 17 da Lei, o legislador teve o intuito de assegurar os propósitos e valores, dentre os quais “a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade”, fato este que demonstra a intenção em proteger, além dos dados pessoais, também os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania, conforme pode ser constatado em interpretação sistemática com o art. 2°, inciso VII.

Entre os direitos elencados, pode-se observar a prescrição dos seguintes: i) liberdade; ii) liberdade de expressão, informação, comunicação e opinião; iii) privacidade e intimidade; iv) livre desenvolvimento da personalidade; v) autodeterminação informativa; vi) honra; vii) imagem; viii) direitos do consumidor; ix) direitos humanos e x) cidadania.

Não se pode olvidar que alguns dos direitos elencados na lei decorrem dos princípios descritos no art. 6°, tratados em capítulo anterior; assim, o princípio da finalidade (art. 6°, I) exige propósitos legítimos, específicos, explícitos e informados

---

[71] FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. p. 99-129. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 104.

[72] *Ibidem*, p. 103.

ao titular, sem a possibilidade de tratamento posterior de forma incompatível com as finalidades.

O direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento, decorre do princípio da adequação, art. 6°, II.

Ainda, do princípio da necessidade (art. 6°, III) decorre o direito à 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.

O princípio do livre acesso confere o direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6°, IV).

O direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento, decorre do princípio da transparência (art. 6°, V).

A garantia às informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados o segredo comercial, são decorrentes do princípio da transparência (art. 6°, VI).

O direito à segurança dos dados, ao qual se contrapõe o dever, por partes dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, decorre de princípio de mesmo nome (art.° 6, VII).

O princípio da prevenção determina direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6°, VIII).

Não se pode olvidar o princípio da não discriminação, que garante o direito de não ser discriminado de forma ilícita ou abusiva (art. 6°, IX).

Por último, dos direitos decorrentes dos princípios, pode-se constatar o princípio da responsabilização e prestação de contas, que garante o direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6°, X).

Além destes direitos, decorrentes dos princípios, de forma esparsa a lei confere outros direitos aos titulares de dados pessoais, a seguir explicitados.

O art. 7° da Lei prescreve o direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais, no inciso I, c/c § 8°, sendo que no § 6° é garantido o direito de exigir o cumprimento de todas as obrigações de tratamento na lei, mesmo para os casos de dispensa de exigência de consentimento. Quanto ao direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento, há menção no § 5° e, ainda, no §3°, há o direito de que o tratamento de dados pessoais, cujo acesso é público, esteja adstrito à finalidade, à boa-fé e ao interesse público, os quais justificam a sua disponibilização.

Em adição a estes direitos, o art. 8° ainda adiciona o direito à inversão do ônus da prova quanto ao consentimento (§2°); o direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais (§ 4°); o direito de revogar o consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado (§5°); direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados (§6°) e, ainda, no mesmo parágrafo, o direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações.

O rol extenso, de improvável memorização, não termina por aí, sendo que o art. 9° ainda garante acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva, acerca da: finalidade específica, forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a

finalidade; responsabilidades dos agentes que realizarão o tratamento; direitos do titular, com menção explícita aos direitos contidos no art. 18; entre outras.

No art. 9°, § 1°, confere-se o direito de requerer a nulidade do consentimento, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo, ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Outrossim, é garantido no art. 9°, § 3° o direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos.

O art. 10 prescreve dois direitos: no § 1°, o direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida, quando o tratamento for baseado no legítimo interesse do controlador; e, no § 2°, o direito à transparência do tratamento de dados baseado no legítimo interesse do controlador.

O art. 11, inciso II, *c*, prescreve o direito a anonimização dos dados pessoais sensíveis, sempre que for possível, na realização de estudos por órgãos de pesquisa, bem como o direito a ter a devida publicidade em relação às hipóteses de dispensa de consentimento para tratamento de dados sensíveis nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador ou tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos, no § 2°.

Ainda, o art. 11, § 4°, prescreve o direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados, quando consentido pelo titular.

O art. 13, § 1°, trata do direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto de estudo ou pesquisa sobre saúde pública, sendo que o art. 16 trata do direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, autorizada a conservação somente nas exceções legais.

3.6 AS BASES LEGAIS DO TRATAMENTO DE DADOS PARA O SETOR PRIVADO

O artigo 7° da Lei 13.709/2018 estabelece os requisitos para o tratamento de dados pessoais, em dez incisos, sem hierarquia entre eles, sendo que cinco incisos destinam-se à abordagem do setor privado: i) consentimento; ii) cumprimento de obrigação legal ou regulatória pelo controlador; iii) execução de contrato ou de procedimentos preliminares; iv) legítimo interesse; e v) proteção de crédito.

Desta maneira, em cada caso concreto que vislumbrar a necessidade de tratamento dos dados pessoais, o controlador utilizará a base legal mais adequada, sempre respeitando os limites da finalidade do tratamento, requisito este previsto no artigo 5°, XII, da lei de dados, veja-se:

i) O consentimento prescrito no inciso I, do artigo 7°, como condição para o tratamento de dados, deve ser analisado em conjunto com a previsão do inciso XII, do artigo 5°, que prescreve que a manifestação deverá ser “livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais, para uma finalidade determinada.”

A importância do consentimento é tão grande, que vem seguida de três adjetivos, os quais, na verdade, figuram como requisitos ou condições da validade do consentimento, sendo que a ausência de qualquer um deles não irá adjetivar o consentimento como válido.

Por *livre* deve-se entender a ausência de coação ou constrangimento, sem vício na manifestação de vontade, ato por meio do qual a pessoa natural tem a capacidade de agir e não agir.

Por *informado* pode-se compreender que as informações são visíveis, completas e diretas, sendo compreensíveis de imediato, para que não reste dúvida sobre a finalidade do tratamento.

Em adição, o adjetivo *inequívoco* transmite a ideia daquilo que não se admite engano ou dúvida, a concepção de que não há questionamento, como regra geral que autorize o tratamento de dados pessoais, podendo ser demonstrado por qualquer meio de prova lícita.

Em oposição a esta regra geral, cumpre mencionar que o artigo 11 da Lei Geral de Proteção de Dados requer o consentimento específico e destacado para as hipóteses de tratamento de dados sensíveis, de forma semelhante ao exigido pela Lei 12.965/2014 (Marco Civil da Internet).

Outra exceção à regra geral do consentimento *inequívoco* depreende-se da leitura do parágrafo 5°, do artigo 7°, que prescreve sobre a necessidade de comunicar ou compartilhar dados pessoais com outros controladores, sendo que, nesta hipótese, deverá haver o consentimento específico, ressalvadas as hipóteses legais de dispensa.

Desta maneira, a lei evitou a chamada "fadiga do consentimento", que nas palavras de Leonardi[73], pode ser entendido como:

> Ademais, do ponto de vista do titular de dados, a exigência de obtenção de consentimento específico/expresso para toda e qualquer atividade de tratamento de dados geraria um fenômeno conhecido como "fadiga de consentimento", em que o titular passa a concordar como todo e qualquer pedido de consentimento, ficando paradoxalmente menos protegido por não prestar atenção às hipóteses de tratamento que envolvem riscos maiores e que mereceriam maior cautela por parte do titular.

Importante mencionar que o consentimento é utilizado pelo controlador dos dados, em regra, quando há uma relação direta entre ele e o titular dos dados pessoais, especialmente nas hipóteses de aceite de contratos, termos de uso, políticas de privacidade etc.; desta maneira, a lei, ao prescrever como regra geral o adjetivo *inequívoco*, admitiu a inovação, o que permite ao controlador fazer a prova do consentimento, da maneira que a sua tecnologia comportar, sem gerar encargos excessivos do consentimento específico e destacado.

Por último, cabe esclarecer que consentimento adquirido de maneira indireta ocorre nas hipóteses em que o controlador utiliza o consentimento específico obtido pelo titular ao primeiro controlador.

ii) cumprimento de obrigação legal ou regulatória pelo controlador destina-se à execução de disposição legal, haja vista que cada controlador deve conhecer as

[73] LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 321-322.

determinações regulatórias de sua atividade, especialmente em setores regulados, como o financeiro e o de saúde.

Não se pode olvidar que, a despeito de o cumprimento de obrigação legal permitir o tratamento de dados, este deve-se vincular à finalidade de sua atividade, pois o princípio da finalidade (art. 6°, I), juntamente com o da boa-fé (art. 6°, *caput*), destinam-se a todos os tratamentos de dados, e não permitem a discricionariedade para o tratamento, sob pena de o tratamento ser incompatível com a finalidade legal.

Na hipótese de o controlador ter a intenção de tratar estes mesmos dados, impostos por obrigação legal, mas para finalidade diversa, deverá se socorrer de outra base legal prevista no art. 7°, tal como o já tratado consentimento previsto no inciso I.

iii) execução de contrato ou de procedimentos preliminares deve ser compreendido nas hipóteses em que o titular de dados seja parte no contrato, e este seja realizado a seu pedido.

Esta situação ocorre em contratos em cadeia, quando a realização de um contrato depende de outro, devendo os dados ser tratados entre os controladores, para que o contrato principal seja efetivado. Como ilustração, pode-se apontar um contrato de locação, com seguro fiança, que depende do tratamento dos dados pela imobiliária, sendo que esta, após seu aceite, deverá fornecer os dados relativos à renda e capacidade financeira à seguradora, para que esta os trate e decida, igualmente, se o titular do contrato poderá ser seu segurado.

Importante considerar que as mesmas ressalvas feitas em item anterior aqui se aplicam, pois o tratamento de dados para execução de contrato ou de procedimentos preliminares deverá ser vinculado a uma finalidade específica, do contrato original; assim, no exposto exemplo, os dados do titular não poderão ser tratados para o fim de a seguradora se aproveitar da análise e ofertar um consórcio ou qualquer outro produto ou serviço, em vista de que a capacidade financeira já fora anteriormente aferida.

iv) o legítimo interesse (art. 7°, IX) autoriza o tratamento de dados pessoais 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", sendo esta a base legal de tratamento mais ampla de todas, pois não está adstrita a uma finalidade específica.

No entanto, isto não configura uma "carta em branco" ao controlador, pois o artigo 10, seus incisos e parágrafos, determinam as balizas a este tratamento, sendo que, quando for ele utilizado, deverá ser elaborado um relatório de impacto à proteção de dados e a Autoridade Nacional de Proteção de Dados poderá revisar e discordar do tratamento (§3°).

Interessante observar que o §3°, do art.10, prescreve que a Autoridade Nacional de Proteção de Dados "poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais", ou seja, se poderá solicitar, o mesmo deve ser feito quando do tratamento dos dados, e não posterior, sendo uma providência concomitante ao tratamento dos dados e não facultativa.

Cumpre ainda mencionar que o art. 10 trouxe um rol exemplificativo, em vez de taxativo, das hipóteses que permitem o tratamento de dados com base no legítimo interesse, ao afirmar que "incluem, mas não se limitam a: i- apoio e promoção de atividades do controlador; e ii- proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta lei."

A razão de a lei ter adotado um rol exemplificativo, em vez de taxativo, deve-se ao fato de que é necessário haver flexibilidade em uma economia baseada em dados, e que a utilização dos dados proporciona a inovação e o crescimento da atividade econômica, sendo estes dados renováveis em todos os setores da economia, ou melhor, tanto no âmbito privado como no estatal.

v) a lei, ao definir a proteção de crédito como uma base legal para o tratamento de dados pessoais, inovou em relação à lei inspiradora da legislação europeia, que não prevê figura semelhante, sendo utilizado para o regulamento europeu o consentimento, o cumprimento de obrigação legal e o legítimo interesse como fundamentos para o tratamento dos dados.

De outro lado, não obstante o ineditismo da medida, a lei brasileira não definiu a amplitude do significado de proteção de crédito, ou seja, se deve ser interpretada

de forma extensiva ou restritiva, prescrevendo tão somente “inclusive quanto ao disposto na legislação pertinente” (art. 7°, X).

Ora, “legislação pertinente” pode figurar como uma cláusula geral, que são as normas com diretrizes indeterminadas, pois não trazem uma solução jurídica imediata.

Neste sentido, pode-se entender que o legislador deixou em aberto o significado de proteção de crédito para envolver todas as atividades que tratem, direta ou indiretamente, da proteção de crédito, haja vista que o tratamento destes dados é elemento basilar, tanto para a parte que deseja o crédito, como para o contratante que tem a intenção de outorgar o crédito.

Inclusive, o Código de Defesa do Consumidor, em uma possível interpretação em diálogo das fontes, quando trata do crédito, o adota em intepretação extensiva para englobar as atividades de natureza bancária, financeira, securitária, entidades de proteção ao crédito e congêneres (art. 3°, §2° e art. 43, §4°, da Lei 8.078/1990).

Nas palavras de Leonardi[74], a proteção de crédito “deve ser interpretada extensivamente, autorizando o tratamento de dados pessoais tanto para atividades inerentes à concessão de crédito quanto para atividades de apoio”.

Por derradeiro, quanto à proteção de crédito, a devida amplitude será definida pela Autoridade Nacional de Proteção de Dados, sendo que na hipótese de se entender por uma interpretação restritiva, esta limitaria o tratamento para o gerenciamento de risco de crédito, o que seria pouco eficaz, pois o controlador poderá utilizar o consentimento ou o legítimo interesse para tratar os referidos dados.

[74] LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 330.

4 DO CONSENTIMENTO

4.1 O QUE SE ENTENDE POR CONSENTIMENTO NA LEI DE PROTEÇÃO DE DADOS PESSOAIS

A Lei 13.709/2018 define o significado de consentimento no artigo 5°, XII, como sendo “a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”, e estabelece no Capítulo II, Seção I, artigo 7°, I, que o consentimento é um entre os dez requisitos previstos para o tratamento dos dados pessoais.

Pode-se entender o consentimento como o ato de dar permissão, anuir, assentir, autorizar, concordar e dar licença, mas para a Lei Geral de Proteção de Dados, além destes sinônimos, o consentimento pode ser classificado como uma das bases legais para o tratamento dos dados pessoais, sendo que tanto o poder público, como as empresas do setor privado (ressalvadas as hipóteses de sua dispensa), precisam demonstrar a sua concessão para legitimar o tratamento dos dados pessoais, sendo “a hipótese que pode trazer mais segurança jurídica para o controlador, a quem incumbe o ônus da prova de que foi obtido em conformidade com a lei”[75].

Para Simão Filho[76], o consentimento, para que seja considerado válido, exige por parte do controlador o cumprimento de alguns requisitos, razão pela qual mostra-se oportuno colacionar importante esclarecimento:

> Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. O consentimento deverá referir-se à finalidade determinada, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. É vedado o tratamento de dados pessoais mediante vício de consentimento, cabendo ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com as normas legais.

---

[75] VAINZOF, Rony. **Lei Geral de Proteção de Dados Comentada**. 2. ed. rev. atual. amp. São Paulo: Revista dos Tribunais, 2019, p.117.

[76] SIMÃO FILHO, Adalberto. Regime Jurídico do Banco de Dados – Função Econômica e Reflexos na Monetização. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. p. 167-204. São Paulo: Quartier Latin, 2019, p. 178.

Ademais, a título de conhecimento, o requisito do consentimento é mencionado 35 (trinta e cinco) vezes na Lei Geral de Proteção de Dados, devido à sua importância, devendo ele ser observado tanto na fase pré-tratamento (art. 7°, I), como na fase de tratamento (art. 7°, §5°) e, inclusive, na fase pós-tratamento (art. 8°, § 5° e 6°; art. 9°, §2°) dos dados, como condição de validade.

O consentimento relativo aos dados sensíveis (art. 11, I), além das exigências prescritas aos demais dados, exige do controlador que o requerimento de concessão seja feito de forma específica e destacada, por se tratarem de informações potencialmente discriminatórias. Pela relevância destas informações, alguns doutrinadores entendem se não seria conveniente suprimir o direito de consentir, sobre os dados sensíveis, do âmbito de disposição individual[77].

De outro lado, cumpre ainda mencionar que nos dados relativos a crianças e adolescentes (art. 14, §1°), ou para transferência internacional (art. 33, VIII), o consentimento, igualmente, deverá ser específico e em destaque, sendo que para os menores e adolescentes, ainda, deverá ser concedido por pelo menos um dos pais ou responsável.

Outro fator que deve ser observado é sobre a questão do ônus da prova de sua concessão, pois o artigo 8° determina que o consentimento deverá ser comprovado por escrito ou por qualquer outro meio de prova, sendo que na hipótese de ter sido concedido por escrito deverá constar de cláusula destacada das demais.

Importante ainda considerar que em bases semelhantes ao Código de Defesa do Consumidor[78], a Lei Geral de Proteção de Dados reconhece a assimetria de forças entre a pessoa natural, concedente de seus dados, e o Poder Público e as empresas privadas, controladoras de seus dados, para promover a inversão do ônus da prova, e impor que a prova da outorga/permissão do tratamento deverá ficar ao encargo do controlador (art. 8°, §2°, c/c art. 42, § 2°).

---

[77] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 62.

[78] A Lei n° 8.078/90, de 11 de setembro de 1990, prescreve no artigo 6°, VIII, que são direitos básicos do consumidor: a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiência.

Ademais, pode-se entender da redação do dispositivo legal do art.42, §2°, que o juiz poderá inverter o ônus da prova quando a alegação for verossímil ou houver hipossuficiência para fins de produção da prova ou quando a produção da prova for excessivamente onerosa, sendo desnecessária a exigência cumulativa da verossimilhança e da hipossuficiência.

Referido entendimento pode se depreender tanto da redação do dispositivo legal, que utiliza a conjunção alternativa *ou*, em vez da conjunção aditiva *e*, bem como de uma interpretação em diálogo das fontes como o Código de Defesa do Consumidor, que em seu artigo 6°, VIII, adota a hipossuficiência como um conceito fático, ou seja, quando houver uma disparidade no caso concreto.

Tanto no Código de Defesa do Consumidor, como na Lei Geral de Proteção de Dados, em estudo, a hipossuficiência pode ser classifica de 04 (quatro) maneiras: i) econômico financeira (fragilidade econômica); ii) política social (acesso à justiça); iii) técnica (não tem o costume de utilizar a tecnologia) e iv) informacional (não tem o conhecimento da tecnologia).

Desta maneira, o consentimento é o ato jurídico pelo qual a pessoa natural manifesta o seu aceite ao tratamento de seus dados pessoais, e faz valer a sua autonomia privada, para que seus dados sejam tratados no exato limite da finalidade informada.

Interessante observar que o substantivo “finalidade”, previsto no fim do inciso XII, do artigo 5°, deve ser considerado como uma verdadeira condição ou pressuposto para o tratamento dos dados pessoais, haja vista que o consentimento recai na exata medida da finalidade informada, sendo que, sem esta finalidade, haveria uma verdadeira “carta em branco” para o tratamento dos dados pessoais.

Oportuna colocação é feita por Mendes[79] a respeito do consentimento no tocante à proteção de dados pessoais, veja-se:

> [...] na medida em que consentimento do indivíduo permite o processamento dos seus dados, na eventual hipótese de violação ao seu direito à privacidade, como poderia ele reivindicar a reparação daquela violação, se tinha autorizado o tratamento de seus dados pessoais?

[79] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 61.

Com relação ao questionamento de Mendes[80], pode-se entender que o desrespeito à finalidade seria fato ensejador suficiente ao direito de reparação, haja vista que o consentimento livre, informado e inequívoco, são balizados pela finalidade informada, como um verdadeiro limite à sua realização.

A finalidade, além de constar como um vetor do consentimento, está elencada entre os princípios que devem ser observados pelos agentes de tratamento de dados (controlador e operador), conforme previsão do artigo 6°, I.

Assim, para Mendes[81] "é fundamental compreender que o consentimento não representa a ausência de interesse do indivíduo na tutela dos dados pessoais, mas constitui um ato de escolha no âmbito da autodeterminação individual".

4.2 CONSENTIMENTO INEQUÍVOCO DA LEI GERAL DE PROTEÇÃO DE DADOS *VERSUS* O CONSENTIMENTO EXPRESSO DO MARCO CIVIL DA INTERNET

Anteriormente à Lei Geral de Proteção de Dados, o consentimento era tratado pelo Marco Civil da Internet, Lei 12.965, de 23 de abril de 2014, no art. 7°, IX, da seguinte maneira: "**consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (grifo nosso).

De outro lado, o art. 5°, XII, da Lei Geral de Proteção de Dados prescreve o consentimento como a "manifestação livre, informada e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (grifo nosso).

A divergência das duas leis recai sob o adjetivo que autoriza a utilização dos dados, sendo que para o Marco Civil da Internet deve ser *expresso*, e para a Lei Geral de Proteção de Dados é *inequívoco*, o que aparentemente, em uma análise superficial, tem o mesmo sentido de permitir o tratamento dos dados.

Na realidade, o entendimento empregado pela doutrina implica em exigências diferentes, ou melhor, o controlador deverá utilizar diferentes métricas para conferir o

---

[80] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 61.
[81] *Ibidem,* p. 61-62.

cumprimento da lei, a depender se a comprovação do consentimento se der sob o Marco Civil da Internet ou sob a Lei Geral de Proteção de Dados.

Desta maneira, primeiramente, urge solucionar a questão de antinomia, a fim de saber qual lei deverá ser aplicada, em cada caso concreto, para após ser tratada a amplitude e consequência de cada adjetivo empregado.

O Marco Civil da Internet é lei geral, que instituiu princípios, garantias, direitos e deveres para a utilização da internet*,* já a Lei Geral de Proteção de Dados pode ser classificada como uma lei específica para o tratamento de dados, ou nas palavras de Lima[82], como "um microssistema de proteção de dados pessoais, à semelhança do Código de Defesa do Consumidor".

Desta forma, pelas regras de solução de antinomia, a lei posterior e especial dever prevalecer sob a lei geral e anterior; portanto, para o tratamento de dados pessoais no âmbito on-line e off-line*,* o controlador dos dados deverá exigir o consentimento inequívoco, em razão da Lei Geral de Proteção de Dados ser lei específica e posterior.

Resolvida esta questão, o debate recai sob a qualificação do consentimento: o que se entende por *expresso* ou *inequívoco*.

Para solução desta qualificação, traz-se a lição de Lima[83], para quem o consentimento dever ser entendido como uma manifestação de vontade; assim, veja-se:

> [...] é possível aplicar aos contratos eletrônicos a teoria de Karl Larenz sobre as condutas socialmente típicas ou, como preceituava Pontes de Miranda, tacitude *stricto sensu*. Portanto, o consentimento do titular dos dados pode ser obtido por meio de condutas incompatíveis com a discordância da coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais. Vejamos a prática dos *cookies*, ou seja, um programa utilizado para rastrear a navegação do usuário, que é informado de tal prática de maneira clara no início do site, inclusive com a indicação da finalidade específica, qual seja a otimização da navegação. O usuário concorda com tal prática ao continuar navegando no site. Tal conduta é incompatível com a recusa. Este é um exemplo claro de que é possível obter o consentimento inequívoco, por meio de condutas socialmente típicas.

[82] LIMA, Cíntia Rosa Pereira de. Consentimento inequívoco versus expresso: o que muda com a LGPD? **Revista do Advogado**. AASP. São Paulo, n.144, nov., 2019, p. 63.
[83] *Ibidem*, p. 63-64.

Pela lição acima, o consentimento inequívoco pode ser obtido por meio de “condutas socialmente típicas”, que demonstram de forma cabal a intenção da pessoa natural em autorizar o tratamento dos dados, haja vista que a sua conduta de “surfar” no site que ingressou livremente serve como prova da autorização de seu consentimento.

A Lei Geral de Proteção de Dados, por ser posterior, evoluiu e ficou em sintonia com a evolução da tecnologia, por exigir um consentimento mais dinâmico, mais condizente com a evolução diária que ocorre no mundo digital, sendo este, inclusive, a opinião de Lima[84], para quem “a LGPD está mais apropriada à dinâmica das relações on-line, quando utiliza o termo “inequívoco” em vez do que utiliza o MCI (“expresso”).

Outro não é o entendimento de Leonardi[85], para quem:

> A adoção de um conceito de consentimento inequívoco como regra geral, em oposição a específico e destacado, viabiliza o tratamento de dados no ambiente online, permite a contínua inovação baseada em dados e assegura um nível de proteção adequado ao titular sem gerar ônus excessivos para os responsáveis pelo tratamento de dados.

Este entendimento de constante evolução é respaldado, inclusive, pela Constituição Federal, no artigo 170, caput, que prescreve que “a ordem econômica, fundada na valorização do trabalho e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social”, pois, nada mais consonante com a evolução do que a valorização da livre iniciativa.

Ademais, não se pode esquecer o parágrafo único, do mesmo artigo, que assegura “a todos o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos, salvo nos casos previstos em lei”.

Não há forma melhor de garantir existência digna do que proporcionar a evolução, a livre concorrência, o livre exercício da atividade econômica, valores estes

---

[84] LIMA, Cíntia Rosa Pereira de. Consentimento inequívoco versus expresso: o que muda com a LGPD? **Revista do Advogado**. AASP. São Paulo, n.144, nov., 2019, p. 64.

[85] LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 321.

que ressoam com a inovação, ao se exigir o consentimento pela forma inequívoca, em vez da expressa.

4.3 CONSENTIMENTO DOS DADOS SENSÍVEIS: CATEGORIA DE DADOS QUE REQUER PROTEÇÃO ADICIONAL

Para além da proteção aos dados pessoais, a Lei Geral de Proteção de Dados prescreveu a existência dos dados pessoais sensíveis como sendo dados de uma categoria superior, por tratarem de informações relacionadas diretamente à personalidade da pessoa natural, razão pela qual este tratamento irá demandar análise específica da entidade controladora.

O artigo 5°, inciso II, classifica como dado pessoal sensível aquele de "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;" (grifos nossos).

Conforme os grifos acima, a lei prescreveu doze dados pessoais, relativos à personalidade, como sensíveis, sem, no entanto, ao final da descrição do inciso, estipular cláusulas gerais, tais como, "entre outros direitos relativos à personalidade", a fim de permitir uma interpretação extensiva, o que possibilitaria a inclusão de outros dados como sensíveis, tanto pela doutrina, como pela Agência Nacional de Proteção de Dados.

No entanto, esta não é a posição de Mulholland[86], para quem os dados pessoais sensíveis não estão dispostos de forma exaustiva na lei, veja-se:

> Ressalte-se que esta definição não é, de forma alguma, taxativa ou exaustiva. Trata-se de conceito que enumera de maneira exemplificativa algumas das hipóteses em que serão identificados os dados pessoais que tenham natureza considerada sensível. Isto quer dizer que não somente o conteúdo dos dados previsto neste inciso merecerão a qualificação como dados sensíveis, podendo abarcar outras situações não previstas.

Não obstante a assertividade das considerações e o peso que o argumento da autora impõe, pode-se entender que este não foi o objetivo da lei, que visa conceder

[86] MULHOLLAND, Caitlin. Dados Pessoais Sensíveis e Consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. AASP. São Paulo, n.144, nov., 2019, p. 48.

segurança jurídica às entidades controladoras e à pessoa natural que irá outorgar o tratamento de seus dados, ao estabelecer duas categorias de dados.

Pode-se entender que tem-se os dados pessoais “simples”, que não atingem os direitos da personalidade destacados pela lei, e os dados sensíveis, que ao tratarem de temas relativos à personalidade da pessoa natural, foram colocados em um patamar superior, que exige das entidades controladoras o consentimento “de forma específica e destacada, para finalidades específicas (art. 11, I)”.

Entender que existem outros “dados sensíveis, podendo abarcar outras situações não previstas” para a entidade que irá tratar os dados, seria o mesmo que instaurar a imprevisibilidade e o caos, pois como o consentimento, que deverá ser prévio em muitas situações, e de forma específica e destacada, irá ser tratado? As entidades estariam em eterna possibilidade de desconformidade, e sob pena de sanção?

Lógico que se deve respeitar o direito da personalidade da pessoa natural, previsto como garantia constitucional (art. 5°, *caput* e inciso X), mas, de outro lado, deve-se fazer a ponderação com o art. 170 da Constituição Federal, que, igualmente, resguarda entre os princípios da atividade econômica, a valorização do trabalho humano na livre iniciativa, a fim de assegurar a todos existência digna, razão pela qual não se deve atribuir à entidade controladora dos dados a Caixa de Pandora[87].

Como justificativa de seu pensamento, a conceituada civilista Mulholland[88] traz à tona um exemplo, veja-se:

> No entanto, não só a natureza de um dado, estruturalmente considerado, deve ser avaliada para a sua determinação como sensível, mas deve-se admitir que certos dados, ainda que não tenham, a princípio, essa natureza especial, venham a se considerados como tal, a depender do uso deles é feito no tratamento de dados. Por exemplo, se considerarmos numa base de dados o nome e o bairro em que uma pessoa mora, pode ser possível identificar a origem racial desta pessoa. Significa dizer que no tratamento de dados pessoais, em que se consideram estes dois dados não sensíveis,

[87] Caixa de Pandora é um artefato da mitologia grega, tirada do mito da criação de Pandora, que foi a primeira mulher criada por Zeus. A “caixa” era na verdade um grande jarro dado a Pandora, que continha todos os males do mundo. Pandora abre o jarro, deixando escapar todos os males do mundo, menos a “esperança”. NATHAN, Andrea. O que é a caixa de Pandora? Entenda a origem do mito – e descubra o que tinha lá dentro, **Revista Super Interessante,** 2018. Disponível em: https://super.abril.com.br/historia/o-que-e-a-caixa-de-pandora/. Acesso em: 12 out. 2020.

[88] MULHOLLAND, Caitlin. Dados Pessoais Sensíveis e Consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. AASP. São Paulo, n°144, nov.2019, p. 49.

> pode-se chegar à determinação de um dado sensível – raça – que, por sua vez, pode gerar consequências no tratamento de dados indesejadas, discriminatórias ou prejudiciais a seu titular.

Aludido entendimento, além de confrontar o espírito da lei, que prescreve de forma taxativa os dados que devem ser considerados sensíveis, vislumbra uma intepretação que, além de extensiva, presume a má-fé, pois se o bairro em que uma pessoa mora pode configurar uma origem racial e, por consequência, discriminação racial, em contrapartida, o mesmo bairro poderia, em razão da raça, justificar uma ação afirmativa ou inclusiva por parte do controlador.

Não se pode olvidar que, nos termos do artigo 113 do Código Civil, lei geral aplicável a todos as relações jurídicas, os "negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração", razão pela qual na Lei Geral de Proteção de Dados, o tratamento dos dados deve ser interpretado como um comportamento de lealdade em todas as fases do tratamento dos dados, e não de forma diversa.

É possível que, após o tratamento de dados, o controlador obtenha uma informação de caráter sensível, mas isto não implica dizer que na fase antecedente, de concessão dos dados, tenha sido imposto à pessoa natural um consentimento específico e destacado.

Inclusive, como já destacado, a boa-fé implica a observância de deveres laterais ou anexos de conduta, entre eles: cuidado, respeito, informação, colaboração, transparência, confiança e razoabilidade; portanto, a observância destas condutas justifica a não ampliação incondicional dos dados classificados como sensíveis.

Em consonância com este entendimento, é possível trazer lição de Doneda[89], que entende: "um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz, pode sê-lo", razão pela qual, como no tratamento de dados deve ser observada a boa-fé, um dos onze princípios prescritos no art. 6° da Lei 13.709/18, sendo que o seu descumprimento, por si só, já acarreta uma desconformidade no tratamento dos dados.

---

[89] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 144.

Portanto, não há como entender que o rol de dados sensíveis é exemplificativo, permitindo-se a “criação” de novos dados sensíveis a cada tratamento, haja vista que o princípio da boa-fé é suficientemente amplo a conferir proteção à pessoa natural, sem a necessidade de se admitir a interpretação de que os dados sensíveis estão dispostos de maneira exemplificativa na lei.

Expostas tais premissas, há de se concluir que o consentimento, para o tratamento dos dados pessoais sensíveis, deve ser destacado e realizado de forma específica, sob pena de invalidade do tratamento (art. 11, I), devendo ser respeitado o princípio da finalidade.

4.4 O CONSENTIMENTO LIVRE, INEQUÍVOCO E INFORMADO SERIA UMA UTOPIA?

Não obstante o consentimento inequívoco ser mais adequado à evolução da tecnologia e à dinâmica da sociedade digital, uma pergunta pode se apresentar: o consentimento expresso não seria mais seguro, haja vista que, a princípio, poderia exigir maior atenção da pessoa natural ao outorgar o consentimento?

Talvez, na hipótese de a maioria das pessoas naturais serem capazes de compreender a amplitude do que estivessem a autorizar, dos termos rebuscados e técnicos, e, ainda, se este homem médio despendesse tempo de leitura maior do que os segundos necessários a encontrar o “ícone” do sim[90].

Desta forma, o consentimento, como um único ato, tanto o *expresso* como o *inequívoco*, leva a uma falácia quanto à sua anuência, pois o homem médio, primeiro, dificilmente irá entender a complexidade dos termos descritos e, segundo, mesmo que seja capaz de compreender, provavelmente não irá dispor de tempo para tanto, pois a dinâmica da atual sociedade não permite tamanha disponibilidade.

[90] Pesquisa da Deloitte com dois mil consumidores americanos descobriu que 91% consentem com os termos e condições de uso sem lê-los. Para os mais jovens, com idades o entre 18 e 34 anos, a taxa é ainda maior, com 97% concordando com as condições antes de ler. CAKEBREAD, Caroline. You’re not alone, no one reads terms of service agreements. **Businessinsider,** 2017. Disponível em: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11. Acesso em: 10 out. 2020.

Por consequência, o melhor será compreender o consentimento como uma sequência de atos, por manifestações de vontade sequenciais que levem a entender que o consentimento, para o tratamento dos dados pessoais, está sendo outorgado a cada *click*.

Cumpre ressaltar que o consentimento é uma entre as dez bases legais de tratamento dos dados pessoais, descritos no art. 7° da Lei Geral de Proteção de Dados, sendo que não há hierarquia entre eles, apesar de a referida lei ter estabelecido tratamento destacado a este requisito[91].

O consentimento é um dos pontos de maior estima no quesito do tratamento de dados pessoais, sendo que por meio deste ato, para Doneda[92], o "direito civil tem a possibilidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão."

Oportuno mencionar que, em decorrência dos princípios elencados no art. 6°, em especial os da finalidade (art. 6°, I) e o da necessidade (art. 6°, III), o consentimento deve ser interpretado de maneira restritiva, não podendo o controlador adotar uma interpretação extensiva, a fim de objetivar um tratamento estendido ou maximizado dos dados, inclusive, para fins posteriores ou diversos do requerimento inicialmente previsto.

O consentimento consiste na manifestação individual de vontade, tendente a aderir e legitimar, nos limites mínimos, uma autorização para o tratamento de seus dados pessoais, sendo que, para muitos autores, está ele situado no campo dos direitos da personalidade (Stefano Rodotà, Danilo Doneda, Laura Mendes, Guilherme Tepedino, entre outros), haja vista ser inadequada a caracterização de natureza negocial, "visto que tal entendimento reforçaria o sinalagma entre o consentimento para o tratamento dos dados pessoais e determinada vantagem econômica obtida por aquele que consente", pois, ao se adotar tal entendimento, iria "reforçar indesejada

---

[91] TEPEDINO e TEFFÉ entendem que em análise minuciosa da LGPD, os princípios orbitam em torno do consentimento e no comportamento humano. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Revista dos Tribunais, 2019.

[92] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais:** elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019a, p. 297-298.

índole contratual e de fomento à utilização de esquemas proprietários para o trato dos dados pessoais”[93].

Este assunto será tratado em outro tópico, mas não se pode negar vantagem econômica em uma sociedade movida por dados, onde milhões de pessoas, principalmente nos países subdesenvolvidos, somente são incluídas na sociedade digital, única e exclusivamente, por poderem outorgar o tratamento de seus dados, o que fazem em troca da utilização de aplicativos ou programas, já que não teriam condições de pagar se fosse exigida uma remuneração prévia.

Inclusive, se não houvesse a troca de dados pessoais, como compensação financeira, a indústria dos dados não estaria no atual estágio de desenvolvimento, em que se fabricam aparelhos de celular, com sistemas sofisticadíssimos, sem o repasse do custo financeiro desta tecnologia ao consumidor final.

Não obstante estas considerações em apartado, o consentimento *livre* pode ser entendido como o realizado isento de constrangimento, ou melhor, como a capacidade da pessoa natural de aceitar ou recusar a utilização de seu dado pessoal, sem interferências que viciem seu consentimento.

Ponto relevante pode se extrair deste requisito, diante da assimetria de forças da entidade controladora dos dados e a pessoa natural, em especial, nas políticas de “pegar ou largar” (*take-it-or-leave-it choice*[94]), em que existem duas possibilidades: aceita-se o tratamento dos dados e passa-se a desfrutar do serviço ou, de outro lado, se há negativa, sequer tem-se a oportunidade de abrir o programa ou aplicativo.

Nestas situações, apresenta-se o questionamento: diante da flagrante vulnerabilidade, em semelhança aos contratos de adesão regulados pelo Código de Defesa do Consumidor, em que o contratante somente tem a discricionariedade do sim ou não, o consentimento da pessoa natural é isento de vício?

---

[93] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 299.

[94] BORGESIUS, Frederik J. Zuiderveen *et al.* **Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation**. Universiteit Van Amsterdam, 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 14 out. 2020.

Para tanto, deve ser observado qual é o poder efetivo que tem a pessoa natural, com relação ao tratamento de seus dados pessoais, ou seja, considerar quais são as opções que tem o titular dos dados em relação ao dado coletado e o seu possível uso.

Outro requisito previsto na lei é o adjetivo *informado*, que revela o dever de a pessoa natural estar devidamente instruída ou esclarecida, cabendo à entidade controladora dos dados fornecer informações necessárias e suficientes para a correta avaliação de como os dados serão tratados.

A informação deve ser antecedente, sendo este um fator determinante para a inexistência de vício e concessão do consentimento, não podendo ser olvidado que o art. 9° prescreve que “o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva”.

A amplitude do requisito informado é delimitado nos incisos do art. 9°, nos seguintes termos: 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.

Com exceção do inciso *ii),* fácil será o cumprimento dos deveres de informação pela entidade controladora; no entanto, a ressalva de não informar sobre os “segredos comercial e industrial” não poderá servir de pretexto para o fim de não prestar todas as informações relativas ao tratamento dos dados.

Cumpre mencionar que o artigo 8°, §6, ressalva que se ocorrer “alteração de informações referida nos incisos I, II, III ou V do art. 9°, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o consentimento é exigido, revogá-lo”, na hipótese de discordar de tais alterações.

Para o cumprimento do requisito do consentimento, o mesmo ainda deverá ser *inequívoco*, que deve ser entendido como a manifestação não ambígua, sempre vinculada ao princípio da finalidade.

Vale lembrar que o consentimento não precisa ser obtido de forma escrita pelo controlador dos dados, mas na hipótese de o ser, deverá constar em cláusula apartada das demais (art. 8°, I).

Importante esclarecer que o consentimento não poderá ser obtido pela omissão, ou seja, o consentimento deverá resultar de uma ação positiva e volitiva, que não decorra do acaso, e que demostre claramente a intenção da pessoa natural em outorgar o consentimento.

Outro ponto que não pode fugir da memória é a vinculação do consentimento ao controlador para qual foi concedido, sendo esta a eficácia subjetiva do consentimento.

Outrossim, como já mencionado, o consentimento é manifestação de vontade temporária, pois pode ser revogado mediante manifestação simples, gratuita e facilitada (art. 8°, §5°, c/c art. 18, IX e art. 15, III), já que está relacionado à autodeterminação da vontade da pessoa natural. No entanto, a retirada do consentimento, licitamente concedido, não irá comprometer o tratamento regularmente realizado pela entidade controladora.

Para sintetizar o consentimento, como ato de autodeterminação da vontade da pessoa natural, "há de ser interpretado de forma que seja o instrumento por excelência da manifestação da escolha individual, ao mesmo tempo em que faça referência direta aos valores fundamentais em questão[95]"; desta forma, o autor sintetiza que "o consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade[96]".

4.5 AS PAREDES DE RASTREAMENTO E AS OPÇÕES DE PEGAR OU LARGAR (*TRACKING WALLS, TAKE-IT-OR-LEAVE-IT CHOICES*) CONFIGURAM VIOLAÇÃO AO CONSENTIMENTO LIVRE, INEQUÍVOCO E INFORMADO?

No ambiente on-line, encontram-se facilmente as opções do "tipo pegar ou largar", que funcionam como verdadeiras *tracking walls*, nas palavras de Frederik

[95] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais:** elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 297.
[96] *Ibidem,* p. 298.

Borgesius e colaboradores[97], o que, em tradução livre, pode ser interpretado como “paredes de rastreamento”.

A parede de rastreamento consiste em uma restrição imposta pela entidade controladora dos dados, que limita a discricionariedade da pessoa natural a um “sim” ou um “não”. Na hipótese de se eleger o “sim”, a pessoa natural terá seus dados tratados, nos limites e finalidades impostos pelo controlador e, na hipótese do “não”, sequer haverá a possibilidade de o indivíduo verificar qualquer disposição do *website* ou qualquer outro aplicativo para dispositivo móvel.

Neste sentido, não se pode olvidar que, além de ser um ato de autodeterminação da vontade, o consentimento também detém um caráter acessório, que está diretamente relacionado à situação que o fundamenta, o qual pode ser a realização de um contrato ou qualquer outro ato de intenção volitiva. Para Doneda[98]:

> A alternativa a não revelação dos dados pessoais pelo seu titular costuma ser uma – por vezes, brutal – renúncia a determinados bens ou serviços. A disparidade de meios e de poder entre a pessoa de quem é demandado o consentimento para utilização dos dados pessoais em contemplação da realização de um contrato e aquele que os pede faz com que a verdadeira opção que lhe reste seja, tantas vezes, a de “tudo ou nada”, “pegar ou largar”.

Diante deste entendimento, as paredes de rastreamento, com a opção de pegar ou largar, podem configurar imposição injusta e inaceitável ao livre consentimento e, por consequência, ao tratamento dos dados da pessoa natural. Haveria um vício de consentimento, da pessoa natural, diante desta imposição pela entidade controladora dos dados?

De princípio, cumpre esclarecer que a legislação brasileira específica de tratamento dos dados, Lei 13.709/2018, bem como a legislação esparsa, Marco Civil da Internet, Lei de Acesso à Informação, entre outras, não conferem resposta a estas indagações; inclusive, a lei inspiradora da lei de dados brasileira, o RGPD (Regulamento Geral sobre Proteção de Dados – 2016/679), não abriga resposta ao tema.

---

[97] BORGESIUS, Frederik J. Zuiderveen *et al.* **Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation.** Universiteit Van Amsterdam, 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 14 out. 2020.

[98] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 298-299.

É no mínimo discutível afirmar que as pessoas teriam controle sobre seus dados pessoais, já que lhes é imposta, pela entidade controladora, a condição de ter que consentir com o rastreamento imposto para poder acessar *websites*, razão pela qual podem ser feitos os seguintes questionamentos: i) devem haver regras para o rastreamento?; ii) deve haver proibição ao rastreamento, em certas circunstâncias? e, iii) deve haver proibição total às paredes de rastreamento?

Não se pode olvidar que o conteúdo financiado por publicidade existe há muitos anos, mesmo antes da origem da internet, tanto no ambiente da imprensa escrita, do rádio, e no sistema de televisão, sendo o atual modelo de conteúdo "grátis" nada mais do que uma evolução, segundo a qual, em decorrência dos modos de captura, a publicidade está mais direta e inclusiva aos desejos e preferências da pessoa natural.

A possibilidade de o controlador dos dados ter ciência da localização e a quais vídeos a pessoa assiste, a título de exemplo, implica em uma combinação de informações que favorece a terceiros vender publicidade mais assertiva e, por consequência, poderia haver violação da privacidade.

O ato de consentir ao tratamento dos dados, por meio de uma imposição ou, ao menos, de uma limitação da discricionariedade, pode configurar um "paradoxo de privacidade", onde as pessoas se preocupam com sua privacidade, mas autorizam a divulgação de seus dados para obterem benefícios e conveniências, que não poderiam obter se desta maneira não agissem; portanto, as pessoas podem se importar com suas respectivas privacidades, mas não têm condições de agir conforme suas preferências.

Do ponto de vista da proteção de dados, a outorga no tratamento dos dados pode ser considerada como feita "livremente", quando a pessoa concorda com o rastreamento após optar pelo "sim", em um "banner de consentimento de *cookie*"? Para Kosta[99], uma parede de rastreamento torna o consentimento involuntário, pois, "em tal caso o usuário não tinha uma escolha real, portanto, o consentimento não é dado livremente".

---

[99] No original: "*in such a case the user does not have a real choice, thus the consent is not freely given*". KOSTA, Eleni. Consent in European Data Protection Law (Phd tese, University of Leuven 2013) apud BORGESIUS, Frederik J. Zuiderveen *et al.* **Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation.** Universiteit Van Amsterdam, 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em 14/10/2020.

No Brasil, como a lei não regula o tema, bem como não veda esta prática, o âmbito de regulação ficará sob responsabilidade da Autoridade Nacional de Proteção de Dados, conforme prescreve o art. 55-J, XIII, “editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade”.

Diante da possibilidade que se apresenta para a ANPD, seguem algumas hipóteses para ilustrar como poderá ser feita essa regulação: i) ausência de regras específicas para as paredes de rastreamento; ii) banimento das paredes de rastreamento, em algumas circunstâncias e, iii) banimento completo das paredes de rastreamento.

i) Na ausência de regras específicas para as paredes de rastreamento, a situação permaneceria da forma atual; assim, a voluntariedade do consentimento teria que ser avaliada em cada caso concreto.

Neste caso, na hipótese de uma empresa ter posição dominante de mercado, haveria maiores chances de desequilíbrio entre as partes, pois os indivíduos teriam pouco poder de negociação.

Inclusive, em casos de empresas dominantes, por exemplo, o *Facebook,* qual seria a possibilidade de uma pessoa utilizar outra rede social para interagir com os seus amigos, em uma situação de parede de rastreamento, em que há um bloqueio ao ingresso se não houver o consentimento no tratamento dos dados?

Pode-se dizer que há liberdade no consentimento? Existe outra empresa que permita a liberdade de manifestação e interação com a sociedade, a fim de caracterizar liberdade no consentimento? Neste exemplo, alguém que não queira divulgar seus dados teria sua liberdade interpretada como a recusa ao serviço.

ii) Banimento das paredes de rastreamento, em algumas circunstâncias, pode ser entendido como viável, especialmente quando se tratar de serviços do governo, em que a exclusividade da prestação impossibilita, por absoluto, considerar como livre o consentimento da pessoa natural.

Para ilustrar, um aplicativo do governo da previdência social não poderia exigir permissão de geolocalização, como parede de rastreamento, para conceder acesso ao aplicativo do celular e permitir o cadastro do usuário.

Outro ponto relevante, em que deveria ser implementada a vedação à barreira de rastreamento, são os sites que tratam de temas de liberdade de expressão, em especial os que tratam de direitos sensíveis, como o art. 5°, II, em razão do tratamento permitir a discriminação.

Permitir o tratamento de dados sensíveis, que tratam de características da personalidade do indivíduo, por meio de paredes de rastreamento, na modalidade pegar ou largar, não parece lícito e tampouco condizente com os princípios da Lei Geral de Proteção de Dados, pois as pessoas preocupadas com a privacidade podem não querer aceitar os *cookies* de rastreamento e, portanto, podem não acessar os sites que estão atrás destas paredes.

A privacidade deve ser considerada como um vetor importante para o direito de ter acesso e receber informações; por consequência, deve ser garantido o direito de "ler livremente", ou seja, sem tratamento.

Outro ponto que deve ser considerado são os sites que tratam de sigilo profissional, como os médicos, advogados e contadores; a título de exemplo, uma pessoa tem o direito de marcar uma consulta para a especialidade médica que desejar, sem lhe ser ofertada a compra de um determinado medicamento, relacionado à doença consultada, ou melhor, sem que as operadoras de planos de saúde tenham conhecimento.

No entanto, pelo exemplo utilizado, o problema recairia na definição do que são serviços médicos, ou serviços relacionados à saúde da pessoa, em contraposição a um site relacionado à pesquisa acadêmica, onde seria possível o tratamento dos dados.

iii) A outra opção sugerida seria a vedação por completo das paredes de rastreamento, o que implicaria um descompasso com as demais legislações, haja vista que esta modalidade de captura de dados é utilizada em nível mundial e, portanto, prejudicaria em muito as empresas que estão no Brasil, para ficar em conformidade com as demais legislações alienígenas.

Pelo exposto, pode-se concluir que as paredes de rastreamento são amplamente utilizadas, em razão de não haver legislação que vede a sua prática, motivo pelo qual o art. 55-J, XIII, facultou à ANPD a possibilidade de regular tal prática.

Desta maneira, pela argumentação supra, podem-se extrair duas sugestões para a regulamentação da matéria: i) que as pessoas tenham oportunidade de escolher livremente quais *cookies* desejam aceitar ou recusar (hipótese mais onerosa para a cadeia, mas mais garantidora) ou ii) que os *websites* e aplicativos de celular deixem de limitar integralmente o acesso caso não haja aceitação geral de todos os *cookies*, devendo liberar o acesso parcial e, somente para algumas áreas, vetar o acesso na hipótese de recusa ao tratamento dos dados (hipótese que permite maior liberdade e, mesmo assim, resguarda os princípios do livre consentimento).

4.6 A NATUREZA JURÍDICA DO CONSENTIMENTO NO ÂMBITO DO TRATAMENTO DE DADOS

Um dos pontos essenciais para entender o consentimento é compreender a sua natureza jurídica, pois em razão de ser um ato volitivo, uma demonstração de vontade afirmativa, surge a indagação se deverá ser classificado como um negócio jurídico.

No entanto, antes de adentrar na questão, a fim de permitir uma melhor abordagem sobre o tema, cumpre trazer ao texto expressão utilizada por Doneda[100] - “paradoxo de privacidade” -, que, para o respeitado autor, consiste na contradição de primeiro ter que se autorizar o tratamento dos dados, para depois valer-se da tutela, na hipótese de ter ocorrido alguma irregularidade no tratamento dos dados, ou esta ter sido realizada em desconformidade.

Por este lógico e correto entendimento, primeiro, deve ser outorgado o consentimento pela pessoa natural, para posterior tutela, fato este que traz grande relevância à natureza jurídica do consentimento.

Inclusive, neste sentido, Doneda[101] faz menção a uma hipótese em que o consentimento seria incentivado pelo próprio Estado, veja-se:

> Por outro lado, o consentimento pode ser incentivado pelo próprio Estados sob a (falsa) premissa de conceder aos cidadãos um instrumento forte e

[100] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 299.
[101] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 300.

> absoluto para determinar livremente a utilização dos dados pessoais – conforme Stefano Rodotà, o Estado assim teria um falso álibi para não intervir em uma situação na qual deveria agir positivamente na defesa de direitos fundamentais e, assim, “lavar as mãos”.

Pelo exposto, a premissa de que a pessoa natural poderia utilizar livremente seus dados pessoais e, por consequência, seria responsável pelos danos decorrentes da outorga, seria falsa, sendo que, na verdade, é o Estado o ente responsável por garantir o exercício dos direitos fundamentais, em especial o direito da personalidade no tratamento dos dados.

Neste ponto, consoante o entendimento anterior, cumpre trazer lição de Tepedino e Teffé[102], que assim esclarecem:

> Nas últimas décadas, a privacidade vem sendo gradualmente compreendida como direito de manter controle sobre as próprias informações, passando a fazer referência à possibilidade de a pessoa natural conhecer, controlar, endereçar e, até mesmo, interromper o fluxo das informações a ela relacionadas. Abriu-se, assim, espaço para a chamada autodeterminação informativa, que representa a faculdade de o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos a ele.
> Nessa perspectiva, a atenção voltou a se dirigir para o consentimento dos interessados, havendo uma evolução do consentimento implícito (situação em que se entende que uma pessoa consentiu com algo em razão da conduta que assume) para o consentimento informado, o qual orienta inclusive normas relativas à circulação de informações, visto que se manifesta em uma série de disposições que prescrevem quais devem ser as informações fornecidas ao interessado para que seu consentimento seja validamente expresso.

Por ser um tema novo, de uma legislação que acabou de entrar em vigor, resta claro que ainda haverá muito debate e divergência sobre a natureza jurídica do consentimento, sendo que Mendes[103], uma das coautoras do anteprojeto do Executivo da vigente Lei Geral de Proteção de Dados, não se furtou ao debate, e trouxe importantes considerações sobre o posicionamento da doutrina alemã, veja-se:

> A natureza do consentimento no âmbito do tratamento de dados pessoais é um tema bastante polêmico. Na Alemanha, existem três correntes principais: i) a primeira entende que o consentimento para o processamento de dados

[102] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 291.
[103] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 62.

> 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 o terceiro entendimento é o de que o consentimento para o tratamento de dados pessoais é um ato que se assemelha ao negócio jurídico, sem o ser (*geshäftsähnliche Handlung*). Este último posicionamento é atualmente o dominante e nos parece também ser o mais correto. Afinal, resta nítida a natureza atípica do consentimento para o processamento de dados, que tem características negociais, ao mesmo tempo em que possui também caráter personalíssimo.

Apesar de a autora esclarecer que a terceira corrente é a dominante, não resta clara a natureza jurídica do consentimento: primeiro, porque parece ululante a atipicidade da natureza jurídica, pois, se fosse típico, estaria certamente prescrito em algum ordenamento civil, portanto, não é questão de debate e, segundo, constatar que "é um ato que se assemelha ao negócio jurídico, sem o ser", igualmente, esclarece pouco ou praticamente nada.

De outro lado, a segunda corrente defende que o consentimento seria um ato jurídico unilateral, sem natureza negocial, o que de pronto o define, ao menos, como um ato jurídico, demonstrando estar mais de acordo com a intenção volitiva da pessoa natural, nos casos em que o consentimento é um dos requisitos para o tratamento dos dados pessoais.

No entanto, afirmar que o consentimento não teria natureza negocial parece negar as evidências, pois não seria crível que uma pessoa natural, voluntariamente, de forma livre, informada e inequívoca, ceda seus dados pessoais em troca de benefícios, sem ter que efetuar contraprestação em favor do controlador dos dados.

Vale dizer, não parece aceitável que o ato de uma pessoa natural fornecer os seus dados, que são uma parcela de sua personalidade, a uma terceira pessoa, como forma de pagamento, não tenha característica negocial.

Neste sentido, traz-se a lição de Mulholland[104], que entende que "todo consentimento representa aquiescência, assentimento, manifestação de vontade com vistas à produção de efeitos negociais".

---

[104] MULHOLLAND, Caitlin. Dados Pessoais Sensíveis e Consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. AASP. São Paulo, n.144, nov., 2019, p. 50.

Não obstante este entendimento, cumpre mencionar que Doneda[105] refuta em absoluto esta posição, pois entende que:

> [...] não parece apropriada a caracterização de uma natureza puramente negocial a esse consentimento. Se assim fosse, seria legitimada a inserção desse consentimento em estruturas contratuais, dificultando a sua valorização em função dos atributos da personalidade que estão em jogo.

No entanto, conferir entendimento de que a natureza jurídica do consentimento é negocial permite a vinculação a tutelas existentes e de fácil exercício à pessoa natural, de outra lado, entender de forma contrária, que estaria vinculado a direitos da personalidade, seria relegar ao Estado o exercício desta proteção.

Como parte da argumentação, não se pode olvidar, a título de exemplo, que a rede social *Facebook,* em 19 de fevereiro de 2014, comprou o aplicativo de mensagem *WhatsApp* pelo valor de US$16 bilhões[106], valor este que poderia chegar a US$19 bilhões, dependendo do pagamento de adicionais, sendo, portanto, uma das maiores transações da história até os dias de hoje, passados mais de 06 (seis) anos.

O *WhatsApp* surgiu como um aplicativo de troca de mensagens privadas, de celular para celular, com a garantia de que os dados não seriam revertidos para fins de publicidade, e que, após um ano de utilização, o usuário deveria pagar US$1,00 (um dólar) e assim, sucessivamente.

Ora, por qual razão a rede social se ofereceu a pagar tamanha quantia para um aplicativo de troca de mensagens, que até os dias de hoje não veicula publicidade e é baixado nos celulares gratuitamente? Ao que tudo aponta, para poder vincular os números de telefone de todos os usuários e transmiti-los às demais redes sociais da "Família *Facebook"*, como se intitulam.

O termo de condições[107] do *WhatsApp* deixa claro que as mensagens são "criptografadas de ponta a ponta, nós e terceiros, não podemos lê-las de maneira

---

[105] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais:** elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 302.

[106] UNIVERSO ON LINE. Facebook anuncia compra do aplicativo WhatsApp por US$16 bilhões. **UOL**, 2014. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2014/02/19/facebook-anuncia-compra-do-aplicativo-whatsapp.htm#:~:text=Facebook%20anuncia%20compra%20do%20aplicativo,%2F02%2F2014%20%2D%20UOL%20TILT. Acesso em: 01 out. 2020.

[107] WHATSAPP. **Termos de serviço do WhatsApp.** 2020. Disponível em: https://www.whatsapp.com/legal/?lang=pt_br&eea=0#terms-of-service. Acesso em: 01 out. 2020.

alguma", sendo que logo abaixo existem outras condições para que o aplicativo possa ser utilizado: a primeira, refere-se sobre o consentimento dos dados da lista de contatos do usuário e, a segunda, sobre o tratamento e transmissibilidade dos dados, veja-se:

> Lista de contatos. Você fornece os números de usuários do WhatsApp e de outros contatos em sua lista regularmente. Você confirma ter autorização para nos fornecer tais números de forma que possamos prestar nossos Serviços (grifo nosso).
> Empresas afiliadas
> Passamos a fazer parte da família de empresas do Facebook em 2014. Como parte desta família, o WhatsApp recebe e compartilha dados com os demais membros. Podemos usar os dados fornecidos por eles, e eles podem usar os dados compartilhados por nós para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços e as ofertas deles. Isso inclui a ajuda no aprimoramento dos sistemas de infraestrutura e entrega, a compreensão de como nossos Serviços ou os serviços deles são usados, a proteção dos sistemas e o combate a spam, abuso ou atividades que violem o uso lícito destes. O Facebook e outras empresas do mesmo grupo também podem usar dados do WhatsApp para fazer sugestões (por exemplo, de amigos, de contatos ou de conteúdo interessante) e mostrar ofertas e anúncios relevantes. No entanto, suas mensagens do WhatsApp permanecem privadas e não serão compartilhadas no Facebook para que outros vejam. Na verdade, o Facebook não usará suas mensagens do WhatsApp por qualquer motivo que não seja nos auxiliar na operação e na execução dos Serviços (grifo nosso).

Na data da transação, o *WhatsApp* tinha 450 milhões de usuários e o vulto da quantia chamou atenção, pois os múltiplos estavam muito díspares, tendo sido objeto de investigação pela *Federal Trade Commission* (FTC). A investigação apurou que o valor de US$19 bilhões fora uma "bagatela"[108], pois o tratamento dos dados elevou a remuneração inicialmente prevista de US$1,00 dólar por usuário para US$12,00 por usuário, ou seja, o tratamento dos dados multiplicou doze vezes a remuneração do aplicativo, caso fosse monetizado via pagamento[109].

A título de conhecimento, em 12 de fevereiro de 2020[110], o aplicativo de mensagens *WhatsApp* divulgou que é utilizado por 2 bilhões de pessoas, o que

---

[108] YAROW, Jay. The Chart That Shows WhatsApp Was A Bargain At $19 Billion. **Business Insider,** 2014. Disponível em: http://assets.businessinsider.com/price-per-user-for-whatsapp-2014-2. Acesso em: 01 out. 2020.
[109] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2020a, p. 30.
[110] LOUBAK, Letícia. WhatsApp ultrapassa 2 bilhões de usuários em todo o mundo. **TechTudo**., 2020. Disponível em: https://www.techtudo.com.br/noticias/2020/02/whatsapp-ultrapassa-2-bilhoes-de-usuarios-em-todo-o-mundo.ghtm. Acesso em: 01 out. 2020.

demonstra o quanto os dados são potencialmente mais lucrativos que a remuneração via cobrança por uso.

O exemplo trazido à tona tem o objetivo de expressar o consentimento como um negócio jurídico, ou seja, a existência do sinalagma do consentimento para o tratamento de dados, além de determinada vantagem patrimonial para a pessoa natural, pois se assim não fosse, não haveria a indústria dos dados.

Desta forma, urge questionar se o consentimento deve ser tratado como um negócio jurídico, do ponto de vista de proteção de interesses patrimoniais, ou sob outra ótica, a de proteção de direitos existenciais, sendo que para Rodotà[111]:

> [...] salvaguardas não deveriam ser baseadas em princípios que consideram o indivíduo somente ou principalmente como dono dos dados a seu respeito. O direito à proteção dos dados tem a ver com a proteção da personalidade, não da propriedade. Isto significa que certas categorias de dados, especialmente os de natureza médica e genética, não podem ser utilizados para fins negociais.

Embora as palavras de Rodotà, na opinião de Moraes[112], "constituem um farol, um guia, uma direção para todos os que se preocupam com os destinos da pessoa no mundo contemporâneo", pode-se manifestar o entendimento de que o consentimento deve ser entendido como um negócio jurídico, haja vista que é um dos fatos geradores da indústria dos dados e informação.

Feitas estas indagações, cabe pontuar que o Código Civil de 2002, no Livro III, da Parte Geral, dedica atenção aos atos jurídicos, tratando, a partir do artigo 104, especificamente do negócio jurídico.

Por negócio jurídico pode-se entender, para Chaves de Farias e Rosenvald[113], como o "acordo de vontades que surge da participação humana e projeta efeitos desejados e criados por ela. Há, nesse passo, uma composição de interesses com escopo negocial, visando criar, adquirir, transferir, modificar ou extinguir direitos".

---

[111] RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância** – A Privacidade Hoje. Rio de Janeiro: Renovar, 2008, p. 14.
[112] MORAES, Maria Celina Bodin de. Apresentação. *In:* RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.
[113] CHAVES DE FARIAS, Cristiano; ROSENVALD, Nelson. **Direito Civil**. Teoria Geral. 7. ed. Rio de Janeiro: Editora Lumen Juris, 2008, p. 426.

Não há como negar que os dados são ativos econômicos, os quais, quando tratados, fomentam a indústria da informação, aproximando os titulares dos dados (potenciais contratantes compradores) dos titulares dos bens de capital (potenciais contratantes vendedores de bens: móveis ou imóveis, tangíveis ou intangíveis, materiais ou imateriais etc.)

Os negócios jurídicos, quanto à manifestação de vontade, podem ser classificados como unilaterais, bilaterais e plurilaterais; desta forma, o consentimento, por ser um ato afirmativo da vontade, a princípio, poderia ser classificado como um ato unilateral; no entanto, deve-se indagar a que o consentimento se destina: ao simples fato de entregar seus dados ou ao recebimento de uma contraprestação do controlador que irá tratá-los?

Como solicitante do consentimento, o controlador manifesta em sua requisição à pessoa natural a intenção em contratar, pois ao receber os dados irá tratá-los, para uma finalidade específica, sendo que de outro lado está a pessoa natural, que tem por meio de seu aceite a “caneta” para o início da relação negocial.

Desta maneira, como há duas partes, com intenções idênticas de celebrar um negócio jurídico, mas com formas diferentes de realizá-los - pois uma irá ceder uma parcela de seus dados e a outra irá tratá-los, como forma de contraprestação -, entende-se pela existência de uma bilateralidade no negócio jurídico.

Quanto à vantagem patrimonial, os negócios jurídicos podem ser classificados como gratuitos (atos de liberalidade, vantagem sem impor uma contraprestação ao beneficiário), onerosos (há sacrifícios e vantagens patrimoniais para todos os contratantes), neutros (não há uma atribuição patrimonial determinada) e bifronte (tanto podem ser gratuitos como onerosos, dependendo da autonomia privada, como ocorre no contrato de mandato)[114].

Este é o ponto nevrálgico, pois, para o controlador que irá tratar os dados, não resta dúvida que há sacrifício e vantagem patrimonial em tratar os dados das pessoas naturais, pois, se assim não fosse, não haveria a indústria da informação; no entanto, apesar de o dado pessoal tratar de características da personalidade, ou melhor, de todos os caracteres que a pessoa é para si, e para a sociedade, não há como negar

[114] GOMES, Orlando. **Contratos**. 26 ed. Rio de Janeiro: Editora Forense, 2007, p. 83-159.

que estas informações (dados) são passíveis de serem remuneradas e, portanto, o ato volitivo de consentir, em ceder seus dados, pode ser entendido como um sacrifício também para a pessoa natural, em prol de receber uma contraprestação.

Com relação aos efeitos, no aspecto temporal, o consentimento é um ato *inter vivos*, pois é destinado a produzir efeitos durante a vida dos negociantes.

De outro lado, cumpre mencionar que a lei não é taxativa ao classificar os dados pessoais e os dados pessoais sensíveis à pessoa natural viva, sendo, no entanto, este o entendimento expressado por Pinheiro[115].

Quanto à necessidade ou não de solenidade e formalidade, este negócio jurídico deve ser classificado como informal ou não solene, sendo inclusive livre ao controlador dos dados demonstrar a ocorrência do consentimento da pessoa natural (art. 8°, §2°).

De modo simultâneo, é preciso classificar se o consentimento é um negócio jurídico impessoal, em que a prestação não depende de qualquer condição especial dos envolvidos, podendo ser cumprida tanto pelo obrigado, como por terceiro, ou *intuitu personae*, em que há uma obrigação infungível. Em análise ao inciso XII, art. 5° e art. 6°, I, depreende-se que o consentimento está vinculado a uma finalidade específica, que deverá ser cumprida por um controlador específico, razão pela qual entende-se ter caráter personalíssimo.

Em adição, há necessidade de classificar quanto ao momento do aperfeiçoamento, se real ou consensual. Os negócios jurídicos reais geram efeitos a partir da entrega do objeto do bem jurídico tutelado; desta maneira, parece mais adequado classificar como um negócio jurídico consensual, em que o consentimento gera efeitos a partir do momento em que há o acordo de vontade, ou seja, a partir do aceite.

Em companhia destas classificações, não se pode deixar de analisar em face das extensões dos efeitos, ou seja, se constitutivos ou declarativos. Por ato constitutivo, pode se entender aquele que gera efeito *ex nunc*, a partir da conclusão; de outro lado, por efeito declarativo, se entende o negócio jurídico que gera efeito *ex*

---

[115] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020a, p. 36.

tunc, ou a partir do momento do fato que constitui seu objeto. Portanto, da imediatidade do tratamento dos dados pelo controlador, não há dúvida que se trata de um ato com efeito *ex nunc*, ou seja, constitutivo.

Ainda não há como deixar de analisar quanto à independência ou autonomia do consentimento. Os negócios jurídicos independentes são aqueles que tem "vida própria" e não dependem de nenhum outro negócio jurídico; de outro lado, os negócios jurídicos acessórios estão subordinados a outros. Em razão do consentimento ser um requisito para o tratamento dos dados, outro não pode ser o entendimento senão um negócio jurídico principal ou independente.

Por último, mas não menos importante, o consentimento deve ser analisado quanto à causa determinante, se material ou formal. De acordo com Gomes, os negócios jurídicos causais ou materiais são aqueles em que os motivos de sua realização constam expressamente de seu conteúdo; já nos abstratos ou formais, em oposição, as razões não constam em seu teor[116]. Assim, mais uma vez, o atributo da finalidade faz entender que o consentimento quanto à causa determinante é um negócio causal ou material.

Pela exposição, pode-se classificar o consentimento como um negócio jurídico: i) bilateral, quanto à manifestação da vontade; ii) oneroso, quanto à vantagem patrimonial; iii) *inter vivos*, quanto ao aspecto temporal; iv) informal, quanto à necessidade de solenidade; v) principal ou independente, quanto à autonomia; vi) personalíssimo ou *intuitu personae*, quanto às condições dos negociantes; vii) causal ou material, quanto à causa determinante; viii) consensual, quanto ao momento do aperfeiçoamento; e ix) constitutivo, quanto à extensão dos efeitos.

Em síntese, abalizada doutrina, como Rodotà, Tepedino e Mendes, entende que o consentimento não deve ser compreendido como de natureza negocial, ou seja, compreendido em uma "visão da privacidade, como uma liberdade negativa que confie ao indivíduo a autodeterminação de sua esfera privada, o consentimento é o instrumento por excelência para o exercício desse poder[117]".

---

[116] GOMES, Orlando. **Contratos**. 26 ed. Rio de Janeiro: Editora Forense, 2007, p. 83-159.
[117] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 298.

A despeito desse entendimento, cabe mencionar, mais uma vez, a opinião de Mendes[118], que traz lição de Kothe, para quem o consentimento deve ser como um negócio jurídico, aplicáveis as regras do contrato, veja-se:

> A função do consentimento para o tratamento de dados pessoais é a mesma da declaração de vontade no âmbito do negócio jurídico, pois ambos visam à autodeterminação da pessoa. Nesse sentido, é possível aplicar as regras referentes aos negócios jurídicos e contratos em geral a esse consentimento, sempre que essa aplicação mostrar-se cabível e adequada.

Em síntese, a despeito do gabarito dos autores que entendem que o consentimento não deve ser classificado como um negócio jurídico, mesmo em corrente minoritária há autores que se contrapõem a este pensamento, permitindo, portanto, a classificação e a tutela nos moldes dos atos contratuais.

De outra lado, o consentimento deve ser entendido como um ato revogável: a uma, sendo um ato relacionado à personalidade, entre os seus atributos estaria a indisponibilidade, o que por si só caracteriza o ato como revogável; e a outra, sendo um ato negocial, tem por característica a permissibilidade de revogação dos negócios jurídicos.

Inclusive a Lei Geral de Proteção de Dados, no art. 8°, § 5°, prevê como um dos direitos do titular a possibilidade de revogação do consentimento para o tratamento dos dados pessoais.

Não se pode deixar de mencionar que o ato de revogar o consentimento pode ser passível de indenização, na hipótese dessa conduta caracterizar dano a quem anteriormente recebeu a concessão para tratar os dados pessoais.

Além disso, este é mais um fundamento para que o consentimento possa ser classificado como um ato negocial, sem furtar-se ao entendimento de que, na hipótese de ser classificado como um direito da personalidade, a verificação de abusividade na revogação deverá ser guiada pelos mecanismos do abuso de direito ou do *venire contra factum proprium*.

---

[118] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor:** linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014, p. 63.

Em síntese, a lei deixa clara a permissibilidade da revogação do consentimento, sendo que as consequências deste ato, se abusivo for, devem proporcionar ~~a~~ indenização a quem de direito.

CONCLUSÃO

Deve-se entender o consentimento como uma das bases legais do tratamento de dados pessoais, segundo o qual a pessoa natural, no exercício de sua autonomia individual e no controle de seu direito de personalidade, expressa de maneira livre, informada e inequívoca a concordância em relação ao tratamento de seus dados.

Não seria exagero afirmar que o consentimento, por ser uma proposição discricionária que coloca a pessoa natural no centro da decisão, em exercício de sua autonomia privada, transparece a ideia de ser a mais importante base legal do tratamento de dados pessoais.

Inclusive, no marco regulatório da Lei Geral de Proteção de Dados, o consentimento figura no inciso I, do artigo 7º, como primeiro requisito, dentre os demais, para que o tratamento de dados possa ser realizado.

Desde o artigo de Warren Samuel e Brandeis Louis, que provocou as primeiras reflexões sobre o direito à privacidade, como o direito de ficar sozinho, de caráter formalmente individualista, concebido como um direito negativo, que conferia à pessoa natural o direito de ficar só e de o Estado não interferir em sua esfera privada, o consentimento era a pedra de toque.

De um direito negativo no século XIX, este direito sofreu mutação no decorrer do século XX, para ser considerado um direito positivo, devido à alteração da função do Estado, associado à evolução da tecnologia que contribuiu para modificar o conteúdo e o sentido do direito à privacidade.

Percebe-se essa evolução no ordenamento jurídico brasileiro, que apesar de não prescrever propriamente proteção à privacidade, de forma oblíqua garante a sua efetividade, pois a Constituição Federal, em seu artigo 5º, inciso X, prescreve que “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”. O Código Civil, ademais, em seu artigo 21, determina que “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”.

Neste sentido, o direito à privacidade está diretamente ligado a um direito subjetivo e discricionário da pessoa natural e, por consequência, o consentimento seria uma ferramenta condizente ao seu exercício.

De forma a fazer coro a este entendimento, o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, lei anterior à Lei Geral de Proteção de Dados, e que cuidava do tratamento de dados no âmbito on-line, impôs que, para o exercício de qualquer atividade envolvendo dados pessoais, dever-se-ia obter o consentimento de seu titular, que por sua vez, deveria ser livre, expresso e informado.

Em razão desta previsão legislativa, a parte que processava os dados teria a obrigação de obter o consentimento expresso, livre e informado, e o titular dos dados o direito à sua autodeterminação informacional, fundada na perspectiva de ter o controle sobre suas informações pessoais.

A intenção do legislador pode ser transportada para o papel, mas isto não impede a dissonância da lei com a realidade, pois firmar um modelo regulatório de proteção de dados pessoais para a *internet,* no qual se exige, para a efetividade do consentimento, a exigência cumulativa de três adjetivos (livre, expresso e informado) é propagar letra morta.

De fácil percepção a qualquer pessoa que utiliza a internet, que os termos e condições, manifestados por um simples aceite, não configuram um consentimento livre, expresso e informado, mas, muito pelo contrário, mascaram um falso consentimento e aumentam a assimetria de poder.

O Marco Civil da Internet, ao atribuir ao consentimento o principal elemento para garantir a proteção do usuário, falhou, pois ainda estava vinculado ao pensamento do século XIX, em que a proteção da privacidade era um direito subjetivo.

Não se pode olvidar que a proteção de dados está vinculada ao direito à privacidade, mas, igualmente, não se pode esquecer que a proteção de dados evoluiu e se deslocou para se tornar um direito autônomo e, inclusive, mais amplo que o direito à privacidade.

O direito à privacidade, de ordem subjetiva, se relacionava a tópicos e situações específicas, em que se podia enxergar o ponto nevrálgico, e determinar ou não o aceite; de outra ordem, dados pessoais representam conotação primitiva e

fragmentada, que de princípio, sequer se pode vincular a informação a uma determinada pessoa natural, sem a prévia realização do tratamento.

O dado pessoal pode ser compreendido como uma pré-informação, um conhecimento em potência, que não se desenvolveu completamente, que aguarda um trabalho para ser decifrado, que transmite a amplitude de proteção para uma informação latente; portanto, sem correlação imediata à determinada pessoa natural, sendo esta a razão para não ter o mesmo atributo do direito à personalidade.

Em evolução bem-vinda ao Marco Civil da Internet, a Lei Geral de Proteção de Dados ampliou o centro gravitacional para o tratamento de dados, pois, para a lei da *internet,* era fundamental a obtenção de consentimento livre, expresso e informado, para que pudesse ser realizado; já a lei geral classificou em dez as bases de dados (cinco para o setor privado e cinco para o setor público), sem hierarquia, para o tratamento de dados pessoais.

Como o referencial normativo anterior era fundado no consentimento, havia uma fratura entre o modelo regulatório teorizado e a proteção de dados pessoais efetiva, razão pela qual não se deve atribuir ao consentimento um caráter de primazia na Lei Geral de Proteção de Dados Pessoais.

Há necessidade de se equilibrar a balança e recalibrar o peso atribuído ao consentimento, pois a pessoa natural que declina o seu aceite no tratamento, muitas das vezes, o faz por fadiga, desconhecimento ou até mesmo ciente de que os termos informados são contrários à sua concordância, mas, que por não haver outra solução, manifesta seu aceite.

Deve-se fazer uma leitura da Lei Geral de Proteção de Dados como uma moeda, em que uma das faces, voltada para as organizações, contém o *elemento segurança*, pois há o esclarecimento de quais são os requisitos a cumprir para o tratamento de dados. Do outro lado, dirigido às pessoas naturais, pode-se observar o *elemento direito*, para que estas possam exercer não propriamente o direito à privacidade, pois este não é o objetivo da lei, mas para que possam exercer o direito de controle de seus próprios atos.

Interpretar o consentimento como a principal base no tratamento de dados seria conferir atributo maior do que aquele previsto em lei, pois: (i) o direito ao tratamento

dos dados pessoais é um direito diferente do direito à privacidade, do qual se originou e evoluiu, e (ii) a subjetividade não está no plano de vocação da lei, que conferiu bases objetivas e seguras ao tratamento dos dados pessoais.

A massificação do tratamento não permite a existência de um vetor subjetivo, em razão do dinamismo das relações entre as pessoas naturais e as organizações que irão tratar os dados.

Até mesmo em situações do cotidiano, o consentimento perde sua importância, pois seria impossível imaginar, em um rol de um prédio comercial, exigir do visitante a assinatura de um termo de consentimento para autorizar a coleta de foto e a cópia de seu documento de identidade. O interesse legítimo do controlador (art. 7º, IX) supre de forma elegante a requisição do consentimento, pois está umbilicalmente atrelado ao princípio da finalidade (art. 6º, I), isto sem mencionar o princípio da boa-fé.

Desta forma, nos dias atuais, a enorme maioria dos tratamentos de dados no setor privado se dão sem a outorga do consentimento, mas ao invés, por legítimo interesse, cumprimento de obrigação legal ou regulatória, execução de contrato ou proteção de crédito.

Existe um abismo entre imaginar o consentimento como um instrumento regulatório principal, núcleo central de legitimidade, e o modelo regulatório do consentimento na Lei Geral de Proteção de Dados. Seria possível fazer a pessoa natural ler os termos e políticas de privacidade, se o mesmo não tem disposição para fazê-lo? Seria razoável impor à organização que irá trabalhar os dados da pessoa natural criar subterfúgios, na expectativa de que a pessoa natural leia ou tenha disposição para ler os termos de privacidade? Ou seria mais fácil desvincular a base legal de tratamento do consentimento, para a do legítimo interesse ou cumprimento de obrigação legal?

Com o deslocamento do tratamento de dados pessoais do consentimento para o legítimo interesse ou cumprimento de obrigação legal, evita-se o discurso falso e a sensação de inaplicabilidade da lei, que permeia cada pessoa natural que confere o “de acordo” nos *websites* em que ingressa.

O consentimento está diretamente ligado à autonomia da vontade (no sentido de determinar algo para si), com relação à intenção de ler os termos e disposições de

tratamento de dados pessoais, sendo, neste caso, a vontade de dispensar um consentimento consciente. O direito à proteção de dados pessoais, além de utilizar o consentimento, para estas hipóteses, deve se valer das demais bases legais de tratamento e dos princípios prescritos na lei, a fim de obrigar as entidades que irão tratar os dados pessoais a ter um real vetor de proteção.

O direito da personalidade evoluiu, de seu caráter subjetivo e individual, para o tratamento de dados, de característica objetiva, que tem correlação com o tratamento em grande escala por sistemas de computadores poderosos que evoluem a cada dia; assim, não há espaço na atual sociedade da informação para se buscar o consentimento, na maioria das hipóteses de tratamento de dados, pois a dinâmica e a velocidade da informação a impossibilitam.

Vale ressaltar, por fim, que o presente trabalho buscou demonstrar que o consentimento perdeu seu núcleo central de protagonismo, seja pela dinâmica da sociedade ou mesmo pela massificação no tratamento de dados, devendo o aplicador do direito revisitar seus conceitos, em especial o paradigma do consentimento, para que utilize as outras bases legais de tratamento de dados pessoais previstas na Lei Geral de Proteção de Dados Pessoais, como o legítimo interesse ou o cumprimento de obrigação legal.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. 2. ed. 5. tir. São Paulo: Ed. Malheiros, 2017.

ARGENTINA. **Proteccion de los datos personales, Ley 25.326**. Buenos Aires: Congreso Argentino, 30 out. 2000. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf. Acesso em: 30 jan. 2021.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: Os conceitos fundamentais e a construção do novo modelo. 8. ed. São Paulo: Saraiva, 2018.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Rio de Janeiro: Ed. Zahar, 2014.

BELLEIL, Arnaud. **@-Privacidade:** O Mercado dos Dados Pessoais: Protecção da Vida Privada na Idade da Internet. Lisboa: Dunod, 2001.

BIONI, Bruno Ricardo. **Xeque-Mate**. O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI, USP, 2015. Disponível em: https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 31 ago. 2020.

BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. **AB2L**, 2018. Disponível em: https://ab2l.org.br/de-2010-2018-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados/. Acesso em: 29 de ago. 2020.

BIONI, Bruno Ricardo. Abrindo a “Caixa de Ferramentas” da LGPD para dar Vida ao Conceito ainda Elusivo de *Privacy by Design*. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 239-260.

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

BIONI, Bruno Ricardo. **LGPD: O Essencial**. Data Privacy Brasil, 2020b. Curso on-line, Módulo II, Parte 2, Cenário prévio: um quebra-cabeça regulatório denominado. Disponível em: https://dataprivacy.com.br/curso/curso-online-protecao-de-dados-pessoais-muito-alem-da-lgpd/. Acesso em: 04 set. 2020.

BOBBIO, Norberto. **O Futuro da Democracia:** Uma Defesa das Regras do Jogo. 15. Edição. São Paulo: Paz & Terra, 2018.

BORGESIUS, Frederik J. Zuiderveen *et al.* **Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation.** Universiteit Van Amsterdam, 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 14 out. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**, Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jul. 2020.

BRASIL. **Projeto de Lei 2.796, Câmara dos Deputados**, 1980. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD557906FEB1829EFEA68AED.proposicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 05 fev. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso em Habeas-Data: RHD 22 DF**. Relator: Min. Marco Aurélio. Voto do Min. Sepúlveda Pertence. Data de Julgamento: 19/09/1991. Data de Publicação: DJ 01-09-1995.

BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Extraordinário 22.337-8/RS**. Data do Julgamento 13/02/1995. Publicado no DJ de 20/03/1995, p. 6119, RSTJ vol. 77, p. 205, Registro nº 92.0011446-6, Relator Ministro Ruy Rosado de Aguiar. Disponível em https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=199200114466. Acesso em: 30 jan. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso em Habeas-Data: RHD 22 DF**. Relator: Min. Marco Aurélio. Voto do Min. Celso de Mello. Data de Julgamento: 19/09/1991. Data de Publicação: DJ 01-09-1995, p. 3. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=362613. Acesso em: 28 jan. 2021.

BRASIL. **Discurso da Presidenta da República, Dilma Rousseff**, por ocasião do Debate Geral da 68ª Assembleia Geral das Nações Unidas. Brasília: Ministério das Relações Exteriores, 2013. Disponível em: https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/presidente-da-republica/presidente-da-republica-federativa-do-brasil-discursos/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas. Acesso em: 28 ago. 2020.

BRASIL. Superior Tribunal de Justiça. Segunda Seção, **REsp: 1457199 RS 2014/0126130-2**, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 12/11/2014, Data de Publicação: DJe 17/12/2014.

BRASIL. Superior Tribunal de Justiça. **REsp: 1457199 RS 2014/0126130-2**, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 12/11/2014, S2 – Segunda Seção, Data de Publicação: DJe 17/12/2014. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/158643665/recurso-especial-resp-1457199-

rs-2014-0126130-2/certidao-de-julgamento-158643667?ref=juris-tabs. Acesso em: 28 ago. 2020.

BRASIL. **Proposta de Emenda Constitucional n° 17**, de 2019, Senado Federal, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 24 jul. 2020.

BRASIL. **Projeto de Lei 4060/2012**, Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 05 set. 2020.

BRASIL. **Código Civil**, Presidência da República, ano 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm#art65. Acesso em: 24 abr. 2020.

BRASIL. **Lei 13.709, de 14 de agosto de 2020, Lei Geral de Proteção de Dados**, Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 19 set. 2020.

BRASIL. **Lei 14.058, de 17 de setembro de 2020,** Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14058.htm. Acesso em: 19 set. 2020.

BRASIL. **Projeto de Lei 4723/2020**, Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/noticias/696533-projeto-determina-que-dados-pessoais-de-brasileiros-sejam-armazenados-no-territorio-nacional/?mkt_tok=eyJpIjoiTUdGbU9EbGxaamhsWm1KaiIsInQiOiJHNVdsN3FFaXlVV2dNa2hTajd5S2pXWTJJTTRTWURaZkxoR0lpMkhYZDFzcExFM3d3OExzTzRaOGo5TFJtTXVKRVFtN2s5WFBFY2JFRXFCaXIzd1dWTnFadlA0VGI5TThqcjZ2ZnJuclwvczYzdjNJWTN1VU9WY0oyNUlxbGQyRVwvIn0%3D. Acesso em: 14 out. 2020.

BRASIL. **Resolução CGI.br/RES/2009/003/P**, 2020. Disponível em: https://www.cgi.br/resolucoes/documento/2009/003/#:~:text=Liberdade%2C%20privacidade%20e%20direitos%20humanos,uma%20sociedade%20justa%20e%20democr%C3%A1tica.. Acesso em: 05 set. 2020.

BRASIL. **Resolução n. 4658**. Banco Central do Brasil, 26 abr. 2018. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 30 jan. 2021.

BRASIL. Senado Federal. **Assessoria de Imprensa**, 2020. Disponível em https://www12.senado.leg.br/assessoria-de-imprensa/notas/nota-de-esclarecimento-vigencia-da-lgpd. Acesso em: 20 set. 2020.

BRASIL. Senado Federal. **Regimento Interno**, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/regimento-interno. Acesso em: 20 set. 2020.

BRASIL. Ministério da Justiça. **Anteprojeto de Lei para a Proteção de Dados Pessoais**. Pensando o Direito. Disponível em: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em: 05 set. 2020.

BRASIL. **Ministério das Relações Exteriores**. Disponível em: http://www.itamaraty.gov.br/pt-BR/discursos-artigos-e-entrevistas-categoria/presidente-da-republica-federativa-do-brasil-discursos/5898-discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas-nova-iorque-estados-unidos-24-de-setembro-de-2013. Acesso em: 28 ago. 2020.

CALIFORNIA. Legislative Information. **California Consumer Privacy Act of 2018** [1798.100 – 1798.199]. Disponível em: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 19 set. 2020.

CALIFORNIA. Department Of Justice. Attorney General. **California Consumer Privacy Act (CCPA)**. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 19 set. 2020.

CAKEBREAD, Caroline. You’re not alone, no one reads terms of service agreements. **Businessinsider,** 2017. Disponível em: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11. Acesso em: 10 out. 2020.

CÂMARA DOS DEPUTADOS. **Projeto de Lei 4723/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2263413. Acesso em: 07 out. 2020.

CAMBI, Eduardo. **Neoconstitucionalismo e Neoprocessualismo**: Direitos Fundamentais, Políticas Públicas e Protagonismo Judiciário. São Paulo: Ed. Almedina, 2016.

CASTELLS, Manuel. **A Era da Informação:** Economia, Sociedade e Cultura. v. 1: A Sociedade em Rede. São Paulo: Ed. Paz & Terra, 2020.

CHUNG, Kenny. Personal Data And 33 Bits of Entropy. **Synchlaw**., s.d. Disponível em: https://synchlaw.se/personal-data-and-33-bits-of-entropy/. Acesso em: 07 set. 2020.

CREEMERS, Rogier *et al.* China's Draft 'Personal Information Protection Law' (Full Translation). **New America,** 2020. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/. Acesso em: 06 fev. 2021.

DANTAS, Bruno. A Análise Econômica do Direito Pode Auxiliar no Cálculo da Indenização Por Dano Moral? *In:* **Estudos Jurídicos em Homenagem ao Ministro Cesar Asfor Rocha**, v. I. Ribeirão Preto: Ed. Migalhas, 2012, p. 198-216.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III**: Marco Civil da Internet Lei n° 12.965/2014. São Paulo: Quartier Latin, 2015.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. **Direito & Internet IV:** Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

DE LUCCA, Newton; MACIEL, Renata Mota. A Lei n° 13.709, de 14 de Agosto de 2018: a Disciplina Normativa que Faltava. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 21-50.

DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, ano 4, n. 16, out./dez., 2003.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019a.

DONEDA, Danilo; MACHADO, Diego. **A Criptografia no Direito Brasileiro**. São Paulo: Thompson Reuters Revista do Tribunais, 2019b.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz; BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2020, p. 03-20.

DWORKIN, Ronald. **O Império do Direito**. 3. ed. São Paulo: Martins Fontes.

ECO, Umberto. **Como se Faz Uma Tese**. 26. ed. São Paulo: Ed. Perspectiva, 2016.

ESTADO DE MINAS. STJ confirma legalidade de sistema de score de crédito. **Jornal Estado de Minas**, 2014. Disponível em: https://www.em.com.br/app/noticia/economia/2014/11/12/internas_economia,589362/stj-confirma-legalidade-de-sistema-de-score-de-credito.shtml. Acesso em: 13 set. 2020.

EUROPEAN UNION. **Judgment in Case C-582/14**. Court of Justice of the European Union. Luxembourg, 19 oct. 2016. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.pdf. Acesso em: 05 set. 2020.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Direito Civil**. Teoria Geral. 7. ed. Rio de Janeiro: Editora Lumen Juris, 2008.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados.** Lei 13.709/2018. São Paulo: Ed. Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial e Direito:** Ética, Regulação e Responsabilidade. São Paulo: Thompson Reuters Revista dos Tribunais, 2019.

FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 99-129.

G1 GLOBO. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA, **Portal G1,** 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 29 ago. 2020.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil**. Contratos: Teoria Geral. v. IV, t. 1, 5. ed. São Paulo: Editora Saraiva, 2009.

GOMES, Orlando. **Contratos**. 26 ed. Rio de Janeiro: Editora Forense, 2007.

GRAU, Eros Roberto. **Por Que Tenho Medo Dos Juízes** (a interpretação/aplicação do direito e os princípios). 9. ed. São Paulo: Ed. Melhoramentos, 2018.

HAN, Byung-Chul. **Agonia de Eros**. 2. reimp. Rio de Janeiro: Ed. Vozes, 2019.

HOLANDA, Sérgio Buarque de. **Raízes do Brasil.** 27. ed. 9. reimp. São Paulo: Companhia das Letras, 2019.

INGRAM, David. Factbox: Who is Cambridge Analytica and what did it do? **Reuters**, 2018. Disponível em: https://www.reuters.com/article/idUSKBN1GW07F. Acesso em: 29 ago. 2020.

INTERNATIONAL PHOTOGRAPHY HALL OF FAME AND MUSEUM. George Eastman: 1854-1932. **IPHF**. Disponível em: https://iphf.org/inductees/george-eastman/. Acesso em: 21 jul. 2020.

JABUR, Gilberto Haddad. A Dignidade e o Rompimento de Privacidade. *In:* MARTINS, Ives Gandra da Silva; PEREIRA JR, Antonio Jorge. **Direito à Privacidade**. 1. ed. Aparecida: Editora Ideias & Letras, 2005, p.85-106.

LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado*. In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 317-331.

LEVY, Wilson. **Teoria Democrática e Reconhecimento**. Curitiba: Ed. Juruá, 2012.

LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. A Proteção dos Dados Pessoais na Fase de Coleta: Apontamentos sobre a Adjetivação do Consentimento Implementada pelo Artigo 7, Incisos VIII e IX do Marco Civil da Internet a Partir da *Human Computer Interaction* e da *Privacy By Default*. *In*: DE LUCCA, Newton;

SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (coord.). **Direito & Internet III**. Marco Civil da Internet Lei n° 12.965/2014. São Paulo: Quartier Latin, 2015.
LIMA, Cíntia Rosa Pereira de. Consentimento inequívoco versus expresso: o que muda com a LGPD? **Revista do Advogado**. AASP. São Paulo, n.144, nov., 2019.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados Pessoais e a Efetividade da Lei Geral de Proteção de Dados**. São Paulo: Ed. Almedina, 2020a.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Ed. Almedina, 2020b.

LISBOA, Roberto Senise. Boa-fé e Confiança na Lei Geral de Proteção de Dados Brasileira. **Revista do Advogado**. AASP. São Paulo, n.144, nov., p.74-79, 2019.

LOUBAK, Letícia Ana. WhatsApp ultrapassa 2 bilhões de usuários em todo o mundo. **TechTudo**, 2020. Disponível em: https://www.techtudo.com.br/noticias/2020/02/whatsapp-ultrapassa-2-bilhoes-de-usuarios-em-todo-o-mundo.ghtml. Acesso em: 01 out. 2020.

LOWY INSTITUTE. Covid Performance Index. Deconstructing Pandemic Responses. **Lowy Institute,** 2021. Disponível em: https://interactives.lowyinstitute.org/features/covid-performance/. Acesso em: 03 fev. 2021.

MACKAAY, Ejan; ROUSSEAU, Stéphane. **Análise Econômica do Direito**. 2. ed. 2. tir. São Paulo: Atlas, 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Editora Thomson Reuters, 2019.

MARCACINI, Augusto Tavares Rosa. Considerações sobre a Proteção à Privacidade e aos Dados Pessoais em uma Sociedade Digital. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV.** São Paulo: Quartier Latin, 2019, p. 129-146.

MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman de Vasconcellos; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. 2. ed. Porto Alegre: Editora Revista dos Tribunais, 2006.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. **Direito Digital:** Direito Privado e Internet; 2. ed. Indaiatuba: Editora Foco, 2019.

MELLO, Celso Antonio Bandeira de. **O Conteúdo Jurídico do Princípio da Igualdade.** 3. ed. 25. tir. São Paulo: Editora Melhoramentos, 2017.

MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz; BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2020.

MEZZAROBA, Orides; MONTEIRO, Cláudia Servilha. **Manual de Metodologia da Pesquisa no Direito**. 8. ed. São Paulo: Saraiva, 2019.
MORAES, Maria Celina Bodin de. Apresentação. *In:* RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.

MULHOLLAND, Caitlin. Dados Pessoais Sensíveis e Consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. AASP. São Paulo, n.144, nov., p. 47-53, 2019.

NATHAN, Andrea. O que é a caixa de Pandora? Entenda a origem do mito – e descubra o que tinha lá dentro, **Revista Super Interessante,** 2018. Disponível em: https://super.abril.com.br/historia/o-que-e-a-caixa-de-pandora/. Acesso em: 12 out. 2020.

NEVES, Marcelo. **Transconstitucionalismo.** São Paulo: Ed. WMF Martins Fontes, 2009.

OECD. Education at a Glance 2020. **OCDE**, 2020. Disponível em: https://www.oecd.org/education/education-at-a-glance/. Acesso em: 03 fev. 2021.

OLIVEIRA, Ricardo; COTS, Márcio. **O Legítimo Interesse e a LGPDP**. São Paulo: Ed. Revista dos Tribunais, 2020.

PASQUALE, Frank. **The Black Box Society**. The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015. Disponível em: https://www.semanticscholar.org/paper/The-Black-Box-Society%3A-The-Secret-Algorithms-That-Pasquale/16d48c78afb6a9880486ce1b2111a611b4007557. Acesso em: 22 out. 2020.

PATEL, Nell. How Netflix Uses Analytics to select movies, create content, and make multimillion dollar decisions. **Neilpatel**. Disponível em: https://neilpatel.com/blog/how-netflix-uses-analytics/. Acesso em: 07 set. 2020.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020a.

PINHEIRO, Patrícia Peck. **Segurança Digital**. Proteção de Dados nas Empresas. São Paulo: Editora Atlas, 2020b.

PODESTÁ, Fabio Henrique. A Privacidade e o Consentimento (Informado) em Face da Nova Lei de Proteção de Dados. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p. 81-103.

RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância** – A Privacidade Hoje. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 4. ed. São Paulo: Saraiva, 2015.

SEVERINO, Antônio Joaquim. **Metodologia do Trabalho Científico**. 24. ed. São Paulo: Cortez, 2016.

SIMÃO FILHO, Adalberto. Regime Jurídico do Banco de Dados – Função Econômica e Reflexos na Monetização. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. (coord.). **Direito & Internet IV**. São Paulo: Quartier Latin, 2019, p.167-203.

SMITH, Adam. A Mão Invisível. 1. reimp. São Paulo: Penguim Classics/Companhia das Letras, 2017.

SOMBRA, Thiago Luís Santos. **Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais:** Pluralismo Jurídico e Transparência em Perspectiva. São Paulo: Thomson Reuters Revista dos Tribunais, 2020.

STOLTON, Samuel. **TikTok unclear on how old EU data will be transferred to new Irish data centre**. Euractiv.com, 23 set. 2020. Disponível em: https://iapp.org/news/a/tiktok-clarifies-plans-for-eu-info-when-irish-data-center-launches/. Acesso em: 07 out. 2020.

TARTUCE, Flávio. **Direito Civil:** Teoria Geral dos Contratos e Contratos em Espécie. 4. ed. v. 3. São Paulo: Editora Método, 2009.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Revista dos Tribunais, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 287-322.

TEPEDINO, Gustavo; OLIVA, Milena Donato. **Fundamentos do Direito Civil**. v.1: Teoria Geral do Direito Civil. Rio de Janeiro: Ed. Forense, 2020.

UNIVERSO ON LINE. Facebook anuncia compra do aplicativo WhatsApp por US$16 bilhões. **UOL**, 2014. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2014/02/19/facebook-anuncia-compra-do-aplicativo-whatsapp.htm#:~:text=Facebook%20anuncia%20compra%20do%20aplicativo,%2F02%2F2014%20%2D%20UOL%20TILT. Acesso em: 01 out. 2020.

URUGUAI. **Ley N° 18331 Ley de proteccion de datos personales**. Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 30 jan. 2021.

U. S. Department of Commerce. Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States. **U. S. Department of Commerce,** 2020. Disponível em: https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect. Acesso em: 19 set. 2021.

VAIDHYANATHAN, Siva. **A Googletização de Tudo:** E Por Que Devemos Nos Preocupar. 10. ed. São Paulo: Ed. Cultrix, 2018.

VAINZOF, Rony. **Lei Geral de Proteção de Dados Comentada**. 2. ed. rev. atual. amp. São Paulo: Revista dos Tribunais, 2019, p.117.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, Dec.15, 1890, Boston. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 21 jul. 2020.

WHATSAPP. **Termos de serviço do WhatsApp.** 2020. Disponível em: https://www.whatsapp.com/legal/?lang=pt_br&eea=0#terms-of-service. Acesso em: 01 out. 2020.

WOLKART, Erik Navarro. **Análise Econômica do Processo Civil:** Como a Economia, O Direito e a Psicologia Podem Vencer a Tragédia da Justiça. São Paulo: Thompson Reuters Brasil, 2019.

YAROW, Jay. The Chart That Shows WhatsApp Was A Bargain At $19 Billion. **Business Insider,** 2014**.** Disponível em: http://assets.businessinsider.com/price-per-user-for-whatsapp-2014-2. Acesso em: 01 out. 2020.