UNIVERSIDADE FEDERAL DE MINAS GERAIS
Programa de Pós Graduação em Inovação Tecnológica
Mestrado Acadêmico em Inovação Tecnológica

Lucas Martins Gama

O TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES: uma Análise do Consentimento Parental na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Belo Horizonte
2023

Lucas Martins Gama

O TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES: uma Análise do Consentimento Parental na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Dissertação apresentada junto ao Programa de Pós-Graduação em Inovação Tecnológica pela Universidade Federal de Minas Gerais – UFMG, vinculada à Área de Concentração "Gestão da Inovação, Propriedade Intelectual e Empreendedorismo", na linha de pesquisa "Sistemas de inovação e de desenvolvimento: aspectos jurídicos, econômicos e sociais", após o desenvolvimento do Projeto de Pesquisa "PROTEÇÃO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES: uma análise do consentimento parental da Lei 13.709/2018", como requisito para obtenção do grau de Mestre.

Orientador: Prof. Dr. Fabricio Bertini Pasquot Polido

Belo Horizonte
2024

Lucas Martins Gama

O TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES: uma Análise do Consentimento Parental na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Texto apresentado ao Programa de Pós-Graduação em Inovação Tecnológica da Universidade Federal de Minas Gerais como requisito para obtenção do grau de Mestre.

APROVADO EM:

COMISSÃO JULGADORA

_____

Prof. Dr. Fabricio Bertini Pasquot Polido
Universidade Federal de Minas Gerais (UFMG)

_____

Prof. Dra. Juliana Corrêa Crepaldi Medeiros
Universidade Federal de Minas Gerais (UFMG)

_____

Prof. Dr. Felipe Costa Camarão
Universidade Federal do Maranhão (UFMA)

RESUMO

O presente trabalho aborda a ineficácia da Lei Geral de Proteção de Dados brasileira, com um recorte específico para dados pessoais de crianças e adolescentes, decorrentes da incorporação de um texto estrangeiro sem a correspondente adaptação para a realidade brasileira. Ao não considerar as especifidades do país, à exemplo da taxa de analfabetismo digital e a ausência de um debate conjunto com a população acerca da relevância do tema e da lei, cria-se um cenário de insegurança jurídica que decorre da clara ineficácia do texto que corresponde à proteção de dados de crianças e adolescentes. Assim, o presente estudo visa, entre outros objetivos, a abordagem por meio do direito comparado da Lei Geral de Proteção de Dados (LGPD) com a *General Data Protection Regulation* (GDPR), compreendendo o fenômeno de incorporação do texto legislativo, as consequências práticas e apresentar possíveis soluções para auxiliar na efetividade do texto na prática. A pesquisa sustenta-se na análise bibliográfica de textos sobre o tema e revisão legislativa, utilizando-se da metodologia de direito comparado e hermenêutica jurídica para compreensão do tema, bem como utilização de dados oficiais para fundamentar a pesquisa. Foi possível constatar, através das metodologias utilizadas, a real insegurança jurídica decorrente da incorporação do texto da LGPD, aliado à própria falta de independência do órgão de controle, que seria o responsável por assegurar a eficácia da lei.

Palavras-chave: Lei Geral de Proteção de Dados; Crianças e Adolescentes; Consentimento Parental;

ABSTRACT

This paper addresses the ineffectiveness of the Brazilian General Data Protection Act, with a specific focus on personal data of children and adolescents, resulting from the incorporation of a foreign text without the corresponding adaptation to the Brazilian reality. By not considering the specificities of the country, such as the rate of digital illiteracy and the absence of a joint debate with the population about the relevance of the topic and the act, a scenario of legal uncertainty is created resulting from the clear ineffectiveness of the text that corresponds to the protection of data of children and adolescents. Thus, this study aims, among other objectives, to approach through comparative law the brazilian General Data Protection Act (LGPD) with the General Data Protection Regulation (GDPR), understanding the phenomenon of incorporation of the legislative text, the practical consequences and presenting possible solutions to assist the effectiveness of the text in practice. The research is based on bibliographical analysis of texts on the topic and legislative review, using the methodology of comparative law and legal hermeneutics to understand the topic, as well as the use of official data to support the research. It was possible to verify, through the methodologies used, the real legal uncertainty resulting from the incorporation of the LGPD text, combined with the lack of independence of the control body, which would be responsible for ensuring the effectiveness of the act.

Keywords: General Data Protection Act; Children and Adolescents; Parental Consent;

SUMÁRIO

1 INTRODUÇÃO

Estudos indicam que, atualmente, quem possui dados, possui poder, tendo em vista que esses dados, se utilizados com expertise, podem aumentar o potencial econômico de uma empresa, por exemplo, mediante o direcionamento de propagandas específicas, e até mesmo influenciar no resultado de eleições, porquanto inúmeros estudos apontam que dados pessoais seriam o "novo petróleo".

Nesse contexto, tornam-se cada vez mais comuns modelos de negócios baseados em uma nova moeda de troca: a de dados pessoais. Empresas fornecem testes gratuitos ou até mesmo produtos grátis, com o objetivo de recolher dados pessoais e repassá-los a terceiros.

Tais dados, quando analisados em conjunto e cruzados por algoritmos são capazes de traçar perfis que auxiliam grandes empresas no direcionamento de anúncios, propagandas e serviços de modo a influenciar diretamente na vida dos usuários, alterando a forma como eles vivem.

Tal realidade já é perceptível no universo das redes sociais, quando você se depara, por exemplo, com um anúncio que lhe interessa, levando-o a crer que está sendo espionado por seu próprio celular. O direcionamento de anúncios com base no seu perfil é possível através do *profilling*, ou seja, a criação de um perfil com base no conjundo de seus dados, como pesquisas feitas em seu celular, sua idade e interesses, na maioria dos casos obtidos de maneira irregular.

O escândalo divulgado na manchete publicada pelo *The Guardians*, importante jornal britânico, em dezembro de 2015 trouxe os holofotes para a utilização de dados de redes sociais na política. O escândalo internacional, que envolveu a rede social *Facebook* e a *Cambridge Analytica*, esta última, empresa privada conhecida pela mineração e análise de dados visando comunicação estratégica para o processo eleitoral, trouxe um importante debate acerca da segurança dos dados de usuários disponíveis em redes sociais.

Após o episódio, alguns ex-funcionários relataram que a empresa britânica utilizava indevidamente, e sem o consentimento dos usuários, dados fornecidos pelo *Facebook*, para manipulação da corrida eleitoral em diversos países, indicando, inclusive, que a eleição do então presidente americano, Donald Trump, teria sido facilitada graças à utilização indevida desses dados.

Nesse contexto, narra o documentário "Privacidade Hackeada" (*The Great Hack*), dirigido e produzido por Karim Amer e disponível na *Netflix,* por meio do depoimento de ex-funcionários da *Cambridge Analytica,* que a empresa cruzava dados para compreender e traçar

o perfil eleitoral de cada usuário e, em posse desses dados, direcionar anúncios e ações mais efetivas em regiões críticas, influenciando diretamente o resultado das eleições.

Embora tal relato tenha ganhado notoriedade pelo tamanho da violação e o volume de dados envolvidos, a utilização indevida de dados pessoais não se restringe a grandes empresas e disputas eleitorais, sendo uma realidade próxima, que despertou a atenção internacional para a necessidade de regulamentação do tratamento desses dados pessoais, visando trazer maior segurança jurídica e equilíbrio para essa relação.

Nesse contexto, cada vez mais preocupados com a segurança da coleta e o do tratamento desses dados pessoais, os Estados, movidos por essa necessidade, passaram a editar normas para regulamentar toda a cadeia que envolve a coleta e o tratamento de dados pessoais, com o objetivo de trazer maior segurança ao usuário – ou, ao menos, tentar.

Embora já existissem legislações que tratassem do uso da internet na maior parte dos Estados, buscando regulamentar seu ambiente, não havia uma norma de referência com foco na coleta e tratamento de dados pessoais.

Nesse cenário surge a *General Data Protection Regulation – GDPR*, a legislação vigente em todo o território europeu para suprir essa lacuna e tentar conter o fenômeno causado pelo *Big Data*, limitando a utilização de dados pelas empresas.

Tal legislação inspirou a edição de uma norma específica com o objetivo de regulamentar e controlar o uso de dados pessoais no território brasileiro, a Lei nº 13.709/2018, popularmente conhecida como Lei Geral de Proteção de Dados, ou, simplesmente LGPD. Inspirada na GDPR, a LGPD surgiu na tentativa de trazer maior segurança ao tratamento de dados no território brasileiro.

No Brasil, segundo levantamento realizado pelo Instituto Brasileiro de Defesa do Consumidor (IBDEC), as queixas relacionadas ao uso indevido de dados pessoas cresceram 1.134% de 2015 a 2017. Segundo o *ranking*, a principal reclamação era referente à coleta, consulta ou publicação de dados pessoais sem o consentimento ou autorização do consumidor.

Com a sua vigência as empresas são obrigadas adaptar seus Termos e Políticas de Privacidade, adequando-se ao texto legal da LGPD, devendo seguir, entre outras regras, a do consentimento para a coleta de dados.

Tal requisito foi incorporado com o objetivo de coibir a prática abusiva da utilização indevida de dados pessoais, implicando na observância obrigatória da aceitação do usuário, que deve ser expressa e inequívoca, no momento do fornecimento de dados, trazendo assim, ao menos em teoria, maior segurança ao tratamento de dados pessoais.

Uma preocupação ainda maior da lei brasileira foi com o tratamento de dados pessoais de crianças e adolescentes, considerando sua incapacidade e vulnerabilidade frente às grandes empresas e redes sociais, que em sua grande maioria recolhem dados pessoais de menores sem observância dos requisitos da lei.

Em meio a tantos conceitos e princípios presentes na lei brasileira, este trabalho preocupou-se em tratar acerca do consentimento parental, que reforça a necessidade de aceitação expressa e inequívoca dos pais e/ou responsáveis no momento da coleta, ressaltando a preocupação do legislador com a hipossuficiência do menor, colocando essa barreira para impedir o recolhimento de dados pessoais de crianças sem o seu consentimento (uma vez que essas, por serem incapazes, não podem dar tal consentimento).

Contudo, ao transferir essa responsabilidade para os pais, bastante inspirada na lei europeia, a lei brasileira incorporou algumas das diretrizes referentes ao tratamento de dados pessoais de crianças e adolescentes que não são adqueadas à realidade do país.

Isso porque, conforme será demonstrado durante o texto, a lei brasileira incorporou esses termos e restrições sem um debate profundo e sem a participação e conscientização da população acerca da matéria, deixando de considerar, por exemplo, a taxa de letramento digital da população brasileira.

Um outro exemplo claro refere-se ao texto que trata da fiscalização acerca da validade do consentimento parental, indicando que as empresas seriam responsáveis por adotar meios tecnológicos suficientes para comprovar o consentimento parental dos pais quanto ao tratamento de dados pessoas de crianças.

Apesar da eficiência ser uma característica intrínseca de toda e qualquer legislação, ao analisar o texto da Lei Geral de Proteção de Dados, foi possível perceber inúmeras barreiras e aberturas legais que, para além de autorizar a utilização indevida de dados pessoais de crianças e adolescentes, não coadunam com a realidade brasileira, tendo em vista o analfabetismo digital e a falta de letramento digital, bem como o baixo índice de consciência da população sobre a importância do tema.

Além disso, o órgão que seria responsável por fiscalizar e auxiliar no cumprimento da legislação possui uma configuração que impede a sua independência plena, uma vez que é subordinado à Presidência, dificultando ainda mais a aplicação da lei e, principalmente, das sanções.

Sendo assim, mediante análise bibliográfica, o presente trabalho tem por objetivo analisar o instituto do consentimento parental, previsto na Lei Geral de Proteção de Dados,

fazendo, sempre que possível, um comparativo com o texto da *General Data Protection Regulation*, lei que a inspirou, por meio de uma abordagem jurídico-comparada.

Assim, o presente trabalho pretende contribuir com a lacuna teórica verificada ao decorrer do texto, a importância e a sensibilidade do tratamento de dados pessoais de crianças e adolescentes no território brasileiro, frente os inúmeros desafios decorrentes da realidade do país.

Tendo em vista a inexistência de estudos com esse recorte, com foco específico em dados pessoais de crianças e adolescentes e mediante uma abordagem comparada da legislação brasileira e europeia, demonstrando para além da relevância do presente estudo, a clara insegurança jurídica decorrente da não efetividade da lei geral de proteção de dados quanto aos menores.

Para isso, incialmente, este trabalho traz um recorte histórico das legislações anteriores que versam sobre dados, ainda que de maneira primitiva, para, posteriormente, tratar acerca dos principais conceitos e princípios presentes na LGPD e, por fim, analisar o consentimento parental e todos os seus elementos com base na lei europeia e os entraves para o seu efetivo cumprimento no território brasileiro.

2 METODOLOGIA

A metodologia utilizada no presente estudo concentra-se majoritariamente em revisão bibliográfica, realizada por meio da pesquisa de estudos que abordam sobre a proteção de dados pessoais, buscando sempre que possível a interpretação para o contexto de crianças e adolescentes.

Quanto às técnicas de pesquisa, o trabalho foi realizado com a consulta a dados primários levantados por pesquisas nacionais, com vistas a embasar as teorias aqui defendidas, mediante solicitação juntos aos principais sites de consulta e consulta a pesquisas divulgadas no âmbito nacional e internacional, retirados de fontes oficiais.

Além disso, a pesquisa foi baseada na análise documental, produção legislativa e jurisprudencial sobre o objeto. Ademais, possuiu como alicerce produções doutrinárias de autores consagrados na área, por meio da hermenêutica jurídica., seja pela leitura e interpretação dos documentos citados.

O presente estudo se deu também pela técnica do direito comparado, realizando um comparativo entre as legislações brasileiras e estrangeiras, sempre que possível fazendo um recorte considerando a especialidade decorrente do tratamento de dados pessoais de crianças e adolescentes.

3 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: A CONSQUISTA DO *STATUS* DE DIREITO FUNDAMENTAL E ABORDAGENS COMPARADAS

Antes de proceder ao aprofundamento do objeto deste trabalho, qual seja, os dados pessoais de crianças e adolescentes e a sua interpretação sob a ótica das legislações de proteção de dados brasileira, americana e europeia, o presente estudo realizará um breve recorte acerca do direito à privacidade e sua evolução até a discussão a respeito da proteção de dados pessoais, assim como abordará sua busca pelo *status* de direito fundamental.

Apesar de não possuir um marco temporal específico, é possível identificar a origem do direito à privacidade, que é remontada aos primeiros casos que utilizaram-se do termo *"right to be alone".*

3.1 "*Right to privacy*" e os primeiros casos nos Tribunais dos Estados Unidos

A ideia do direito (interesse) de ser deixado só, o *"right to be alone"*, tem sua primeira manifestação no caso Wheaton *v.* Peters, decidido pela Suprema Corte dos Estados Unidos em 1834. É difícil acreditar que essa manifestação tenha surgido tão cedo; contudo, importante destacar que o conceito de privacidade somente foi abordado e difundido com a publicação do artigo de Samuel D. Warren e Louis D. Brandeis.

A relevância da proteção de dados surge em decorrência da evolução do conceito de privacidade, que está intimamente ligado à proteção de dados pessoais. No artigo destacado anteriormente, intitulado *"The Right to Privacy"*, apresentado à Universidade de Harvard em 1890, os autores Samuel Warren e Louis Brandeis defendiam que os veículos de comunicação em massa da época, principalmente jornais, estavam invadindo a privacidade das pessoas.

Nesse contexto, surgem os primeiros escritos acerca do *"right to be alone",* que pode ser traduzido livremente como o direito de ser deixado só, como uma forma de combater a invasão à privacidade denunciada por Warren e Brandeis. Apesar de ser incomum para o sistema da *common law* que um artigo científico apresentado a uma universidade seja decisivo para o início de um debate doutrinário sobre o tema, essa foi a realidade.

A discussão, logo em seguida, saiu do campo doutrinário e finalmente chegou aos Tribunais. Estudiosos apontam os casos Schuyler *v.* Curtis (1891) e Marks *v.* Jaffa (1893) como os que teriam iniciado a discussão a respeito do *"right of privacy",* que pode ser traduzido como direito à privacidade, nos Tribunais americanos.

Além disso, a doutrina cita dois casos emblemáticos e igualmente fundamentais, apesar

de posteriores, na discussão do direito à privacidade. O primeiro, conhecido como "*Flour of the Family*" (Roberson *v.* Rochester Folding Box Co.), diz respeito à inserção da fotografia de uma moça em um cartaz publicitário divulgado por um fabricante de farinha. Apesar da ação ter sido rejeitada em 1902 pela Corte de Apelação de Nova Iorque, o direito à privacidade havia sido reconhecido pelos tribunais inferiores.

Vejamos trecho da decisão do caso Roberson *v.* Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902):

> The history of the phrase 'right of privacy' in this country seems to have begun in 1890 in a clever article in the Harvard Law Review — already referred to — in which a number of English cases were analyzed, and, reasoning by analogy, the conclusion was reached that — not withstanding the unanimity of the courts in resting their decisions upon property rights in cases where publication is prevented by injunction — in reality such prevention was due to the necessity of affording protection to thoughts and sentiments expressed through the medium of writing, printing and the arts, which is like the right not to be assaulted or beaten; in other words, that the principle, actually involved though not always appreciated, was that of an inviolate personality, not that of private property[1].

No julgamento do referido caso, a autoridade reconhece em seu voto a importância da decisão para a discussão do problema. Além disso, cita por diversas vezes que não é pela não existência de uma lei formal tratando sobre o tema que o direito não exista.

Isso porque a sociedade, que encontra-se em constante evolução, vai apresentando inúmeras situações jamais vistas no mundo jurídico. A partir desse ponto, é importante que se inicie o debate em algum momento, na intenção de ver garantido um direito que, apesar de não ser previsto formalmente em uma lei ordinária, pode existir pela interpretação de um princípio ou através da própria constituição.

Estamos falando de uma sociedade de cem anos atrás, na qual ainda não era possível precisar os impactos da internet e das tecnologias subsequentes na sociedade e no cotidiano. Esse debate, apesar de parecer irrelevante sob a ótica atual, representou um importante passo no reconhecimento ao direito à privacidade. Destaca-se o trecho seguinte da decisão:

> The so-called right of privacy is, as the phrase suggests, founded upon the claim that

[1] Portanto, em um caso como o que está diante de nós, que é reconhecidamente novo para este tribunal, é importante que o tribunal tenha em mente o efeito sobre o litígio futuro e sobre o desenvolvimento da lei que necessariamente resultaria de um passo tão longe fora dos caminhos batidos do direito comum e da equidade, assumindo – o que tentarei mostrar em um momento – que o direito à privacidade como uma doutrina legal exequível em equidade não foi, até agora, estabelecido por decisões. A história da frase "direito à privacidade" neste país parece ter começado em 1890 em um artigo inteligente na Harvard Law Review — já referido — no qual vários casos ingleses foram analisados e, raciocinando por analogia, chegou-se à conclusão de que — não obstante a unanimidade dos tribunais em basear suas decisões sobre os direitos de propriedade nos casos em que a publicação é impedida por liminar — na realidade tal prevenção se deveu à necessidade de oferecer proteção aos pensamentos e sentimentos expressos através da escrita, impressão e das artes, que é como o direito de não ser agredido ou espancado; em outras palavras, que o princípio, realmente envolvido, embora nem sempre apreciado, era o de uma personalidade inviolada, não o da propriedade privada.

> a man has the right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written up for the benefit of others, or his eccentricities commented upon either in handbills, circulars, catalogues, periodicals or newspapers, and, necessarily, that the things which may not be written and published of him must not be spoken of him by his neighbors, whether the comment be favorable or otherwise. While most persons would much prefer to have a good likeness of themselves appear in a responsible periodical or leading newspaper rather than upon an advertising card or sheet, the doctrine which the courts are asked to create for this case would apply as well to the one publication as to the other, for the principle which a court of equity is asked to assert in support of a recovery in this action is that the right of privacy exists and is enforceable in equity, and that the publication of that which purports to be a portrait of another person, even if obtained upon the street by an impertinent individual with a camera, will be restrained in equity on the ground that an individual has the right to prevent his features from becoming known to those outside of his circle of friends and acquaintances[2].

O enfrentamento da matéria pelo tribunal, assim, fez reconhecer, ao menos a nível jurisprudencial, uma citação ao direito à privacidade, representando importante avanço no debate que, hoje, reflete na previsão de um direito constitucional à privacidade que está presente na maioria dos textos constitucionais dos Estados.

O segundo caso emblemático, que tem como partes Pavesich *v.* New England Life Ins. Co., de 1905 Ga. 190 (Ga. 1905), foi julgado pela Suprema Corte da Georgia. Em resumo, foi levada à Corte a discussão acerca da reprodução não autorizada em um jornal do retrato do autor, Pavesich. No julgamento do caso, a corte rejeitou os argumentos levados anteriormente ao caso Roberson, pelo que acabou aceitando o entendimento de Warren e Brandeis:

> 1. The absence, for a long period of time, of a precedent for an asserted right is not conclusive evidence that the right does not exist. Where the case is new in principle, the courts can not give a remedy; but where the case is new only in instance, it is the duty of the courts to give relief by the application of recognized principles. 2. A right of privacy is derived from natural law, recognized by municipal law, and its existence can be inferred from expressions used by commentators and writers on the law as well as by judges in decided cases. (…) 7. The constitution declares that the liberty of speech and of the press must not be abused; and the law will not permit the right of privacy to be asserted in such a way as to curtail or restrain such liberties. The one may be used to keep the other within lawful bounds, but neither can be lawfully used to destroy the other. (…) 11. The publication of a picture of a person, without his consent, as a part of an advertisement, for the purpose of exploiting the publisher's

[2] O chamado direito à privacidade é, como a frase sugere, baseado na alegação de que um homem tem o direito de passar por este mundo, se ele quiser, sem ter sua foto publicada, suas empresas discutidas, seus experimentos bem-sucedidos escritos para o benefício dos outros, ou suas excentricidades comentadas em panfletos, circulares, catálogos, periódicos ou jornais, e, necessariamente, que as coisas que não podem ser escritas e publicadas sobre ele não devem ser faladas por seus vizinhos, seja o comentário favorável ou não. Embora a maioria das pessoas prefira muito que uma boa imagem de si mesmas apareça em um periódico responsável ou jornal líder, em vez de em um cartão ou folha de publicidade, a doutrina que os tribunais são solicitados a criar para este caso se aplicaria tanto a uma publicação quanto à outra, pois o princípio que um tribunal de equidade é solicitado a afirmar em apoio a uma recuperação nesta ação é que o direito à privacidade existe e é exequível em equidade, e que a publicação daquilo que pretende ser um retrato de outra pessoa, mesmo que obtido na rua por um indivíduo impertinente com uma câmera, será contido em equidade com o fundamento de que um indivíduo tem o direito de impedir que suas características se tornem conhecidas por aqueles fora de seu círculo de amigos e conhecidos.

> business, is a violation of the right of privacy of the person whose picture is reproduced and entitles him to recover without proof of special damage[3].

Ato seguinte, na decisão, o Tribunal reconhece, mais uma vez, que a inexistência de um direito formal, previsto em lei, não impede o seu reconhecimento pelos tribunais:

> We think that what should have been a proper judgment in the Roberson case was that contended for by Judge Gray in his dissenting opinion, from which we quote as follows: 'The right of privacy, or the right of the individual to be let alone, is a personal right, which is not without judicial recognition. It is the complement of the right to the immunity of one's person. The individual has always been entitled to be protected in the exclusive use and enjoyment of that which is his own. The common law regarded his person and property as inviolate, and he has the absolute right to be let alone' Cooley, Torts, p. 29. The principle is fundamental, and essential in organized society, that everyone, in exercising a personal right and in the use of his property, shall respect the rights and properties of others. He must so conduct himself, in the enjoyment of the rights and privileges which belong to him as a member of society, as that he shall prejudice no one in the possession and enjoyment of those which are exclusively his. When, as here, there is an alleged invasion of some personal right, or privilege, the absence of exact precedent and the fact that early commentators upon the common law have no discussion upon the subject are of no material importance in awarding equitable relief. That the exercise of the preventive power of a court of equity is demanded in a novel case is not a fatal objection. As I have suggested, that the exercise of this peculiar preventive power of a court of equity is not found in some precisely analogous case furnishes no valid objection at all to the assumption of jurisdiction, if the particular circumstances of the case show the performance, or the threatened performance, of an act by a defendant, which is wrongful, because constituting an invasion, in some novel form, of a right to something which is, or should be conceded to be, the plaintiff's, and as to which the law provides no adequate remedy[4].

---

[3] 1. A ausência, por um longo período de tempo, de um precedente para um direito afirmado não é uma evidência conclusiva de que o direito não existe. Quando o caso é novo em princípio, os tribunais não podem dar um remédio; mas quando o caso é novo apenas no caso, é dever dos tribunais dar alívio pela aplicação de princípios reconhecidos. 2. Um direito à privacidade é derivado da lei natural, reconhecida pela lei municipal, e sua existência pode ser inferida a partir de expressões usadas por comentaristas e escritores sobre a lei, bem como por juízes em casos decididos. (…) 7. A constituição declara que a liberdade de expressão e de imprensa não deve ser abusada; e a lei não permitirá que o direito à privacidade seja afirmado de forma a restringir ou restringir tais liberdades. Um pode ser usado para manter o outro dentro dos limites legais, mas nenhum deles pode ser usado legalmente para destruir o outro. (…) 11. A publicação de uma foto de uma pessoa, sem o seu consentimento, como parte de um anúncio, com a finalidade de explorar os negócios do editor, é uma violação do direito de privacidade da pessoa cuja imagem é reproduzida e lhe dá o direito de se recuperar sem prova de danos especiais.

[4] Achamos que o que deveria ter sido um julgamento adequado no caso Roberson foi o defendido pelo juiz Gray em sua opinião dissidente, da qual citamos da seguinte forma: 'O direito à privacidade, ou o direito do indivíduo de ser deixar em paz, é um direito pessoal, que não é sem reconhecimento judicial. É o complemento do direito à imunidade da pessoa. A individualidade sempre foi o direito de ser protegido no uso exclusivo e gozo do que é seu. A lei comum considerava sua pessoa e propriedade como invioláveis, e ele tem odireito absoluto de ser deixado em paz' Cooley, Torts, p. 29. O princípio é fundamental e essencial na sociedade organizada, de que cada um, no exercício de um direito pessoal e no uso de sua propriedade, deve respeitar os direitos e propriedades dos outros. Ele deve se comportar assim, no gozo dos direitos e privilégios que lhe pertencem como membro da sociedade, de modo que não prejudique ninguém na posse e no gozo daqueles que são exclusivamente seus. Quando, como aqui, há uma suposta invasão de algum direito pessoal, ou privilégio, a ausência de precedente exato e o fato de que os primeiros comentaristas sobre o direito comum não têm discussão sobre o assunto não são de importância material na concessão de alívio equitativo. Que o exercício do poder preventivo de um tribunal de equidade seja exigido em um novo caso não é uma objeção fatal. Como sugeri, que o exercício desse poder preventivo peculiar de um tribunal de equidade não seja encontrado em algum caso precisamente análogo, não fornece nenhuma objeção válida à assunção de jurisdição, se as circunstâncias particulares do caso

Desse modo, os julgamentos apresentados convergem no sentido de que consideraram que a publicação da imagem de uma pessoa, sem seu consentimento e com o propósito de exploração comercial, configuraria uma violação do *"right of privacy"*, o que não demandaria da pessoa retratada prova especial do dano.

Além disso, afirmam que a inexistência de uma lei prevendo esse direito não implica necessariamente na sua invalidade no mundo jurídico. Isso porque, no modelo de jurisdição americana, as Cortes possuem a função de enfrentar debates de matérias ainda não tratadas em lei, possuindo papel fundamental na suplementação de lei e na formulação de princípios que guiam a sociedade e moldam as legislações futuras.

Ao rechaçar diferenciação entre conhecer, interpretar e aplicar Dworkin (1999) entende que os princípios são *standards* que devem ser observados por refletirem uma exigência de justiça ou alguma outra dimensão de moralidade, o que os distingue das normas.

Dworkin (1999) destaca, ainda, a diferença qualitativa entre regras e princípios, indicando que ambos são tratados como conjunto de padrões que apontam para decisões, tendo distinções quanto à natureza de orientação. De acordo com o autor, as regras são aplicáveis em formato "tudo ou nada", ou seja, quando se argumenta com base em uma regra, ela é ou não é. Já num argumento de princípio, é necessário se mostrar como sua aplicação mantém uma coerência com o contexto global dos princípios (dimensão de peso).

Assim, a aplicação de um princípio não pode significar a exclusão de outros. Dworkin (1999) entende que o Direito sempre proporciona uma boa resposta, tendo em vista que o juiz ao julgar escreve a continuidade de uma história e, para exemplificar essa similaridade do Direito com a narrativa, utiliza a metáfora do "Romance em Cadeia". Nessa metáfora, elaborada por Dworkin (1999), cada juiz deve se considerar parte de um complexo empreendimento em cadeia, ao lançar-se à criação e à interpretação jurisprudenciais.

O autor concebe a interpretação jurídica como a extensão de uma história institucional do Direito, que se desenvolve a partir de decisões, estruturas, convenções e práticas. Assim, conforme Streck (2006), sustenta que os princípios têm a finalidade de impedir "múltiplas respostas", ou seja, "fecham" a interpretação[5].

O desenrolar da noção de privacidade aconteceu paralelo ao surgimento da própria

---

mostrarem o desempenho, ou o desempenho ameaçado, de um ato por um réu, que é ilícito, porque constitui uma invasão, de alguma forma nova, de um direito a algo que é, ou deve ser concedido, do autor, e quanto ao qual a lei não fornece remédio adequado.

[5] Conforme o autor, antes de estarem cindidos, há um acontecer que aproxima regra e princípio em duas dimensões, a partir de uma anterioridade, isto é, a condição de possibilidade da interpretação da regra é a existência do princípio instituidor (STRECK, 2006, p. 167).

possibilidade material de assegurar esse direito. O nascimento do direito à privacidade, conforme leciona Rodotà (2008), pode ser historicamente relacionado à desagregação da sociedade feudal, em que o isolamento era privilégio de eleitos ou de outras pessoas as quais, por necessidade ou opção, viviam distantes da comunidade.

Ocorre que as inúmeras evoluções tecnológicas, assim como a própria popularização da internet, acarretaram um debate que colocou a privacidade, como se tem hoje, em um patamar de direito constitucional.

A evolução da sociedade, que passou da indústria para a informação – sendo essa uma importante moeda de troca atualmente – levou esse debate a tal nível que hoje é impossível não imaginar a proteção desse direito com *status* constitucional. Conforme será plenamente dissertado a seguir, à medida que a sociedade avança, a legislação deve avançar em conjunto, sob pena de não cumprir com seu papel social, qual seja, o de regulamentar a sociedade e garantir a preservação de direitos.

3.2 Sociedade Informacional x Privacidade

A sociedade passou, ao longo do tempo, por significativas mudanças e evoluções constantes que alteraram a forma como as pessoas viviam de maneira significativa, sempre existindo um elemento central apto a caracterizar cada era, geralmente centrado no modelo econômico experimentado.

A sociedade agrícola, assim, estruturou-se, desde os primórdios, tendo a agricultura como seu elemento principal. Cidadãos utilizavam a terra como sua principal fonte de renda e era o produto agrícola que movimentava a economia.

A sociedade industrial veio logo em seguida. Com o surgimento da eletricidade e a evolução de pesquisas e experimentos, aparecem as primeiras máquinas a vapor, que passam a desempenhar papel central na produção em larga escala de indústrias, gerando empregos e, na mesma proporção, desigualdades.

Pouco a pouco, as máquinas foram incorporadas ao mercado, por vezes substituindo a mão-de-obra braçal, em um fenômeno gradativo conhecido como a Revolução Industrial, que teve seu início na Europa.

Nesse momento, dentre as inovações da época, merece destaque a comunicação via internet, que surgiu em meados da década de 1960, durante a Guerra Fria, em um momento de disputa tecnológica entre União Soviética e Estados Unidos. O projeto foi desenvolvido nos Estados Unidos, com financiamento da *National Aeronautics and Space Administration*

(NASA) e do Pentágono, com o objetivo principal de armazenar dados importantes e protegê-los de um possível ataque nuclear dos seus inimigos.

Nessa época, começaram a rodar os primeiros sistemas que viabilizavam o armazenamento de dados e troca de informações, lançando-se um modelo inicial de banco de dados, classificando esse grande volume de dados como *Big Data.*

A partir disso, após a Segunda Guerra Mundial, a sociedade passa a viver um momento pós-industrial, marcado por intensas desigualdades e com a substituição gradativa do mercado de produtos pelo mercado de serviços, como por exemplo o serviço bancário, médico e de consultoria.

Somente em 1990, quando o cientista, físico e professor britânico Tim Berners-Lee desenvolveu um navegador, no formato *World Wide Web* (www), inaugurou-se a Rede Mundial de Computadores.

Desse modo, a década de 1990 ficou conhecida como o "*boom* da internet", tendo em vista a popularização de computadores, da internet e o surgimento de novos navegadores que conectavam as pessoas em qualquer lugar do mundo.

O crescimento foi exponencial, sendo que, em pouquíssimo tempo, grande parte da população já possuía acesso, de alguma forma, a esse tipo de conexão, marcando a história com a popularização da internet e dos computadores.

Desse modo, após transitar por todos esses modelos de sociedade, graças à evolução tecnológica, é possível afirmar que o elemento central hoje é a informação e, a partir dessa realidade, surge a nomenclatura "sociedade da informação", termo recente e adotado por diversos estudiosos da área para caracterizar essa nova era.

A informação passa, então, a ocupar um lugar relevante e central perante a sociedade, em que os computadores, celulares e a internet passam a desempenhar um papel quase que essencial para todos, impactando diretamente a forma como se vive.

Assim, é inegável que o desenvolvimento das tecnologias nos campos da informação e da comunicação e a popularização de aparelhos que permitem o acesso à internet, produziu reflexos sobre os conceitos de tempo e espaço, provocando uma série de alterações nas formas de relacionamento interpessoais, seja na esfera pública ou privada.

A sociedade informacional, termo preconizado por Manuel Castells, sociólogo espanhol

> [...] consiste em uma terminologia que tenta estabelecer um paralelo entre indústria e industrial. Uma sociedade industrial (conceito comum na tradição sociológica) não é apenas uma sociedade em que há indústrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas de atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana

(CASTELLS, 1999, p. 46).

Assim, o emprego dos termos “sociedade informacional” e “economia informacional” busca uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para as sociedades. Porém, o conteúdo real de “sociedade informacional” tem que ser determinado pela observação e pela análise (CASTELLS, 2008, p. 65).

No mesmo propósito, a revolução tecnológica provoca uma mudança visceral no mundo de hoje; no caso de sua manifestação mais inquietante, a internet, inova nos parâmetros de sua própria análise, na dimensão formal do seu objeto, isto é, a virtualidade (PIMENTA, 2013).

De acordo com Pimenta (2013, p. 1):

> As novas tecnologias, ou tecnologias digitais, expandiram enormemente a possibilidade de acesso à informação e às formas de comunicação, daí porque migraram de tecnologias de informática para serem denominadas Novas Tecnologias da Informação e Comunicação (NTICs). O desenvolvimento do que são comumente denominadas na literatura como novas tecnologias da informação e da comunicação foi propulsor de mudanças que afetaram a sociedade mundial em todos os seus aspectos.

Nesse contexto, Rodotà (2008, p. 95), ao comentar acerca da popularização das tecnologias, afirma que:

> A ampliação da esfera de proteção privada em face dos meios de comunicação de grande divulgação é o grande debate jurídico sobre quais são os limites de proteção e de exercício do direito à privacidade. O indivíduo pretende controle exclusivo. As tecnologias da informação são importantes para o desenvolvimento social, porém, em algumas situações, expõem e ameaçam a tranquilidade daquele que não quer ver a sua imagem repercutir perante a sociedade, principalmente quando envolver fatos negativos que possam levar a processos discriminatórios.

Assim, apenas a previsão de um direito constitucional à privacidade não era mais suficiente para assegurar a eficácia dos dispositivos, sendo necessária uma tutela ainda mais específica sobre o tema, momento em que se iniciam os debates acerca de legislações para regular a utilização da internet no âmbito internacional.

Para tanto, Rodotà (2008) complementa o exposto indicando, ainda, que se faz necessária a migração para uma sociedade do controle, em que seja permitido aos usuários exercer um poder de controle acerca das informações coletadas, traçando assim um caminho para a proteção de dados pessoais.

> E não se pode dizer que tal comportamento esteja em contradição com a tendência, anteriormente referida, segundo a qual existem categorias inteiras de informações pessoais (como aquelas de conteúdo econômico) cuja divulgação é oportuna ou necessária: publicidade e controle não são termos contraditórios, como são publicidade e sigilo. Exatamente onde se admitir a máxima circulação de informações de conteúdo econômico, deve-se permitir aos interessados exercitar um real poder de

> controle sobre a exatidão de tais informações, sobre os sujeitos que as operam e sobre as modalidades de sua utilização (RODOTÀ, 2008, p. 46).

É nesse contexto acalorado de discussão acerca da necessidade de controle e regulação de dados pessoais no âmbito mundial que, em meados de 2010, surgem os primeiros arranjos normativos voltados à essa temática, em que se pode destacar dois modelos principais: o americano e o europeu, que serão brevemente tratados a seguir.

3.3 Regulação de dados pessoais na Europa

Assim como outros Estados, a União Europeia já previa alguns dispositivos legais que tratavam acerca da proteção de dados pessoais, à exemplo o artigo 8º da Carta de Direitos Fundamentais da União Europeia (2006)[6], que prevê a proteção de dados pessoais como um direito universal, que devem ser tratados com fins específicos e com o consentimento do usuário[7].

No mesmo texto, no item 3, a referida legislação estabelece a fiscalização por parte de uma autoridade competente. Essa competência foi atribuída à *European Data Protection Supervisor – EDPS* (Autoridade Europeia para a Proteção de Dados – AEPD), entidade independente com poderes para atuar na fiscalização dos dados.

Seria competência dessa entidade supervisionar todo e qualquer processamento de dados pessoais pela Administração – e aqui reside a principal diferença entre a Agência criada por essa legislação e a *General Data Protection Regulation (GDPR)* – para assegurar o cumprimento da legislação aplicável, bem como conduzir investigações e monitorar as tecnologias que trabalham com dados pessoais.

---

[6] *In verbis:* Artigo 8º. Proteção de dados pessoais: 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito à fiscalização por parte de uma autoridade independente.

[7] A Carta de Direitos Fundamentais da União Europeia, foi promulgada em 2007 com o objetivo de assegurar direitos fundamentais aos cidadãos europeus. Muito embora essa legislação seja anterior à edição da *General Data Protection Regulation* – que trata de maneira específica sobre a proteção de dados – esse trecho demonstra a importância da proteção dos dados pessoais e, sobretudo, da sua regulação. Ademais, assegura o direito à informação, de modo que os usuários possam ter acesso aos seus dados processados e solicitar sua retificação, atribuindo ainda a fiscalização do disposto.

3.4 Regulação da proteção de dados nos Estados Unidos

De outro modo, nos Estados Unidos não havia uma legislação específica para regular o tratamento de dados no território, sendo essa matéria abordada de maneira genérica por leis federais, estaduais e regulamentos, seguindo o modelo de governo americano.

Entre essas legislações, duas merecem destaque: a *Privacy Act* (Lei da Privacidade), que funciona de modo semelhante à Carta de Direitos Fundamentais da União Europeia, estabelecendo diretrizes específicas a serem observadas pelo governo e agências federais para coleta, armazenamento, uso e compartilhamento de dados, colocando como requisito essencial o consentimento por escrito dos usuários, ressalvadas as disposições em contrário; e a ECPA (Lei de Privacidade de Comunicação Eletrônica), que aborda assuntos mais direcionados à comunicação, como a proibição de interceptação de mensagens telefônicas, e limita o acesso a algumas informações tidas como pessoais.

Ao contrário da União Europeia, os Estados Unidos não possuem um órgão específico que com a competência de fiscalizar o cumprimento da legislação vigente e o tratamento de dados no âmbito nacional.

Entretanto, a agência nacional americana conhecida por *Federal Trade Commission* (FTC), muito embora tenha o objetivo de proteger os consumidores da atuação que fere a ampla concorrência, possui legitimidade, também, para investigar as empresas mediante denúncias formuladas pelos usuários, inclusive no que tange ao tratamento de seus dados pessoais, podendo realizar denúncia acerca do uso indevido ou sobre o vazamento desses.

3.5 Regulação dos dados pessoais no Brasil

No Brasil, como era de se esperar, o fenômeno da globalização pegou de surpresa os legisladores, que não estavam preparados para lidar com as demandas decorrentes desse fenômeno. Corroborando esse entendimento, a doutrinadora Ana Cristina de Azevedo, na sua obra “Marco Civil da Internet no Brasil”, assevera que a rede da internet surgiu antes mesmo de uma legislação que viesse a regular tais mecanismos, sendo necessário o preenchimento de lacunas por meio de outras fontes do direito, por meio de analogias.

> A discussão envolvia ‘se’ e ‘como’ o espaço virtual devia ser regulado e, nesse sentido, como a utilização da rede surgiu antes de qualquer previsão legal e rapidamente se expandiu e ocupou lugar de destaque no mundo, a primeira providência para suprir a lacuna jurídica foi lançar mão da analogia, com o uso de velhas regras criadas tendo em vista outras situações, quando possível encontrar alguma semelhança entre as duas realidades, a prevista na lei e a ocorrente na

telemática (AZEVEDO, 2014, p. 91).

A abordagem de cada instrumento que contribuiu para o regulamento atual mostra-se impossível, tendo em vista os inúmeros regulamentos que tratam acerca do tema. Contudo, o presente estudo abordará alguns dos principais instrumentos legislativos que colaboraram para a legislação como se tem atualmente.

3.5.1 Constituição Federal (*Habeas Data*)

Assim, muito embora na época não existisse um diploma legal específico para tratar acerca dos dados e controlar o fenômeno provocado pelo *Big Data,* a Constituição de 1988, em seu Artigo 5º, X, trabalha a inviolabilidade à vida privada, que, em um sentindo amplo, abarca os dados pessoais.[8]

Tal previsão, ainda que de maneira genérica, abarca a proteção de dados, tendo em vista que os dados de natureza pessoal podem ser equiparados ao direito de inviolabilidade da vida privada e afetam diretamente a honra e imagem do usuário

O próprio ordenamento jurídico prevê que, em caso de lacuna legislativa, devem ser utilizadas outras fontes legislativas como forma de suprir esse espaço em branco, como a analogia, os costumes e os princípios gerais de direito. Ademais, como forma de contornar essa inércia legislativa, a hermenêutica jurídica permite ainda uma interpretação extensiva e profunda de alguns dispositivos legais.

Do mesmo modo, Danilo Doneda (2006, p. 323), em sua obra "Da privacidade à proteção de dados pessoais" assevera que deve-se considerar "o problema da informação inicialmente através das garantias à liberdade de expressão e do direito à informação, que devem ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade", deixando claro que, em caso de ausência normativa sobre o tema, deve-se interpretar de maneira extensiva os diversos dispositivos espalhados pela Constituição, com o intuito de preencher tal lacuna.

Ademais, a Constituição brasileira prevê expressamente a figura do *Habeas Data*, também em seu artigo 5º, LXXII, alínea a, como um remédio constitucional que viabiliza o

[8] *In verbis:* Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) X- são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988, não paginado).

acesso às informações presentes em bancos de dados públicos, com o objetivo de promover o acesso, pelo cidadão, aos dados armazenados em bancos de dados governamentais, restando clara a preocupação do legislador desde já em promover esse acesso, ainda que limitando-se à entes públicos.[9]

Emergiu, assim, um debate mundial acerca da necessidade de regulação específica do uso da internet, trazendo diversos modelos regulatórios acerca do tema, à exemplo dos apresentados anteriormente, tratando diretamente acerca do seu uso e das possíveis controvérsias decorrentes da sua popularização, visando trazer maior segurança jurídica para as relações digitais.

3.5.2 Marco Civil da Internet (Lei nº 12.965/14)

De modo semelhante ao modelo europeu, o Brasil publicou a Lei nº 12.965/14, popularmente conhecida como Marco Civil da Internet, visando regular a conectividade e a troca de informações pela internet de maneira democrática e participativa.

Essa lei surgiu com o objetivo de regular as relações jurídicas no âmbito da internet, garantindo direitos civis e sociais, atribuindo direitos e deveres para os usuários da rede mundial de computadores e para os provedores.

Entretanto, muito embora a legislação tenha sido aprovada antes da GDPR, o Marco Civil da Internet não buscou regular especificamente o tratamento de dados, tendo em vista que seu objetivo fundamental, ao contrário da legislação europeia, não é garantir a privacidade e proteção de dados dos usuários de forma ampla, não sendo enquadrada, assim, como uma norma protetiva quanto ao tratamento de dados pessoais.

Assim, entre as maiores economias do mundo, o Brasil restava como um dos poucos países que não possuíam um regulamento específico para regular o tratamento de dados pessoais no seu território, contando tão somente com legislações esparsas e não específicas.

Nesse contexto, com o intuito de complementar o Marco Civil da Internet, adaptando-o à necessidade de regulação do tratamento de dados, promoveu-se a edição do Decreto Legislativo nº 8.771/2016, conhecido como Regulamento do Marco Civil da Internet que, entre outras mudanças, trouxe o conceito de dados pessoais e de tratamento de dados, bem como

---

[9] *In verbis:* Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público. (BRASIL, 1988, não paginado)

trouxe a obrigação às empresas de promover a exclusão dos dados após atingida a finalidade ou encerrado o prazo legal.

3.5.3 Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Seguindo o movimento internacional de edição de legislações que tratassem especificamente da proteção de dados pessoais, muito por influência da própria *General Data Protection Regulation*, surge a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados e apelidada de LGPD, com o objetivo principal de proteger os direitos fundamentais de liberdade e privacidade.

Tal legislação, ao contrário das já existentes no território brasileiro, trouxe princípios e conceitos – que serão melhor trabalhados em capítulo específico – imprescindíveis, como o dado pessoal e dado sensível, bem como instituiu a figura do encarregado, bem próximo ao DPO previsto na GDPR, cuja função essencial é ser responsável por todo o ciclo de tratamento de dados, assim como por garantir a adaptação das empresas às diretrizes previstas na legislação supracitada.

Ademais, a legislação brasileira, assim como se esperava, trouxe como seu núcleo o consentimento, figura que deve estar presente para coleta e tratamento de dados, indicando que este deve ser livre e expresso, ressalvadas as exceções legais, que serão objeto de estudo em capítulo específico.

Importante destacar que as regras previstas na Lei Geral de Proteção de Dados (LGPD) são aplicáveis aos órgãos da administração direta, indireta, bem como às pessoas jurídicas de direito privado.

A LGPD implementou, ainda, a Autoridade Nacional de Proteção de Dados (ANPD) que, entre outros objetivos, tem o dever de zelar, implementar e fiscalizar o cumprimento da legislação em todo seu território, tendo inclusive poder de polícia para aplicação de multas e sanções previstas no texto.

Importante frisar que o trecho que instituía a ANPD foi objeto de veto pelo então Presidente da República, pois, segundo ele, tratava-se de uma competência específica da Presidência instituir órgãos e Agências Reguladoras, tendo sido efetivada por meio da Medida Provisória nº 869, de 27/12/2018, que alterou a lei.

No que tange à proteção de dados pessoais de crianças e adolescentes, tema objeto do presente estudo, a Lei Geral de Proteção de Dados determinou um tratamento específico para os dados que envolvem menores, demonstrando a necessidade de um cuidado redobrado,

tamanha a vulnerabilidade do sujeito de direitos nesse caso.

No capítulo seguinte, o presente estudo abordará de maneira objetiva inicialmente os conceitos referentes ao consentimento, que envolvem o ato de vontade necessário para permitir o tratamento de dados pessoais dos usuários e, ato seguinte, fará uma análise dos requisitos específicos adotados pela legislação visando a proteção de dados de crianças e adolescentes e os princípios e conceitos da legislação brasileira sob a ótica da criança e do adolescente.

4 O CONSENTIMENTO PARENTAL E A PROTEÇÃO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES NA LEI GERAL DE PROTEÇÃO DE DADOS

A partir de um movimento natural e com o avanço das legislações de países desenvolvidos em editar um regramento para regular dados pessoais, os Estados perceberam a necessidade de uma legislação específica para tratar do tratamento de dados pessoais, dentre as quais merece destaque a *General Data Protection Regulation – GDPR*, na Europa, e a Lei Geral de Proteção de Dados – LGPD, no Brasil.

Ambas as legislações possuem suas similitudes e diferenças, e convergem em um ponto comum: ambas trazem o consentimento como seu núcleo. Esse instituto, cumulado com os princípios que serão trabalhados neste capítulo, funciona como elemento norteador do tratamento de dados pessoais no Brasil e na Europa.

É somente mediante o consentimento que o titular pode permitir a coleta e tratamento dos seus dados pessoais. Segundo a LGPD, esse consentimento deve ser livre, específico e informado, sendo que somente em situações específicas e excepcionais o processamento de dados é permitido sem o consentimento do titular.

Danilo Doneda (2006) indica, em sua obra, que o consentimento surge como uma forma de implementar o que o autor defende como “direito à autodeterminação informativa”, que, em síntese, resume-se à participação do usuário na relação, funcionando como uma espécie de mola propulsora.

Do mesmo modo, Laura Mendes (2014, p. 60) considera que, para que o indivíduo seja capaz de exercer esse direito à autodeterminação informativa, faz-se necessário “um instituto jurídico por meio do qual se expresse a sua vontade de autorizar ou não o processamento de dados pessoais: o consentimento”.

Assim, o consentimento surge como uma forma de coibir as atividades abusivas dos controladores, sendo um mecanismo de legitimação para o tratamento de dados pessoais, permitindo que o titular exerça um papel fundamental de controle sobre os seus próprios dados, tendo em vista que somente mediante a sua aprovação expressa é autorizada a utilização de seus dados pessoais.

Essa autorização se restringe à finalidade descrita no momento da coleta, nos moldes do princípio da finalidade, previsto na Lei Geral de Proteção de Dados e também na *General Data Protection Regulation*.

Para facilitar o estudo do consentimento, e considerando que tanto a legislação europeia quanto a brasileira tratam de todo o processo que envolve o tratamento de dados, este capítulo

será direcionado a uma análise objetiva e comparativa, com foco maior no que tange ao consentimento para o tratamento de dados pessoais de crianças e adolescentes.

Para tanto, o presente capítulo se concentrará em comparar os modelos de regulação de proteção de dados, fazendo, sempre que possível, um comparativo entre ambos. Ato seguinte, abordará a natureza jurídica e os pressupostos de validade do consentimento previstos na GDPR e na LGPD, por meio de estudo comparado e, por fim, abordará os princípios e conceitos da lei geral de proteção de dados brasileira sob a ótica da criança e do adolescente.

4.1 Breve comparativo entre os modelos de regulação de proteção de dados no Brasil (LGPD) e na Europa (GDPR)

Quando se estuda a proteção de dados, dois modelos surgem como principais referência: o modelo americano e o modelo europeu. O presente estudo focará no modelo europeu, fazendo um comparativo entre esse e o brasileiro, visto que a legislação brasileira foi inspirada na europeia, mantendo boa parte dos seus artigos.

De um lado, tem-se a GDPR como uma legislação aplicável a todo o território da Europa, podendo enquadrar-se como uma legislação "internacional" acerca do tema, e que serviu de modelo para a edição de diversas outras. Por se tratar de uma legislação aplicável à toda União Europeia, a GDPR possui suas particularidades quanto à aplicação no território e à sua própria natureza jurídica.

A GDPR enquadra-se como uma Diretiva, de modo que, segundo Danilo Doneda (2006), seria uma espécie de fonte secundária no sistema de fontes do direito, com a função primordial de uniformizar a legislação. Assim, com a edição de uma Diretiva, cada país possui um intervalo de tempo para adaptar suas legislações locais ao estabelecido na diretiva, em um processo conhecido como transposição.

No caso de inércia legislativa, a diretiva passa a ser aplicável como forma de suprir a lacuna, e o país pode responder pela inércia perante a Corte Europeia de Justiça, em um processo que se assemelha, nas suas limitações, à Ação Direta de Inconstitucionalidade por Omissão e ao Mandado de Injunção, previstos no ordenamento jurídico brasileiro.

A proteção de dados na Europa é considerada como um direito fundamental, tendo em vista sua previsão expressa no artigo 8º da Carta dos Direitos Fundamentais da União Europeia – CDFUE, que consagra a todos o direito à proteção de dados de caráter pessoal, prevendo ainda que esses dados devem ser objeto de um tratamento leal e com o consentimento da pessoa interessada (UNIÃO EUROPEIA, 2016).

Do outro lado, já no continente sul-americano, tem-se no âmbito brasileiro a Lei Geral de Proteção de Dados – LGPD como uma lei recente, inspirada na lei europeia, com o objetivo de garantir maior proteção à intimidade e à vida privada, e que surge para harmonizar os conceitos e princípios previstos na CRFB/88 e nas leis infraconstitucionais do país.

A Lei surge como uma tentativa de controlar a forma como os dados pessoais são tratados no território brasileiro, prevendo inúmeros regulamentos e sanções, visando obrigar os sujeitos às quais é destinada a cumpri-la.

Assim como na legislação europeia, a LGPD previu o consentimento como principal elemento essencial para a autorização e para o tratamento de dados pessoais. Existem inúmeras camadas que fundamentam esse instituto, que serão abordadas no tópico seguinte.

4.2 Natureza jurídica do consentimento

Com a evolução das leis que têm por objeto a proteção de dados, é claro o papel central do consentimento à medida que impõe ao titular dos dados a opção de fornecer seus dados e, ao controlador, a responsabilidade de lidar com os dados somente para os fins requisitados no momento do consentimento.

Conforme o art. 4º, item 11, da GDPR, consentimento é "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (UNIÃO EUROPEIA, 2016, não paginado).

O doutrinador Orlando Gomes (2006) define o consentimento como um elemento do direito pelo qual os indivíduos são capazes de exprimir sua vontade de contratar, dando ciência à outra parte da sua intenção negocial para que seja selado um compromisso entre os envolvidos. Contudo, essa abordagem refere-se mais ao aspecto contratual do que à própria proteção de dados.

Quanto à natureza jurídica, diversas são as controvérsias que envolvem sua definição. Na doutrina, encontram-se três principais correntes que se contrapõem. A primeira delas compreende que o consentimento para o processamento de dados tem a natureza de uma declaração de vontade negocial.

Por outro lado, parte da doutrina defende que trata-se de um ato jurídico unilateral, sem natureza negocial, contraponto à ideia dos autores já apresentados. Por fim, parte da doutrina sustenta, ainda, que o consentimento nada mais é que um ato que se assemelha ao negócio jurídico sem o ser.

Doneda (2006), contrapondo-se à última doutrina, compreende não ser apropriado atribuir uma natureza puramente negocial ao consentimento, tendo em vista que considera que essa conceituação implica na interpretação meramente contratual, dificultando a compreensão desse conceito sob a perspectiva de proteção de dados. Nesse sentido, aponta que:

> Assim, justifica-se a não consideração deste consentimento como um negócio jurídico, já que esta opção reforçaria o sinalagma entre o consentimento para o tratamento dos dados pessoais e uma determinada vantagem obtida por aquele que consente, reforçando a sua índole contratual e, consequentemente, acarretando a utilização de esquemas proprietários para o tratamento de dados pessoais (DONEDA, 2006, p. 377).

Para o autor, às vezes o consentimento tem o efeito principal de autorizar um determinado tratamento de dados, sem, entretanto, estar vinculado a uma estrutura negocial, o que insere Donena (2006) na segunda corrente doutrinária.

Laura Mendes, contrapondo o entendimento de Doneda, afirma que o consentimento possui algumas características negociais; contudo, ressalta que esse instituto possui, ao mesmo tempo, um caráter personalíssimo, o que aproxima a autora da última corrente, que defende o negócio jurídico sem o ser (MENDES, 2014, p. 60).

Abordando o consentimento vinculado à proteção de dados, Mendes (2014) indica que este pode ser considerado como o mecanismo que o direito possui para fazer valer a autonomia privada do cidadão, dando a ele esse poder de escolha.

Assim, apesar das divergências doutrinárias acerca da natureza jurídica do consentimento, há de se concordar, por fim, que trata-se de um instituto de natureza híbrida, reunindo, por vezes, elementos de natureza negocial, conforme defende parte da doutrina e, por vezes, sendo um ato jurídico unilateral, sem essas vestes negociais.

4.3 O consentimento como requisito para tratamento de dados pessoais e seus pressupostos de validade

Apesar das divergências doutrinárias acerca da natureza jurídica do consentimento, conforme apresentado anteriormente, a maior parte da doutrina concorda em um ponto: o consentimento é um pressuposto para o tratamento de dados pessoais.

Como já exposto no presente trabalho, buscando trazer maior segurança jurídica ao tratamento de dados pessoais nos seus territórios, os Estados buscam inserir barreiras e limitações para controlar a atividade ilimitada de empresas que monetizam esses dados, de forma a coibir esse mercado.

Assim, surge como elemento principal nas legislações brasileira e europeia o instituto do consentimento, uma barreira, quase intransponível, para dar maior segurança aos dados pessoais e, conforme apontado por Laura Mendes (2014), dar esse poder de escolha ao titular, que opta ou não por consentir com o tratamento de seus dados.

Ambas as legislações, dando esse poder de escolha ao titular, centraliza nele a decisão de consentir (ou não) com o fornecimento dos dados pessoais. Entretanto, não basta apenas que o consentimento seja registrado pelo titular, tendo em vista que esse instituto possui requisitos intrínsecos e essenciais para que seja garantida sua validade.

Entre os requisitos para um consentimento válido podemos destacar: o consentimento livre e espontâneo, com uma finalidade específica, com informações sobre os objetivos da coleta e tratamento dos dados, dentre outros que serão melhor abordados a seguir.

No que tange à GDPR, tem-se no artigo 4º, item 11, alguns desses critérios de maneira expressa. No texto da lei, tem-se que o consentimento deve ser livre, específico, explícito, informado e inequívoco.[10]

Tais critérios impactam diretamente nos Termos de Uso e Políticas de Privacidade de alguns *sites*, empresas e redes sociais, que, por vezes, ao longo de seus formulários, acabam por disfarçar detalhes quanto ao consentimento do usuário.

4.3.1 Elementos do Consentimento na *General Data Protection Regulation*

A Lei europeia traz, no artigo 4 da Diretiva 95/46, que o consentimento deve possuir alguns elementos para ser considerado como válido. Os pressupostos de validade do consentimento serão trabalhados a seguir de maneira individualizada.

4.3.1.1 Livre e espontâneo

Segundo a *General Data Protection Regulation*, por livre e espontâneo entende-se que o indivíduo, dotado de sua liberdade, sem qualquer coação, deve aderir às condições impostas pela empresa quando da coleta de dados. Assim, ele deve concordar, por um ato de vontade, com os termos estabelecidos, devendo ser precedida por um ato de vontade livre e espontâneo.

[10] *In verbis:* Artigo 4º: Para efeitos do presente regulamento, entende-se por: Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento (UNIÃO EUROPEIA, 2016, não paginado).

Corroborando esse entendimento, Schermer, Custers e Hof (2014) defendem que esse aspecto se enquadra como a ausência de coerção por terceiros. Assim, segundo os doutrinadores, para que o consentimento seja válido ele deve ser oferecido de maneira livre, como resultado de uma escolha autônoma e inequívoca do titular.

Insta destacar que parte da doutrina defende que o objetivo do legislador ao inserir esses termos foi coibir práticas abusivas, como por exemplo o site que já deixa uma caixa de diálogo pré-marcada, restando ao usuário somente confirmar ao final da página.

Segundo o considerando 42 da GDPR, tal prática é abusiva e viola os dispositivos, tendo em vista que o usuário deve manifestar sua vontade de maneira espontânea e, portanto, não pode haver caixas pré-selecionadas.

Além disso, seriam consideradas como inválidas as confirmações dadas, de acordo com o próprio regulamento europeu.

4.3.1.2 Específico

Outrossim, no momento da coleta, deve-se respeitar a finalidade para qual os dados estão sendo recolhidos. Sendo assim, o controlador deve informar detalhes acerca de quais dados pessoais estão sendo coletados, para quais finalidades eles serão utilizados e, também, quanto a sua necessidade. Ademais, insta destacar que não pode haver a alteração da finalidade com o objetivo de burlar a legislação.

Além disso, coloca que o responsável pelo tratamento deve aplicar: i) especificação da finalidade como proteção contra desvio de função; ii) granularidade nas solicitações de consentimento; e ainda iii) separação clara de informações relacionadas à obtenção de consentimento para atividades de processamento de dados.

4.3.1.3 Informado

Por fim, o consentimento deve ainda ser informado, de modo que, com base no Artigo 5 da GDPR, a exigência de transparência é um dos princípios fundamentais, intimamente relacionado com os princípios de justiça e legalidade.

Sendo assim, fornecer informações aos titulares dos dados antes de obter o seu consentimento é essencial para que possam tomar decisões informadas, compreender com o que estão concordando, e, por exemplo, exercer o seu direito de retirar o seu consentimento.

Para tanto, a lei europeia ainda estipula requisitos para que esse consentimento seja

informado, indicando que pelo menos as seguintes informações são necessárias para obter consentimento válido: i) a identidade dos controladores; ii) a finalidade de cada uma das operações de tratamento para as quais o consentimento é solicitado; e iii) quais (tipos de) dados serão coletados e usados.

4.3.2 Elementos do Consentimento na Lei Geral de Proteção de Dados

Não obstante, inspirados na legislação europeia, a Lei Geral de Proteção de Dados manteve os pressupostos de validade do consentimento disposto na GDPR quando estabelece o conceito, no seu artigo 5º, XII, de uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018, não paginado).

4.3.2.1 Informado

Agregado à boa-fé negocial, o adjetivo informado surge como um direito ao usuário e um dever aos responsáveis pelo tratamento dos dados pessoais: direito-dever de informação. Para tornar o consentimento válido, antes de mais nada, faz-se necessário que o titular detenha informações suficientes para se capacitar e decidir.

Analisando o significado do próprio termo informação, Bioni (2018, p. 191) traz as afirmações de Cláudia Lima Marques de que "é 'dar forma, é colocar (in) em uma forma, aquilo que um sabe ou deveria saber (o expert) e que outro (leigo) ainda não sabe".

Tamanha é sua importância no ambiente da proteção de dados pessoais que, na maior parte da doutrina, a expressão "consentimento informado" é substituída pelo simples termo "consentimento", estando inerentes, portanto, as informações elementares disponíveis ao indivíduo.

4.3.2.2 Livre e espontâneo

Conforme visto anteriormente, o consentimento é um ato de vontade livre e inequívoco do titular dos dados, que, no momento que concorda com os termos apresentados, fornece seus dados pessoais ao controlador, que está autorizado a tratar esses dados.

Com base no histórico normativo, inclusive do brasileiro em relação ao direito privado, verificou-se que o instituto do consentimento esteve muitas vezes atrelado aos defeitos do

negócio jurídico: "para que a relação negocial seja válida, é preciso que o consentimento da parte seja livre e consciente" (BIONI, 2018, p. 190).

Agora, nesta perspectiva, a declaração de vontade deverá advir sem qualquer coação (física ou moral), partindo de uma escolha livre e espontânea vontade do indivíduo (MALHEIRO, 2017, p. 46).

Desse modo, para que o processamento dos dados seja lícito, o consentimento do titular deverá indicar a concordância desse indivíuo na sessão de seus dados que, para ser considerada válida, deverá ter sido entregue de forma livre e específica, numa real demonstração de vontade do mesmo", independente do ambiente em que os dados foram coletados (SOUZA, 2018, p. 30).

Observa-se que, no entendimento de Souza (2018, p. 30), o instituto do consentimento estaria categorizado como um ato unilateral, devendo-se separá-lo em duas etapas: quando da declaração de vontade que concede o processamento dos dados (ingresso no ambiente privado do titular) e quando da autorização acerca do compartilhamento dos dados.

4.3.2.3 Inequívoco e com finalidades determinadas

Inicialmente, tem-se que o tratamento dos dados passa a ser uma atividade exercida com um fim específico e explícito, ao passo que, ao relacioná-lo com o instituto do consentimento, atrela-se à imprescindibilidade de direção, servindo, inclusive, como um caminho a ser perseguido (posteriormente) para a verificação das informações passadas ao usuário que deu origem à declaração de vontade livre (BIONI, 2018).

Partindo para uma carga participativa intermediária do indivíduo sobre seus dados, tem-se a adjetivação com o termo inequívoco, por meio do qual se encontram tácitas autorizações dentro do contexto do fluxo informacional. Nesse sentido, tem-se situações nas quais o consentimento torna-se prescindível, uma vez que encontram-se dentro das legítimas expectativas do titular dos dados.

Já quanto à categorização de consentimento com finalidade determinada, a carga participativa do titular dos dados passa a ser pré-intermediária, tendo em vista que, por estar vinculado aos princípios de informação e transparência, tal adjetivação recebe uma maior importância (MALHEIRO, 2017).

Sob este cerne, o consentimento deve estar voltado a um fim específico, excluindo-se propósitos genéricos que poderiam fazer com que o titular emitisse um cheque em branco aos coletores de dados – afasta-se a possibilidade de uma declaração de vontade genérica por parte

do titular dos dados e de uma interpretação extensiva além das que estariam previstas (DONEDA, 2006).

4.4 Princípios e conceitos da Lei Geral de Proteção de Dados no Brasil sob a ótica da proteção de dados de crianças e adolescentes

A Lei Geral de Proteção de Dados foi nitidamente inspirada na legislação europeia (COTS; OLIVEIRA, 2019), alinhando-se a um dos principais instrumentos legislativos mundiais sobre o tema – principalmente o europeu e o americano.

Houve um grande avanço legislativo, pois a referida lei modificou a interpretação quanto à coleta de dados, dando poderes ao titular e concentrando na figura deste os atos de disposição, revestindo-o inclusive do caráter de irrenunciabilidade (COTS; OLIVEIRA, 2019).

O artigo 5º da Lei nº 13.709/2018 traz alguns dos conceitos mais relevantes para esse estudo, dentre os quais destaca, a priori, em seu inciso I, o conceito de dado pessoal, dispondo que dado pessoal seria toda informação relacionada à pessoa natural identificada ou identificável (BRASIL, 2018, não paginado).

Outrossim, existe ainda uma terceira espécie de dado, com o qual a legislação preocupou-se: o dado pessoal sensível. Esse dado merece tratamento especial, tendo em vista que, nos moldes do inciso II do artigo 5º, trata-se de um dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural[11].

Sendo assim, tal dispositivo reflete a preocupação do legislador em garantir a maior segurança àqueles dados que, se expostos, podem afetar diretamente a honra e a imagem do usuário, causando danos por vezes irreparáveis.

Ademais, por se falar em usuário, a legislação estabelece alguns atores presentes no tratamento de dados, dentre os quais merecem destaque o controlador, o operador, o encarregado e o próprio titular.

Nos moldes do inciso V do artigo 5º, tem-se que a legislação considera como titular toda

[11] *In verbis:* Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018, não paginado).

pessoa natural a quem se referem os dados pessoais que são objeto de tratamento[12]. Tal conceito é autoexplicativo, não sendo necessárias muitas considerações acerca.

Prevê, do mesmo modo, o inciso VI do artigo supracitado, o controlador como toda pessoa natural ou jurídica, de direito público ou privado a quem competem as decisões referentes ao tratamento de dados pessoais[13].

Destaca-se que o legislador também considerou a possibilidade da Pessoa Jurídica de Direito Público figurar como controladora, visando assim trazer maior segurança também ao tratamento de dados efetuados por entes da administração direta e indireta, como autarquias e fundações públicas.

Por fim, a lei prevê, no inciso VIII do mesmo artigo, como sujeito da relação, o encarregado, que será toda pessoa que, indicada pelo controlador, atuará como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, facilitando assim o tratamento de dados pessoais[14]. Esse sujeito foi idealizado no *Data Protection Officer (DPO)* previsto na GDPR.

O inciso VII, por sua vez, indica que se considera como operador toda pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Aqui, tem-se a possibilidade de outorga do armazenamento para, por exemplo, empresas de armazenamento na nuvem, sendo essas igualmente responsáveis em caso de eventuais incidentes, apurada sua responsabilidade nos moldes dos artigos acerca do processo cabível.

Sendo assim, resta claro que, quanto ao espectro de aplicação da LGPD, ela destina-se a todas as pessoas naturais ou jurídicas, de direito público ou privado, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que: a) o tratamento de dados seja realizado no Brasil; b) os dados tenham sido coletados no território nacional; c) o tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no Brasil.

O espectro de aplicação da lei é tão amplo que não é demais dizer que praticamente todas as empresas devem observar suas regras.

No que tange aos princípios, esses justificam a essência da norma, para que essa busque

---

[12] *In verbis:* V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (BRASIL, 2018, não paginado).

[13] *In verbis:* VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018, não paginado).

[14] *In verbis:* VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018, não paginado).

sua legitimação e sustentação no ordenamento jurídico, bem como são considerados como fonte do Direito, funcionando como direcionamento para supressão de lacunas.

Ademais, destacam-se as palavras de Celso Antônio Bandeira de Melo (2004, p. 451), ao discorrer acerca dos princípios, indicando que estes podem ser considerados como:

> O princípio é um mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servindo de critério para a sua exata compreensão e inteligência, exatamente para definir a lógica e racionalidade do sistema normativo, no que lhe confere a tônica de lhe dá sentido harmônico.

Nesse sentido, conforme amplamente discutido no presente trabalho, a Lei Geral de Proteção de Dados inspirou-se na *General Data Protection Regulation,* absorvendo assim grande parte dos seus princípios e conceitos, apenas adaptando-os à realidade brasileira.

Dentre os princípios previstos na Lei Geral de Proteção de Dados, merecem destaque os princípios da finalidade e da adequação. Por mais que não tenham o mesmo significado, tais princípios encontram-se agrupados, pois se complementam. Na medida em que o primeiro estabelece que o tratamento de dados no território brasileiro deve atender aos limites descritos no momento da sua coleta, e que esses devem ser informados ao titular, o segundo indica que esses limites devem ser estritamente cumpridos pelo controlador.

No que tange especificamente ao Princípio da Finalidade, a legislação estabelece que a coleta deve ser pautada em requisitos dispostos no texto legal, dos quais pode-se destacar a observância de propósitos legítimos, explícitos, específicos e informados ao usuário, de modo que é vedado o tratamento de dados com finalidades genéricas e/ou indeterminadas.

Por ser um princípio implícito, não há no texto da Lei nº 13.709/2018 qualquer menção explícita ao Princípio da Finalidade, mas tão somente artigos que fazem referência à observância de tal princípio, dentre os quais se pode destacar o Art. 8º, §§ 4º e 6º, que, de maneira resumida, prevê que o consentimento deverá seguir essas finalidades determinadas, bem como deverá ser destacado[15].

Ademais, quanto ao artigo 26 da Lei Geral de Proteção de Dados, tem-se que esse princípio abarca também o uso compartilhado de dados pelo Poder Público, deixando claro que a finalidade é de observância obrigatória também às Pessoas Jurídicas de Direito Público que

[15]*In verbis:* Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (...) § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração (BRASIL, 2018, não paginado).

compõe a Administração Pública Direta e Indireta[16].

Através do trecho destacado, percebe-se a clara intenção do legislador em garantir a segurança, não somente dos dados por particulares, mas também dos que estão sob a guarda do Poder Público, sendo vedada a utilização desses bancos de dados públicos para finalidades que não as específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas.

De modo semelhante, o Princípio da Adequação indica que o responsável pelo tratamento dos dados, ou seja, o controlador, deve garantir o efetivo cumprimento dos limites já abordados anteriormente. Sendo assim, fica a cargo deste o respeito a esses limites, sendo vedado pela legislação a utilização de modo diverso daquele permitido no momento do consentimento, conforme já amplamente discutido.

A relevância desses princípios se justifica, dentre outras características, pela limitação que trazem à coleta e ao tratamento dos dados, impedindo que o detentor desses dados faça uso distinto do previsto no momento do seu recolhimento.

Sob a ótica de dados pessoais de crianças e adolescentes, os princípios destacados indicam que a empresa que coleta dados pessoais desses sujeitos – a exemplo das escolas, que serão abordadas a seguir de maneira mais clara – não podem desviar da finalidade para os quais os dados foram coletados.

Assim como os princípios ora destacados, a necessidade também insere limites ao tratamento dos dados pessoais. Segundo esse princípio, o controlador deve recolher tão somente os dados e informações necessários à finalidade.

Sendo assim, os dados recolhidos devem ser proporcionais, pertinentes e não excessíveis, atendendo apenas ao alcance da finalidade da empresa. O objetivo desse princípio é inibir a coleta de dados desnecessários, protegendo o usuário e impedindo que o controlador possua dados que não são, literalmente, necessários.

Outrossim, o referido visa também conferir proteção à empresa, uma vez que, conforme visto no início do presente capítulo, o recolhimento de dados sensíveis implica em ônus para o controlador, que deverá garantir maior segurança a esses dados.

Desse modo, trazendo para a realidade, faz-se necessário que uma academia que utilize sistema de biometria recolha a impressão digital e os dados pessoais dos seus usuários; contudo,

[16] *In verbis:* Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. (BRASIL, 2018, não paginado)

não parece razoável que no formulário de cadastro exija-se, por exemplo, a orientação sexual do usuário.

Caso assim o faça, a academia deverá providenciar mecanismos de segurança que garantam que esses dados considerados como sensíveis não sejam alvo de ataques cibernéticos, e, em uma hipótese de vazamento, venham a prejudicar a imagem dos seus clientes, expondo-os de maneira desnecessária.

Tal princípio está previsto no artigo 10 da Lei Geral de Proteção de Dados, indicando expressamente que somente os dados estritamente necessários para atingir a finalidade devem ser tratados[17].

No que tange aos dados de crianças e adolescentes, por lógica, tratam-se de dados naturalmente sensíveis, de modo que as empresas responsáveis por essa coleta devem limitar-se aos dados estritamente necessários para o desempenho daquela finalidade.

Por lógica, como destacou-se anteriormente, o tratamento de dados deve restringir-se àqueles necessários, com o fito de assegurar segurança ao usuário, que tem os seus dados recolhidos, bem como ao controlador, responsável por todos os dados recolhidos.

Esse é o Princípio da Segurança que, de maneira resumida, assevera que o controlador deve adotar mecanismos de segurança capazes de assegurar a segurança dos dados recolhidos, buscando sempre medidas técnicas e administrativas visando à sua proteção.

Insta destacar que tais medidas devem estar ao seu alcance, para prevenir que tais dados possam ser vazados ou divulgados sem autorização. Entretanto, merece destaque, mais uma vez, que tais técnicas devem estar ao alcance do controlador.

Assim, não parece razoável exigir que um microempresário que trata dados pessoais dos seus usuários adote um sistema de proteção que exceda o seu proveito econômico, sob pena de pôr em risco a atividade econômica desenvolvida e prejudicá-la.

Entretanto, quando se fala de grandes corporações, que dispõem de recursos e mecanismos para proteção dos dados recolhidos, mas, ainda assim, não o fazem, seja por negligência ou dolo, devem ser responsabilizadas pelos incidentes ocasionados, bem como pela indenização dos usuários afetados pela sua conduta.

Dessa forma, o artigo 39 da LGPD indica, em um rol exemplificativo, as condutas que devem ser adotadas para garantir a segurança dos dados, remetendo assim ao Princípio da

[17] *In verbis:* Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei (BRASIL, 2018, não paginado).

Segurança, trazendo que "o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria" (BRASIL, 2018, não paginado).

Do mesmo modo, em que pese que os princípios destacados anteriormente sejam relacionados à segurança dos dados, merece destaque o da responsabilização. Esse princípio prima pela responsabilidade dos agentes envolvidos no tratamento de dados em caso de violação das normas aqui descritas.

Semelhante ao instituto da Responsabilidade Civil, previsto no Código Civil de 2002, segundo o qual estabelece-se a necessidade de indenização por parte de quem causar dano a outrem (BRASIL, 2002, não paginado), o artigo 42 da Lei Geral de Proteção de Dados indica que o controlador deve reparar os danos causados em casos de violação ao disposto na lei[18].

A importância desse princípio é tamanha que poderia haver um capítulo destinado apenas a ele e às consequências da sua aplicação. A sua inclusão no presente estudo justifica-se pela sua relevância caso ocorra o vazamento de dados pessoais de crianças e adolescentes, caso em que se recorrerá às sanções previstas na legislação.

Assim, a legislação brasileira deixa claro que, sem consentimento e fora das hipóteses de exceções previstas em lei, o tratamento de dados de crianças será considerado ilícito e, desta maneira, sujeito às sanções legais.

Do mesmo modo, o tratamento de dados de adolescentes que não observar o Princípio da Transparência ou quaisquer das demais normas e princípios da LGPD. O artigo 52 da Lei Geral de Proteção de Dados especifica que a violação às suas diretrizes sujeitará o infrator à inúmeras penalidades, que serão igualmente abordadas a seguir.

Conclui-se, portanto, que, apesar da LGPD prometer ser um marco divisor e propulsor no que diz respeito à proteção de dados de crianças e adolescentes, é notório que a legislação no território brasileiro encontra inúmeras barreiras para garantir o seu efetivo cumprimento no que tange a esses sujeitos – que serão melhor tratadas a seguir.

[18]*In Verbis:* Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018, não paginado).

5 O TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES NA PRÁTICA: O CONSENTIMENTO PARENTAL E A (IN)EFICÁCIA DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Conforme visto no decorrer deste trabalho, apesar de consistir em uma ótima tentativa de proteção dos dados pessoais de crianças e adolescentes, a legislação brasileira, ao "inspirar-se" na legislação europeia, inseriu artigos que podem dificultar a sua efetividade no território brasileiro, visto que, se interpretados em sua literalidade e analisados sob a perspectiva atual, não são favoráveis para a sua aplicação.

Este último capítulo destina-se, assim, a promover reflexões acerca da aplicação dos princípios e regulamentos específicos no que tange à proteção de dados de crianças e adolescentes, com o objetivo principal de verificar sua efetividade e as dificuldades encontradas para sua aplicação, bem como fazer uma análise de direito comparado com o caso americano e promover uma análise sob as perspectivas para o futuro e possíveis soluções, não em uma tentativa de esgotar o tema, mas sim de promover uma profunda reflexão sobre a efetividade do regramento no território brasileiro e os mecanismos que podem ser utilizados para garantir a efetividade da Lei Geral de Proteção de Dados no Brasil.

5.1 O consentimento parental como requisito autorizador para tratamento de dados pessoais de crianças e adolescentes: uma análise jurídico-comparativa entre a Lei Geral de Proteção de Dados e a *General Data Protection Regulation*

Conforme já destacado anteriormente, é nítido que a revolução tecnológica transforma a sociedade e altera a forma como as pessoas vivem e como as relações se desenvolvem. O amplo acesso à informação em tempos em que praticamente todos estão conectados a todo tempo deve ser algo a se preocupar.

Entre essas preocupações, algumas merecem destaque, a exemplo da criação de uma geração datificada e do *profilling* como forma de tomada de decisão, mapeando o comportamento de consumidores praticamente antes do seu nascimento até quando esse atinge a vida adulta.

Exemplo claro disso, informalmente, é o caso da *Target* que, após analisar os dados internos, conseguiu mapear os diferentes produtos que as grávidas adquiriam de acordo com o mês de gestação. Um pai, nos EUA, foi surpreendido com um catálogo de grávidas direcionado à sua filha. Tempos depois, esse pai descobriu que sua filha realmente estava grávida, o que

demonstra de maneira exemplificativa e prática o poder de mapeamento de comportamento de consumidores.

Jessica Baron (2023), ao tratar da geração datificada, indica que todas as relações realizadas hoje estão sendo datificadas, isto é, transformadas em dados computadorizados, de modo que as pessoas estão sendo mapeadas antes mesmo de nascer, quer seja com a exposição do pré-natal ou ainda em tenra idade, expondo-as a estranhos, que poderão usar seus dados contra elas.

É nesse contexto que as legislações cujo objeto é o tratamento de dados pessoais, no caso brasileiro, a LGPD, ao seguir o parâmetro constitucional, estabeleceram um tratamento especial diferenciado para as crianças e adolescentes durante todo o seu texto.

A norma infraconstitucional, por questões de hierarquia, deve sempre respeito à Constituição. Sendo assim, todo regramento infraconstitucional, assim como Leis Ordinárias e Leis Federais, deve observar os princípios e as regras contidas na Constituição. Considerando que a Lei Geral de Proteção de Dados é norma inferior, tratou especificamente a matéria que envolve dados pessoais de crianças e adolescentes.

Assim, ao falar sobre o tratamento de dados pessoais das crianças, é imprescindível ter em mente, além da LGPD, ao menos três outras bases que a inspiraram e sustentam: a Constituição da República Federativa do Brasil de 1988 (CF/88), a Convenção sobre os Direitos da Criança e ainda o Estatuto da Criança e do Adolescente.

A CF/88 consagra a Doutrina da Proteção Integral à Criança e ao Adolescente, promulgando no artigo 127 que "é dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão" (BRASIL, 1988, não paginado).

Tal doutrina promove três premissas de fundamental importância para as normas infraconstitucionais a respeito das crianças e adolescentes: I) são sujeitos de direito; II) destinatárias de absoluta prioridade; III) é devido respeito à sua condição peculiar de pessoa em desenvolvimento.

Quando estabelece que são sujeitos de direitos, garante a possibilidade de adquirir direitos desde antes mesmo do seu nascimento – ponto que ainda gera debate na doutrina e nos Tribunais, a exemplo do direito de vida do feto diante da possibilidade de aborto –; porém, objeto do presente estudo não é esgotar o assunto.

A prioridade garante que a legislação assegure o tratamento especial que verifica-se no

texto presente na Lei Geral de Proteção de Dados. Por fim, quando trata da sua condição de pessoa em desenvolvimento, inspira todo o ordenamento para considerar, por exemplo, sua inimputabilidade e assegurar que todo texto que se refira a essas garanta essa proteção especial.

No mesmo contexto, o Decreto nº 99.710/1990 promulgou a Convenção sobre os Direitos da Criança, da Unicef, a qual, no âmbito internacional, entrou em vigor em 02 de setembro de 1990. Por meio do referido texto, segundo a doutrina e a hermenêutica jurídica, a Convenção tem *status* de norma supralegal no ordenamento pátrio, isto é, estando abaixo da Constituição Federal, mas acima das leis, impondo o controle de convencionalidade – o que, em linhas gerais, significa que a legislação nacional não deve contrariar as diretrizes e princípios da Convenção.

Desse modo, assim como a CF/88, a referida Convenção também acolhe a concepção do desenvolvimento integral da criança, reconhecendo-a como verdadeiro sujeito de direito, que exige proteção especial e absoluta prioridade.

Em seu texto, a referida Convenção define criança como "todo ser humano com menos de 18 anos de idade, a não ser que, pela legislação aplicável, a maioridade seja atingida mais cedo" (UNICEF, 1990).

Apesar do Estatuto da Criança considerar como criança o menor de 13 anos, o intuito da referida convenção é estabelecer o limite da maioridade como marco para não ser considerado criança. Isso porque, em um suposto confronto entre as leis, o Estatuto da Criança e do Adolescente considera criança a pessoa até doze anos de idade incompletos e adolescente aquela entre doze e dezoito anos de idade.

Após as considerações e conceitos de criança de acordo com o ordenamento jurídico brasileiro, importante voltar a atenção para o tratamento especial que a LGPD traz às crianças e adolescentes, especialmente que no que tange ao consentimento.

Conforme visto anteriormente, o consentimento é um ato de vontade livre e inequívoco do titular dos dados, que, no momento em que concorda com os termos apresentados, fornece seus dados pessoais ao controlador, que está autorizado a tratar esses dados.

Assim, segundo a teoria que defende o consentimento como uma espécie de negócio jurídico, tem-se que as crianças e adolescentes, na condição de relativamente incapazes, necessitam ser assistidos por seus representantes legais para que esse negócio jurídico tenha validade.

Assim dispõe o Código Civil brasileiro, ao indicar os limites etários para prática de atos civis, conforme dispõe Silvio Rodrigues (2003, p. 42) ao apontar que:

> O propósito do legislador brasileiro de fixar certa idade para aquisição de uma

> capacidade relativa já se encontra noutras legislações, e merece aplauso, porque a lei não pode ser casuísta, deferindo ao juiz prerrogativa para, examinando cada caso particular, decidir se determinado menor atingiu ou não uma relativa capacidade. A norma fixa em 16 anos a idade da maturidade relativa, e em 18 a da maioridade, baseando-se naquilo que habitualmente acontece.

Entretanto, a Lei Geral de Proteção de Dados não faz muitas menções nem traz esclarecimentos acerca do tratamento de dados envolvendo crianças e adolescentes, sendo o artigo 14 da LGPD o único que trata do tema. Assim, o referido dispositivo legal indica que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado com consentimento específico e, em destaque, dado por pelo menos um dos pais ou pelo responsável legal (BRASIL, 2018).

Essa manifestação de vontade, quando se tratar de menores de idade, segundo a lei, deve ser precedida de representação. Sendo assim, para que o ato ou negócio jurídico seja considerado válido, quando praticado por criança ou adolescente, deve ter como fundamento a representação ou assistência por meio do seu representante legal.

Sabe-se que, na prática, a aplicação desse dispositivo é utópica, tendo em vista que é cada vez mais comum a utilização da internet por menores de idade sem qualquer vistoria dos pais. Contudo, essa análise cabe a cada indivíduo, devendo se manter em destaque a preocupação do legislador em assegurar uma maior proteção, ainda que teórica, aos dados pessoais de crianças e adolescentes.

Quando previu o referido dispositivo, o legislador esperava que, constatando tratar-se de menor de idade, por meio da data de nascimento fornecida no momento do cadastro, as empresas deveriam suspender o tratamento de dados até que obtivessem o consentimento específico dos pais. O que, repise-se, não parece ter aplicação prática no cotidiano.

Nesse contexto, convergem as legislações brasileira e europeia, tendo em vista que a GDPR prevê expressamente no seu artigo 8º, item I, que, caso a criança tenha menos de 16 anos, o tratamento só é permitido caso o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança[19].

Assim, ambas as leis divergem tão somente no que tange ao limite etário atribuído, tendo em vista que a lei brasileira assegurou maior liberdade aos adolescentes ao permitir o tratamento de dados com o consentimento apenas do maior de 12 anos, enquanto a GDPR se mostrou mais

[19] *In verbis:* Artigo 8º. 1. Sempre que se aplique o artigo 6.º, n.º 1, alínea a), em relação à oferta de serviços da sociedade da informação diretamente a uma criança, o tratamento dos dados pessoais de uma criança será lícito se a criança tiver pelo menos 16 anos de idade. 2 Quando a criança tiver menos de 16 anos, esse tratamento só será lícito se e na medida em que o consentimento seja dado ou autorizado pelo titular da responsabilidade parental sobre a criança. 3 Os Estados-Membros podem prever por lei uma idade inferior para esses efeitos, desde que essa idade inferior não seja inferior a 13 anos. (UNIÃO EUROPEIA, 2016, não paginado).

rigorosa ao estipular esse limite em 16 anos.

Outrossim, o artigo 14, *caput*, da Lei Geral de Proteção de Dados aduz que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em respeito ao seu melhor interesse, nos termos da legislação pertinente (BRASIL, 2018).

Entretanto, o legislador não se preocupou em delimitar em que consiste o "melhor interesse", cabendo, então, a interpretação do texto em conjunto com outras regras do ordenamento jurídico brasileiro, tal qual o artigo 228 da CFRB/88 e o próprio Estatuto da Criança e do Adolescente.

Corroborando esse entendimento, Márcio Cots (2018, p. 141) aponta que o termo "melhor interesse" do menor é justamente aquele que não o prejudica, mas também que lhe traz benefícios.

Preocupando-se com a aplicação prática das limitações impostas, a LGPD permite, nos moldes do §3º do artigo 14 da Lei nº 13.709/2018, que poderão coletar os dados de crianças sem o consentimento quando essa coleta se mostrar como necessária para contatar os pais e ou o responsável, devendo ser utilizada somente uma vez e sem o armazenamento, não podendo esses dados serem transferidos a terceiros sem o consentimento (BRASIL, 2018).

Da leitura do dispositivo, extrai-se que o legislador, de maneira sagaz, preocupou-se em como o controlador iria obter os dados para contatar pais e responsáveis, tendo em vista que é vedado o consentimento da criança.

Sendo assim, abriu a exceção para tratar dados pessoais de crianças tão somente para o recolhimento dos dados suficientes para contatar pais e/ou responsáveis, devendo, para tanto, o controlador respeitar os limites impostos quanto ao armazenamento e à vedação a transferência a terceiro.

Sabe-se que, na prática, essa abertura interpretativa do dispositivo legal abrirá margem para escusas no cumprimento do disposto na lei. Isso porque as empresas podem justificar a violação com base no dispositivo apontado, não trazendo a lei mais informações.

A lei manteve a limitação tão somente a crianças que, na forma da lei, são aqueles menores de 12 anos. Isso abre margem para empresas interpretarem que, em se tratando de adolescente, o tratamento de dados poderá ser realizado independente do consentimento dos pais e/ou responsáveis.

A respeito, Renato Opice Blum (2023, não paginado) se questiona "se poderia a LGPD, ao silenciar sobre o consentimento dos pais no tocante à coleta de dados do adolescente, abrir exceção relevante à regra de nulidade da Lei Civil" (que considera, para os atos da vida civil, os menores de 16 anos como absolutamente incapazes). Ainda, se, nesse caso, o menor teria

“carta branca” para “decidir livremente sobre o futuro dos seus dados”. E conclui: embora defensável, tal entendimento é certamente preocupante – com o que devemos concordar.

Ademais, novamente preocupado com a aplicação prática do consentimento de crianças, o legislador prevê, no §5º do artigo 14 da Lei Geral de Proteção de Dados, que o controlador deve utilizar de todos os esforços e da tecnologia disponível para confirmar que o consentimento foi dado pelo responsável pela criança. Desse modo, na prática, fica a cargo do controlador a utilização dos meios possíveis para evitar vícios do consentimento e fraudes.

Tal dispositivo mantém relação direta com o disposto na *General Data Protection Regulation*, que aponta no item 2 do artigo 8º que o responsável pelo tratamento deve envidar todos os esforços possíveis para verificar que o consentimento foi dado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível (UNIÃO EUROPEIA, 2016).

Nesse contexto, tudo o que se refere a dados pessoais de crianças e adolescentes deve submeter-se à norma. Para tanto, é fundamental que o responsável pelo tratamento dos dados pessoais de crianças e adolescentes esteja certo quanto à faixa etária do público que pretende alcançar e, então, adote os meios adequados à aferição da idade e dos riscos potenciais, inclusive utilizando uma linguagem acessível ao seu público. Nesse sentido, inclusive, os §5º e 6º do artigo 14 da LGPD afirma:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> (...)
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

De acordo com o texto destacado anteriormente, isso implica que os Termos de Uso e Políticas de Privacidade de serviços e produtos voltados a crianças e adolescentes devem ser objetivos e em linguagem acessível. Portanto, termos prolixos, confusos, demasiadamente extensos e técnicos, ao menos no que depender da LGPD, estão com seus dias contados.

Ocorre que, após mais de cinco anos da promulgação da legislação, não se percebe mudanças tão significativas por parte da grande maioria das empresas que tratam dados pessoais de crianças e adolescentes no sentido de promover a aplicação da LGPD.

Isso porque, na teoria, constatando que se trata de menor de idade, por meio da data de nascimento fornecida, as empresas deveriam suspender o tratamento de dados até que obtenham

o consentimento específico dos pais. O que, repise-se, não parece ter aplicação prática no cotidiano brasileiro – principalmente se considerarmos as redes sociais mais populares entre as crianças, tais como *Tik Tok* e *Instagram*, além dos clássicos jogos para *smartphones*.

Utilizando como exemplo os Termos de Uso da rede social Tik Tok, possuindo como parte do público alvo menores de idade, estabelece que:

> "Limitação etária. Os Serviços destinam-se exclusivamente a pessoas com idade de 13 anos ou mais (sujeito às limitações adicionais porventura estabelecidas nos Termos Suplementares – Específicos da Região). Ao utilizar os Serviços, você estará confirmando que tem a idade mínima aqui especificada. Se chegar ao nosso conhecimento que alguma pessoa com idade inferior à idade mínima estabelecida acima está utilizando os Serviços, encerraremos a conta do usuário em questão."[20]

Ato seguinte, encaminhando-se para os Termos Suplementares[21], específicos de cada região, ao tratar de usuários domiciliados no Brasil, a rede social estabelece, em um texto em inglês, traduzido livremente, que:

> "Brasil. Se você estiver usando nossos Serviços no Brasil, os seguintes termos adicionais se aplicam. No caso de qualquer conflito entre os seguintes termos adicionais e as disposições do corpo principal destes Termos, os seguintes termos prevalecerão. Representação/assistência de pais e responsáveis. (i) se você tem mais de 16 anos, mas menos de 18 anos, você só pode usar e registrar uma conta com a assistência de seus pais ou responsáveis legais e representa e garante que você obteve assistência para usar os Serviços e concordar com estes Termos; (ii) se você tem mais de 13 anos, mas menos de 16 anos, você só pode usar e registrar uma conta com a representação de seus pais ou responsáveis legais e deve obter o consentimento de seus pais ou responsáveis legais para o uso dos Serviços e aceitação destes Termos. Lei e Jurisdição Aplicáveis. Estes Termos, seu assunto e sua formação, são regidos pela lei brasileira. Você e nós dois concordamos que os tribunais do Brasil terão jurisdição exclusiva."

No presente caso houve a incorporação e adaptação dos Termos de Uso para adequar-se ao disposto na LGPD, porém, sem efetividade prática, visto que no momento de cadastro na plataforma, a empresa não utiliza qualquer mecanismo que viabilize a verificação de consentimento parental, de modo que o cadastro na plataforma ocorre sem adequar-se ao disposto nos Termos de Uso da plataforma.

Do mesmo modo, a rede social X, antigamente conhecida como Twitter, adequou os

[20] Disponível em: https://www.tiktok.com/legal/page/row/terms-of-service/pt-BR (acesso em 12/03/2024).
[21] Disponível em: https://www.tiktok.com/legal/page/row/terms-of-service/en#supplemental-jurisdiction (acesso em 12/03/2024).

seus Termos de Uso[22] e disponibilizou um canal por meio do qual é possível realizar denúncias à contas que pertençam à crianças e adolescentes, demonstrando uma preocupação com o cumprimento da legislação. A rede social também realizou o banimento de inúmeras contas criadas, antes de 2018, por menores sem o devido consentimento, dando a oportunidade de regularização por meio do encaminhamento de documentos para provar a maioridade atual.

Utilizando do mecanismo de direito comparado, sob a égide do Regulamento Geral de Proteção de Dados Europeu (RGPD) ou *General Data Protection Regulation* (GDPR), em vigor desde 25 de maio de 2018, o legislador italiano, por meio da Lei 163, publicada em 6 de novembro de 2017 no Jornal Oficial da Itália, fixou que, quando necessário o consentimento dos pais ou responsáveis para o tratamento de dados de criança, só será considerado lícito se for dado ou autorizado pelo titular da responsabilidade parental da criança.

Neste sentido, entende o Poder Judiciário italiano, por exemplo, que a publicação de uma fotografia *online* se encaixa perfeitamente no escopo de proteção para o processamento de dados pessoais e sensíveis, porque interfere na vida privada da criança. Assim, deve ser dada especial atenção à publicação de imagens de menores, mesmo que isso diga respeito aos próprios filhos.

No mesmo sentido, sob tal perspectiva, um acórdão do Tribunal de Mântua, Itália (novembro de 2017), estabeleceu que, para a publicação de fotos de crianças, é necessário o consentimento dos pais. Na ausência do acordo dos pais, a foto simplesmente não é publicável. Essa questão nos conduz a refletir: considerando que os pais estejam de acordo com a publicação de fotos, vídeos, dados do pré-natal e outras peculiaridades da vida do menor, será que este também concordará com tal exposição, quando adolescente ou adulto? Como poderá exercer seu direito à autodeterminação informacional?

5.2 A proteção de dados no ambiente educacional

Após a compreensão dos princípios e conceitos básicos que regem a LGPD no território brasileiro, é possível chegar à conclusão de que diversas empresas entram no espectro de aplicação dessa lei, a exemplo de aplicativos, mídias sociais e *sites*; jogos também coletam informações pessoais e particulares de seus usuários, de modo que todas precisam se adequar às exigências do regulamento brasileiro de proteção de dados, inclusive no que se refere à nomeação de um responsável pela segurança dos dados coletados – que, conforme visto

[22] Disponível em: https://help.twitter.com/pt/forms/safety-and-sensitive-content/underage-user/x (acesso em 12/03/2024).

anteriormente, pode ser um DPO.

Trazendo o debate para o objeto de estudo do presente trabalho, focando em crianças e adolescentes, um cuidado redobrado deve ser tomado no que tange às escolas e ambientes educacionais.

Isso porque, quando as tecnologias digitais são utilizadas para fins educacionais, vários atores intervêm no processamento de dados de crianças e adolescentes, incluindo governos, legisladores, escolas públicas e privadas (funcionários e professores), empresas, fornecedores de produtos ou serviços, desenvolvedores de *software* e responsáveis legais. Todas as partes interessadas no sistema educativo devem garantir que as crianças possam ter acesso a mecanismos que garantam a proteção de dados e a privacidade, seja no ambiente físico ou no ambiente digital.

A utilização responsável dos dados das crianças desempenha um papel fundamental na promoção de seu bem-estar, especialmente quando se trata da gestão dos dados pessoais das crianças no sistema educativo. A violação da privacidade da informação pode ocorrer com a coleta, armazenamento ou processamento de dados pessoais de menores, especialmente se ocorrer sem o seu consentimento (UNICEF, 2018; Stoilova et al., 2020).

As escolas detêm uma grande quantidade de informações pessoais de menores, recolhidas ou fornecidas por alunos e pais. Os registros educacionais contêm informações sobre o histórico do aluno, fotografias, registros de frequência, impressões digitais, endereços, desempenho acadêmico, notas, resultados de testes padronizados, informações de saúde, avaliações psicológicas, relatórios de deficiência e comentários anedóticos de professores ou autoridades escolares sobre o desempenho acadêmico ou o comportamento dos alunos.

Importante destacar que as escolas, nesse cenário, desempenham papel fundamental para além do cumprimento da legislação. Isso porque participam ativamente da construção do indivíduo e da sua consciência mediante o processo de educação, podendo contribuir na conscientização dos alunos e dos pais com a mudança, em médio e longo prazo, da situação aqui narrada.

Assim, com base nessa confiança dos menores e dos pais, a proteção desses dados por parte das escolas deve ser estabelecida como um requisito. A adoção de boas práticas pode ser útil e deve envolver a consulta dos tutores legais e das crianças – de acordo com a sua capacidade e tendo em conta o melhor interesse da criança – sobre decisões de implantação de novas tecnologias que possam resultar no processamento de dados de crianças.

Van der Hof e Lievens (2017), propõem que outros instrumentos de proteção de dados, ou seja, a privacidade desde a concepção e as avaliações de impacto na proteção de dados, são

melhores ferramentas de proteção e capacitação no RGPD europeu, a fim de salvaguardar os dados das crianças. Analisam a lei e afirmam que a proteção de dados parece ilusória dadas as complexidades do mundo digital, que é largamente dominado por interesses comerciais. Estes princípios exigem que os responsáveis pelo tratamento implementem medidas de proteção de dados na concepção dos seus sistemas de processamento de dados.

Neste sentido, é vital que as instituições públicas (geralmente diferentes autoridades cooperam e partilham informação), sejam obrigadas a aplicar um princípio de minimização de dados e cumprir as restrições de armazenamento e retenção. Além disso, os governos devem aplicar a regulamentação e monitorar qualquer violação dos direitos das crianças por parte das empresas no contexto educativo e no ambiente digital.

É essencial reconhecer que não é apenas o direito da criança à proteção de dados que é afetado quando se trata de educação e tecnologias digitais, mas também que o direito à privacidade e à proteção de dados são direitos que permitem a proteção de outros direitos da criança – direitos esses que possuem *status* de direito constitucional.

5.3 O caso dos EUA: *Federal Education Rights and Privacy Acts* (FERPA) e *Children's Online Privacy Protection Act* (COOPA) e a comparação com a regulação no território brasileiro

Utilizando da metodologia jurídico-comparativa, e trazendo o debate para o contexto americano, nos EUA, o governo estabeleceu proteções de privacidade para crianças, solicitando o consentimento dos pais ou tutores e implementando políticas que responsabilizam as organizações públicas e privadas pela obtenção de consentimento ao recolher, armazenar ou divulgar dados e garantir a utilização adequada. Os EUA possuem duas principais leis que tratam acerca do tema: o *Federal Education Rights and Privacy Acts* (FERPA)[23] e o *Children's Online Privacy Protection Act (*COOPA*)*[24].

A FERPA regulamenta, entre outras questões, a proteção de dados de menores no sistema educacional, sendo destinada tanto a instituições de ensino quanto aos pais e estudantes,

[23] A Lei dos Direitos e Privacidade da Educação Familiar (FERPA) concede certos direitos aos Pais e Alunos Elegíveis em relação aos Registros Educacionais mantidos pelas escolas e universidades, possuindo diversas seções dedicadas a instituições de ensino, pais, estudantes etc. Disponível em: https://www2.ed.gov/print/policy/gen/guid/fpco/ferpa/index.html. Acesso em: 27 out. 2023.

[24] A COPPA impõe determinados requisitos aos operadores de *websites* ou serviços *online* dirigidos a crianças com menos de 13 anos de idade, e aos operadores de outros *websites* ou serviços *online* que tenham conhecimento real de que estão a recolher informações pessoais *online* de uma criança com menos de 13 anos de idade. Disponível em https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. Acesso em 27 out. 2023.

possuindo diversas seções de acordo com o público, enquanto a COOPA, uma lei federal dos EUA adotada em 1998, concentra-se em prestadores de serviços *online* que têm conhecimento direto ou real de menores e coletam suas informações.

A regulamentação COPPA obriga os operadores de *websites* ou serviços *online* dirigidos a crianças (também aplicável a operadores de outros serviços *online* que tenham conhecimento real de que estão recolhendo informações pessoais *online* de uma criança) a notificarem que estão coletando informações pessoais de crianças e recolhendo informações verificáveis para consentimento dos pais. A Comissão Federal de Comércio (FTC) é o órgão federal que supervisiona a implementação da COPPA e deve garantir a utilização de métodos de verificação para consentimento parental de dados de crianças e adolescentes.

A FERPA afirma que as escolas que pretendam divulgar informações contidas nos registos dos alunos devem ter autorização por escrito dos pais ou do aluno elegível, de um indivíduo com 18 anos ou que frequente uma escola pós-secundária.

Percebe-se a preocupação clara com a proteção dos dados pessoais, no caso americano, com a criação de regulamentos específicos para a tutela de dados pessoais de crianças e adolescentes, assim como o apoio do órgão regulamentador (FTC) no cumprimento das políticas adotadas.

Trazendo para o cenário brasileiro, a FTC estaria "diretamente" ligada à ANPD (Autoridade Nacional de Proteção de Dados). A ANPD foi criada em decorrência da necessidade de alguém (um órgão) que zelasse pela proteção dos dados pessoais e que estabelecesse quais providências poderiam ser tomadas no caso de quebra do sigilo por violação da lei, além de atuar, fiscalizar e aplicar, quando o caso, as sanções e, em caso de violação, ser intermediador das reclamações que surgirem.

Apesar de possuir as suas funções bem delimitadas, pelo menos no texto legal, no que tange à proteção de dados pessoais de crianças e adolescentes, como anteriormente destacado, o Brasil carece de um ato normativo que trate de maneira direta as particularidades do processamento de dados pessoais desses sujeitos.

Desde a sua criação, feita por meio de Medida Provisória para preservar a competência originária disposta na constituição, esse órgão já apresentava polêmica. A medida provisória nº 869/2018 alterou a subordinação do referido órgão, retirando-o do Ministério da Justiça e atrelando-o à composição da Presidência da República, alterando também a sua configuração.

A Lei 13.853/2019, responsável por alterar a LGPD para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, ratificou o texto da Medida Provisória anterior, alterando apenas a composição dos membros do Conselho.

O governo federal manteve a ANPD sob seu domínio, ainda que o texto demonstre a tentativa da redação ao relativizar esse vínculo:

> Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.
> § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (BRASIL, 2019, não paginado).

Mais a frente, essa independência é limitada, ao passo que o texto do § 3º do artigo 55-A estabelece que "§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias" (BRASIL, 2019, não paginado).

Ou seja, sem independência financeira, e com a composição formada em mais de um terço por representantes indicados pelo Poder Executivo, fica clara a sua vinculação à Presidência.

Analisando a natureza jurídica da ANPD, e o disposto no artigo 55-B que "É assegurada autonomia técnica e decisória à ANPD", temos que, ao menos na lei, a sua autonomia decisória é assegurada – na prática, isso não foi possível de ser verificado (BRASIL, 2019, não paginado).

Ocorre que, na prática, conforme visto, o Poder Executivo domina integralmente esse órgão, quando observa-se a sua configuração e a porcentagem de origem dos seus integrantes. Apesar do objetivo deste estudo não ser o esgotamento do tema – que ensejaria um trabalho acadêmico por si só – chama-se a atenção para as limitações da ANPD quando do exercício do seu efetivo controle.

Essa subordinação direta da Autoridade ao órgão máximo do Executivo Federal afeta em demasia a autonomia, independência, fiscalização e as decisões de caráter técnico inerentes ao tema, em relação ao conceito previsto na primeira versão da Lei, hospedando a dúvida sobre até que ponto uma futura decisão política do Executivo Federal poderá suplantar uma análise técnica e independente sobre o escopo da LGPD (ATHENIENSE, 2018).

O cenário é ainda mais duvidoso quando ocorrer a necessidade de controle pela ANPD de um ato praticado pelo Poder Público, uma vez que que, conforme visto anteriormente, a administração também está sujeita ao regramento da LGPD.

Inúmeras são as hipóteses de tratamento de dados envolvendo a administração pública, seja no âmbito tributário, dados referentes à saúde ou ainda dados envolvendo investigados no âmbito dos processos penais. O espectro para tratamento de dados pessoais por parte do Poder Público é algo que deveria estar sendo alvo de questionamentos e debates mais incisivos.

Vladimir Aras, no artigo “A título de introdução: segurança pública e investigações criminais na era da proteção de dados”, aborda a temática da proteção de dados no âmbito do processo penal (ARAS et al., 2020, p. 25).

> Nesse sentido, as normas de proteção de dados pessoais devem aplicar-se também ao Estado quando coleta, manipula e difunde dados pessoais de investigados, suspeitos, réus, vítimas, testemunhas, peritos, autoridades e funcionários que atuam na persecução criminal e de terceiros eventualmente alcançados por medidas de apuração. Investigações criminais e medidas de segurança pública são atividades estatais que interferem rotineiramente na vida dos cidadãos, tornando-se relevante a perspectiva da privacidade.

Utilizando a metodologia jurídico-comparativa, é possível identificar que na GDPR foi assegurada a independência plena do órgão na Europa, o que fica claro a partir da leitura do artigo 52 do regramento:

> Artigo 52 – Independência 1. As autoridades de controle agem com total independência na prossecução das suas atribuições e no exercício dos poderes que lhes são atribuídos nos termos do presente regulamento. 2. Os membros das autoridades de controle não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem. 3. Os membros da autoridade de controle abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível. 4. Os Estados-Membros asseguram que cada autoridade de controle disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessárias à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comitê. 5. Os Estados-Membros asseguram que cada autoridade de controle selecione e disponha do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controle interessada. 6. Os Estados-Membros asseguram que cada autoridade de controle fique sujeita a um controle financeiro que não afete a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional.

Fica clara a preocupação do Parlamento em assegurar a independência da Autoridade no referido texto, principalmente ao observar a garantia da independência financeira ao prever que, apesar de estar integrado ao orçamento do Estado ou nacional e estar suscetível a um controle financeiro, esse controle não impacta na independência do referido órgão.

5.4 O analfabetismo digital e a dificuldade de aplicação de regulamentos de proteção de dados no território brasileiro

A maioria dos governos, em todo o mundo, não mede esforços para trabalhar e promover a implantação de redes, a conectividade e a inclusão digital. Várias iniciativas foram postas em prática para alocar recursos públicos e privados para promover a aprendizagem digital,

especialmente para crianças.

Uma vez garantido o acesso à internet, a prioridade para os pais, os decisores políticos e os sistemas educativos é manter as crianças protegidas dos riscos digitais, incluindo o *cyberbullying* e as violações da privacidade. É de extrema importância desenvolver políticas sólidas e claras, proporcionar aos professores e aos pais o apoio de que necessitam para proteger as crianças e fazer cumprir os quadros jurídicos estabelecidos a nível nacional.

Ramonet (1998) sublinha que os notáveis índices de desigualdade refletem-se também na distribuição mundial do acesso digital. Ele salienta, ainda, que têm surgido novas desigualdades, geradas pelo próprio desenvolvimento acelerado da internet. Segundo o autor, a expansão da internet tem gerado uma nova desigualdade, denominada por ele de "inforricos" e "infopobres", destacando que, em primeiro lugar, sempre apenas uma pequena minoria dispõe de computador pessoal, mesmo nos países ricos.

Ademais, lembra Ramonet (1998), a infraestrutura em telefonia e os aspectos cognitivos (no mínimo, a alfabetização, cujos índices são bastante diferenciados entre os diversos países do mundo) contam de maneira decisiva para a definição da clivagem entre "inforricos" e "infopobres". Na seguinte passagem, o autor deixa claro seu ponto de vista (RAMONET, 1998, p.145):

> Não há dúvida de que, com a Internet - mídia, daqui em diante, tão banal quanto o telefone - entramos em uma nova era da comunicação. Muitos estimam, com certa ingenuidade, que o volume cada vez maior de comunicação fará reinar, nas nossas sociedades, uma harmonia crescente. Ledo engano. A comunicação, em si, não constitui um progresso social. E ainda menos quando é controlada pelas grandes firmas comerciais da multimídia. Ou quando contribui para aprofundar as diferenças e as desigualdades entre cidadãos do mesmo país, ou habitantes do mesmo planeta.

No caso brasileiro, as enormes diferenças entre as áreas rurais e as urbanas representam um complicador adicional para que se tenha uma homogeneidade digital no país. As características do processo de industrialização brasileira permitiram a convivência de estruturas produtivas de diferenciados graus de produtividade, as quais, por sua vez, apresentam diferenciadas dificuldades de acesso às TICs, o que se expressa, em um segundo momento, em desiguais possibilidades de acessar dados, informações e atingir mercados para seus produtos, promovendo, por sua vez, heterogêneos resultados em termos de estratégias competitivas empresariais, conforme a capacidade de cada empresa usufruir das TICs como um mecanismo para incrementar sua respectiva participação nos mercados.

Em 2018, de acordo com o levantamento realizado pelo IBGE, 74,7% das pessoas já acessavam a internet, um avanço considerável em relação aos quase 70% alcançados em 2017.

Em 2018, 99,2% dos domicílios com acesso à internet utilizavam o aparelho celular, e

em 45,5% deles essa era a única forma de acesso. Complementando essa informação, a conexão por banda larga móvel subiu de 78,6% para 80,2% em um ano. Na região norte, a soberania do telefone celular é ainda mais expressiva, com o uso do 3G ou 4G chegando próximo de 90%, enquanto a banda larga fixa ficou em 53,4% – bem abaixo dos quase 76% verificados em todo o país.

Esses dados escancaram a dificuldade de inclusão digital no Brasil, demonstrando de maneira clara que, para além de um regramento que garanta uma pseudo-segurança digital, faz-se necessário promover, em princípio, o amplo acesso a essas ferramentas e ao conhecimento sobre o assunto, para desenvolver uma consciência na população por meio de políticas públicas que incentivem essa inclusão digital.

Apesar da legislação de proteção de dados surgir em um cenário emergente, principalmente se forem considerados os números que refletem o aumento de conexão por meio de aparelhos celulares, ainda enfrentará grandes dificuldades até alcançar o seu objetivo e a efetividade no Brasil.

A falta de consciência acerca da importância de um debate sobre proteção de dados e privacidade é decorrente do aceleramento desse debate no Poder Legislativo para aprovação da LGPD. Enquanto na Europa a GDPR necessitou de quase vinte e três anos para sua aprovação, após inúmeros debates e pesquisas, no Brasil, o caminho percorrido foi ao contrário, ocorrendo a tentativa de incorporação de um texto internacional sem debates e sem a participação da população, principais beneficiários da legislação.

De acordo com Maldonado e Blum (2019, p. 24), a autodeterminação informativa se apresenta como fundamento da LGPD, justamente nesse momento em que ainda predomina uma coleta e tratamento desenfreado de dados, "[...] como forma de devolver para o titular o poder sobre o fluxo e o uso dos seus dados, mediante o estabelecimento de determinações objetivas aos agentes de tratamento".

Mas, como é possível falar em autodeterminação informativa se a própria população não possui acesso ao conteúdo e, acima de tudo, não compreende a importância do controle dos dados pessoais fornecidos?

Indo além, como é possível se falar nesse controle em um cenário em que o sujeito titular, incapaz de fornecer seus dados pessoais por conta da sua idade, transfere essa prerrogativa a um responsável que sequer tem conhecimento das consequências do fornecimento dos dados pessoais dos seus filhos?

Fica nítido que o consentimento parental previsto na LGPD, apesar de louvável, tendo em vista que, após tanto tempo, ao menos é possível agora se falar em uma legislação que

garanta a mínima proteção mesmo que de maneira geral, ainda encontra inúmeras barreiras para alcançar sua efetividade.

Assim, mostra-se emergente que o país combata a falta de letramento digital se quiser garantir uma autodeterminação informativa consciente por parte da população, uma vez que a simples previsão desse direito sem a ampla divulgação e conscientização da aplicação da lei não garantem a sua eficiência.

Assim, torna-se inviável falar em um consentimento (nos moldes exigidos pela própria legislação) livre, espontâneo, específico e informado, sem criar na população a consciência acerca da importância da referida proteção.

Esse caminho deve ser percorrido por meio de políticas públicas e campanhas que, em um primeiro momento, demonstrem essa importância, na tentativa de desenvolver, em longo prazo, o discernimento da população brasileira acerca da proteção de dados pessoais.

Somente a partir daí, depois de trilhado um longo caminho, será possível falar em um consentimento conforme previsto na legislação e, somente a partir de então, isso refletirá no consentimento parental na forma esperada pela Lei Geral de Proteção de Dados.

CONCLUSÃO

Por meio do presente estudo foi possível identificar de maneira clara as consequências da incorporação de legislações estrangeiras sem a adequação para a realidade brasileira, de modo que, assim como ocorre em outros casos, a LGPD encontra inúmeros entraves destacados durante o texto que comprometem a sua efetividade.

Assim, a ausência de um regramento específico, associada à limitação da autonomia do órgão que, em tese, deveria ser responsável por garantir o efetivo cumprimento da LGPD, dificultam de modo severo a fiscalização e o cumprimento, por parte das empresas, no que tange aos dispositivos que asseguram o tratamento específico de dados pessoais de crianças e adolescentes.

O que se percebe na prática é que, apesar da intenção da lei em garantir esse cuidado especial ao tratamento de dados pessoais, principalmente de crianças e adolescentes, inúmeros entraves – sejam eles a falta de clareza na legislação ou a falta de uma proteção específica – garantem uma falsa sensação de proteção especial aos dados pessoais de menores.

Isso decorre, principalmente, da incorporação, em grande parte do texto da LGPD, das diretrizes previstas na GDPR, legislação europeia que foi criada após inúmeros debates e de acordo com a realidade de países desenvolvidos.

De fato, a cópia desses conceitos sem um profundo debate e, principalmente, sem considerar a taxa de analfabetismo digital e de letramento digital da população, e do desenvolvimento de uma consciência da população acerca da importância da proteção de dados pessoais, dificultam a efetividade buscada pelos legisladores quando promulgaram a referida lei.

Ademais, a partir da leitura do presente estudo, fica clara a necessidade da tutela específica, seja na própria LGPD ou em uma legislação apartada (recomendado), a proteção de dados pessoais de crianças e adolescentes considerando a realidade do sistema brasileiro, prevendo não somente a criação de obrigações para as empresas responsáveis por esse tratamento, mas também indicando políticas públicas de conscientização da população, a exemplo do que acontece nos Estados Unidos.

Prever regras genéricas, copiadas de uma legislação estrangeira, sem promover a sua adaptação e considerando as inúmeras dificuldades da sociedade brasileira – dentre as quais destaca-se a ausência de mecanismos que garantam a educação digital – mostrou-se insuficiente.

Além disso, merece destaque que o órgão criado para fiscalização deve adotar medidas

mais severas contra empresas que tratam dados pessoais de crianças e adolescentes, promovendo maior fiscalização e atuando, juntamente com essas, em conscientizar a população acerca da importância do tema.

Para tanto, antes de tudo, mostra-se necessária a reformulação desse órgão de modo a garantir uma maior autonomia e independência desse para a tomada de decisões, ao exemplo do que acontece com os órgãos fiscalizadores no território europeu abarcado pela GDPR.

Por fim, mostra-se ainda mais relevante que o debate seja promovido, na medida do estudo apresentado, junto às escolas e instituições de ensino, sendo uma alternativa viável a inclusão na grade obrigatória da BNCC (Base Nacional Comum Curricular) disciplinas que tratem sobre educação digital, segurança cibernética e *cyberbullying*, entre outros temas que combatam o analfabetismo digital e auxiliem na criação de uma consciência acerca da importância da proteção de dados pessoais.

Sugere-se ainda uma tutela específica para proteção de dados pessoais de crianças e adolescentes, políticas públicas por meio campanhas publicitárias, que podem ser inseridas até mesmo nas próprias redes sociais estimulando o consumo consciente e ressaltando a importância dos dados pessoais, bem como imposição de medidas severas em caso de descumprimento.

Importante destacar o papel da ANPD junto às redes sociais para estabelecer padrões mínimos que auxiliem na efetividade da lei, à exemplo da adoção de técnicas utilizando os meios tecnológicos disponíveis para verificação do consentimento parental de pais e responsáveis quando do fornecimento de dados pessoais de menores sob a sua tutela.

Os avanços tecnológicos demonstram-se suficientes para adoção de técnicas que viabilizem essa verificação que, apesar de prevista no texto da lei, não é verificada na prática pelas redes sociais que operam no território brasileiro.

REFERÊNCIAS

ARAS, V. B. A titulo de introdução: segurança pública e investigações criminais na era da proteção de dados. In: ARAS, V. B. et al. (Orgs.). **Proteção de Dados Pessoais e Investigação Criminal:** segurança pública e investigações criminais na era da proteção de dados. 2020. Disponível em: http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais versao_eletronica.pdf. Acesso em: 28 out. 2023.

ATHENIENSE, A. **Impactos das mudanças na Lei de Proteção de Dados Pessoais.** 2018. Disponível em: https://www.conjur.com.br/2018-dez-29/opiniao-impactos-mudancas-lei-protecao-dados-pessoais. Acesso em: 02 maio 2021.

AZEVEDO, A. C. C. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014.

BARON, J. **Nossas crianças estão sendo "datificadas", e isso pode colocá-las em perigo.** Tradução de Daniel Salgado. Disponível em: https://bit.ly/2NMymGx. Acesso em: 28 out. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BLUM, R. O. **Polêmica na proteção de dados de crianças e adolescentes.** Disponível em: https://bit.ly/37g86Mj. Acesso em: 17 out. 2023.

BRASIL. **Lei Geral de Proteção de Dados**. Lei nº. 13.709, de 14 de agosto de 2018. Brasília, 2018.

BRASIL. Câmara dos Deputados. **Marco Civil da Internet.** 2. ed. Brasília: Edições Câmara, 2015.

BRASIL. **Código Civil.** Lei nº. 10.403, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, 2002.

BRASIL. Constituição, 5 de outubro de 1988. **Constituição da República Federativa do Brasil.** Brasília, 1988.

CASTELLS, M. **A Sociedade em rede.** 6. ed. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 1999. v.1.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Ed. RT, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Revista dos Tribunais, 2019.

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

DWORKIN, R. **Los derechos en serio.** Barcelona: Ariel Derecho, 1999.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados: comentada.** 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2019.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet:** uma análise comparada do Regulamento Geral de Proteção de Dados europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (Bacharelado em Direito) — Universidade de Brasília, Brasília, 2017.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo.** 17 ed. São Paulo: Malheiros, 2004.

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

PIMENTA, V. R. Novas Tecnologias da Informação e Comunicação e a Possibilidade de Acesso à Justiça. **Revista de Direito Brasileira**, [S.l.], v. 4, n. 3, p. 544-560, set. 2013. ISSN 2358-1352. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/2649. Acesso em: 15 out. 2023.

RAMONET, I. **Geopolítica do Caos.** Petrópolis (RJ): Ed. Vozes, 1998.

RODOTÀ, S. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Silvio. **Direito Civil: Parte Geral**. v. 1. 34. ed. São Paulo: Saraiva, 2003.

SCHERMER, B. W.; CUSTERS, B.; VAN DER HOF, S. **The Crisis of Consent**: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418. Acesso em: out. 2023.

SILVEIRA, S. A. **Exclusão Digital:** a miséria na era da Informação. São Paulo: Ed. Fundação Perseu Abramo, 2001.

STRECK, L. L. **Verdade e Consenso.** Constituição, Hermenêutica e Teorias Discursivas. 2. ed. Rio de Janeiro: Lumen Juris, 2006.

STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 22 nov. 2023.

STOILOVA, M.; LIVINGSTONE, S.; NANDAGIRI, R. Digital por padrão: capacidade das crianças para compreender e gerenciar dados online e privacidade, mídia e comunicação. 2020. https://doi.org/10.17645/mac.v8i4.3407. Acesso em: 21 nov. 2023.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 22 de dezembro de 2006. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>. Acesso em: 10 out. 2019.

UNIÃO EUROPEIA. **General Data Protection Regulation**. Act 2016/679. 14 de abril de 2016. Disponível em: < https://gdpr-info.eu>. Acesso em: 10 out. 2019.

UNICEF. **Convenção sobre os Direitos da Criança.** Disponível em: https://uni.cf/38rvTJn. Acesso em: 21 nov. 2023.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.