

**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**  
**CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS**  
**FACULDADE DE DIREITO**

**TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES:  
ANÁLISES E PERSPECTIVAS**

**RENAN SANCHO BRANDÃO**

**Rio de Janeiro**  
**2022**

**RENAN SANCHO BRANDÃO**

**TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES:  
ANÁLISES E PERSPECTIVAS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Mestre Filipe José Medon Affonso**.

**Rio de Janeiro  
2022**

**RENAN SANCHO BRANDÃO**

**TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES:  
ANÁLISES E PERSPECTIVAS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Mestre Filipe José Medon Affonso**.

Data da Aprovação: \_\_/\_\_/\_\_\_\_.

Banca Examinadora:

\_\_\_\_\_  
Orientador

\_\_\_\_\_  
Co-orientador (Opcional)

\_\_\_\_\_  
Membro da Banca

**Rio de Janeiro  
2022**

## **AGRADECIMENTOS**

À Fátima Sancho, minha querida mãe, que sempre esteve ao meu lado e apoiou meus estudos independente de qualquer adversidade. Agradeço-a pelo fiel compromisso de ser uma figura materna incrível e por ter me ensinado a valorizar cada coisa e cada conquista em sua mais pura essência.

Ao Caio Matheus, meu companheiro que sempre se dedicou à construção de nossa história de parceria e me apoiou em cada empreitada profissional que decidi arriscar. Sem ele, não seria possível a conclusão deste trabalho.

Ao meu irmão Bruno Sancho e meu pai Alberto Brandão, familiares que acompanharam minha trajetória de vida e deram seu suporte aonde foram capazes de atuar.

À minha sogra Marcia Coelho, que com sua ternura e acolhimento possibilitou que eu tivesse espaços importantes de conforto e bem-estar durante a graduação.

Às minhas queridas amigas de graduação Walquiria Camilo, Jessica Soares, Beatriz Farias, Júlia Baroni e Sofia Ferreira. Talvez elas nem saibam, mas foram essenciais em diversos momentos com seu companheirismo para que eu pudesse concluir esta graduação.

À Liga de Direito e Tecnologia da UFRJ, em especial às professoras Erica Bakonyi, Flavia Lima e Ana Clara Chicrala, que me possibilitaram iniciar meus estudos dentro da área de proteção de dados pessoais.

Ao meu orientador Filipe José Medon Affonso, que me proporcionou o suporte necessário para a completude deste trabalho de monografia e me introduziu com sua influência a uma temática importante que foi meu objeto de estudo.

Às professoras Inês Ferreira Dias Tavares, Carina de Castro Quirino e Ana Luiza Fernandes Calil, que tiveram um papel essencial em minha formação e definitivamente me marcaram.

Aos lugares que estagiei e os profissionais que os integravam: Defensoria Pública do Estado do Rio de Janeiro (NUDEM), LL Advogados, Licks Attorneys e VTEX, que me proporcionaram um desenvolvimento profissional adequado e de qualidade que me permitiram ser o profissional que sou hoje.

À Faculdade Nacional de Direito da UFRJ, que é um ambiente incrível de aprendizado e contatos e espero que permaneça vivo por toda a história.

À minha querida amiga Suellen Gomes, grande parceira em muitos momentos durante meu período de graduação.

Aos meus queridos amigos Thadeu Augusto Rocha, Daniel Ventura e Lucas Lamy, que me proporcionaram acolhimento familiar e momentos de descontração importantes para a completude desta graduação.

*Sei que não é fácil assim  
mas vou aprender no fim  
minhas mãos se unem para que  
tirem do meu peito o que há de ruim.*

*“Indestrutível”, Pablo Vittar*

## RESUMO

O presente trabalho objetiva desenvolver uma análise sobre o tratamento de dados pessoais de crianças e adolescentes para produzir perspectivas sobre o tema. Para tanto, conceitos importantes sobre dados pessoais serão discutidos com vistas à avaliação das vulnerabilidades existentes no contexto digital a partir do público infantojuvenil - grupo focal da pesquisa. Nesse sentido, serão avaliadas as bases legais que permitem o tratamento de dados de crianças e adolescentes e o significado do conceito do melhor interesse presente no artigo 14 da Lei Geral de Proteção de Dados Pessoais brasileira. O estudo toma para análise alguns casos concretos e duas situações específicas envolvendo o uso da internet por crianças e adolescentes e seus responsáveis legais, sendo estas: controle excessivo e superexposição. Nesse sentido, o escopo do debate será subsidiado pela defesa da utilização do direito ao esquecimento para este grupo, bem como pelo questionamento dos aspectos e desafios regulatórios relacionados ao tratamento de dados pessoais de crianças e adolescentes. Pretende-se à conclusão, por fim, na proposta de elaboração de uma agenda regulatória pela Autoridade Nacional de Proteção de Dados Pessoais situada no entendimento do conceito da privacidade por design.

**Palavras-chave:** Direito e tecnologia; Proteção de Dados Pessoais; Crianças e adolescentes; LGPD; Lei Geral de Proteção de Dados Pessoais; Privacy by design.

## ABSTRACT

The present study aims to develop an analysis on the treatment of personal data of children and adolescents to produce perspectives about it. Therefore, important concepts about personal data will be discussed with a view to assessing the vulnerabilities existing in the digital context from the children and youth public - the research focus group. In this sense, the legal bases that allow the processing of data of children and adolescents and the meaning of the concept of best interest present in article 14 of the Brazilian General Personal Data Protection Law will be evaluated. The study takes for analysis some concrete cases and two specific situations involving the use of the internet by children and adolescents and their legal guardians, namely: excessive control and oversharenting. In this sense, the scope of the debate will be supported by the defense of the use of the right to be forgotten for this group, as well as by questioning regulatory aspects and challenges related to the processing of personal data of children and adolescents. It is intended to conclude, finally, in the proposal for the elaboration of a regulatory agenda by the Brazilian National Data Protection Authority situated in the understanding of the concept of privacy by design.

**Palavras-chave:** Law and technology; Personal data protection; Children and adolescents; LGPD; Brazilian General Personal Data Protection Law; Privacy by design.



## SUMÁRIO

<b>INTRODUÇÃO</b> .....	9
<b>1. Tratamento de dados pessoais de crianças e adolescentes</b> .....	10
1.1. Aspectos gerais sobre a proteção de dados pessoais de crianças e adolescentes .....	11
1.2. Bases legais para o tratamento de dados pessoais de crianças e adolescentes e estudo sobre melhor interesse .....	20
<b>2. Limites e mecanismos de controle no meio digital exercidos pelos pais e responsáveis legais em relação aos dados pessoais de seus filhos</b> .....	26
2.1. Nuances envolvendo o controle excessivo de acesso às redes e a superexposição promovidos pelos próprios pais ou responsáveis legais .....	26
2.2. – Direito ao esquecimento na perspectiva do tratamento de dados pessoais de crianças e adolescentes .....	38
<b>3 – Desafios e perspectivas regulatórias para o tratamento de dados pessoais de crianças e adolescentes: um olhar para a privacidade por design</b> .....	43
3.1. – Perspectivas regulatórias para o tratamento de dados pessoais de crianças e adolescentes .....	43
3.2. – Privacidade por design como a possível solução de um problema estrutural .....	48
<b>CONSIDERAÇÕES FINAIS</b> .....	58
<b>BIBLIOGRAFIA</b> .....	62

## INTRODUÇÃO

A proporção com que as tecnologias se desenvolvem e evoluem atualmente é visivelmente exponencial e intensa. Às vezes, chega a ser assustadora. Ninguém está totalmente ciente de tudo que acontece na internet. Este ambiente, que pode soar como “mágico” e ultrapassou diversos limites físicos e intelectuais dos seres humanos, definitivamente possui seus prós e seus contras. Nem todos, porém, lidam com o mundo digital da mesma forma, podendo alguns grupos estarem mais vulneráveis aos seus riscos.

Assim, o presente estudo busca se aprofundar sobre os contextos digitais envolvendo o tratamento de dados pessoais de crianças e adolescentes com foco no cenário brasileiro. Pretende-se entender quais são os aspectos gerais que regulam a proteção de dados desse grupo vulnerável assim como as bases legais possíveis de serem utilizadas para que este tratamento seja adequado.

Nesse sentido, serão analisados os riscos que envolvem crianças e adolescentes no ambiente digital, sejam promovidos por si próprios ou por seus responsáveis legais. Ainda, buscar-se-á entender a importância da internet e dos meios digitais na sociedade atual para seu desenvolvimento psicossocial. Afinal, a internet é um lugar tão perigoso assim? É possível que se encontre um equilíbrio para que as tecnologias sejam utilizadas e programadas focadas ao melhor interesse de crianças e adolescentes?

Para isso, serão estudados alguns casos concretos envolvendo o público infantojuvenil na sociedade digital e serão examinados os desafios regulatórios presentes no tratamento de seus dados pessoais. Para que, ao final, busque-se entender se é possível extrair soluções e medidas concretas para os riscos que envolvem esse tema a partir da regulamentação do design das arquiteturas digitais com vistas ao alcance dos princípios da privacidade e da autodeterminação informativa.

## 1. Tratamento de dados pessoais de crianças e adolescentes

### 1.1. Aspectos gerais sobre a proteção de dados pessoais de crianças e adolescentes

Imagine que o leitor entrou em um restaurante com um colega, sentou-se à mesa e começou a olhar para o cardápio. Logo em seguida uma família composta por um casal que agrega duas crianças e um adolescente sentou-se ao seu lado. Instantaneamente, assim que se sentam, cada um dos três retira de seus bolsos um dispositivo eletrônico: uma das crianças pega um videogame portátil e começa a jogar tão freneticamente que chega a morder seus lábios; a outra criança, com um iPad, liga um vídeo no *YouTube* e entra numa espécie de transe em que não enxerga mais nada ao seu redor; o adolescente saca seu telefone celular e alterna de forma extremamente rápida entre o *TikTok*, o *Twitter* e o *WhatsApp* e interage com amigos em todas essas redes sociais dinamicamente.

Nenhum dos três chega sequer a olhar o cardápio, apenas concorda com a cabeça com a sugestão dos pais. Estes, que conversam “em paz” sem a interrupção das crianças eventualmente também checam seus telefones celulares. Os três filhos do casal passam todo o jantar em seus dispositivos, deixando-os ao lado de seus pratos inclusive na hora de comer. A família mal se comunica entre si. A conta é paga, todos vão embora e as crianças e o adolescente saem do restaurante andando ainda olhando para seus dispositivos. O leitor mira de relance essa família algumas vezes durante sua estadia no restaurante.

Cenas como essa têm se tornado mais comuns a cada dia. Crianças e adolescentes estão constantemente utilizando a dispositivos digitais. Como o leitor se sente assistindo essa cena? O quão expostas pela internet o leitor acha que essas crianças e esse adolescente estão? Quantos dados pessoais estão sendo compartilhados a cada minuto com diferentes tipos de aplicativos? Será que esse excesso causa malefícios ou é benéfico para seu desenvolvimento?

E como o leitor se sentiria sobre um caso recente que dividiu opiniões? Uma criança de 2 anos que protagonizou um comercial para um dos maiores bancos do mundo falando “errado”. A princípio, soa fofo, mas será que essa criança sabe o que está fazendo? Será que sabe das consequências que aquela exposição pode causar

em sua vida? Quem decidiu que ela faria parte de um comercial? Será que a imagem dela pode viralizar? Como ela vai se sentir quando crescer caso isso ocorra? Como os pais dessa criança vão se sentir caso sua filha se torne um meme?

Essas situações descritas causam incômodo no leitor?

Crianças e adolescentes atualmente nascem em uma sociedade conectada e geralmente já são equipadas com aparelhos eletrônicos, sendo muitas vezes guiados pelos momentos de distração que seus dispositivos os podem proporcionar. O uso da Internet e das diversas tecnologias da informação e da comunicação hoje existentes alteraram de forma incisiva as relações sociais e negociais existentes<sup>1</sup>, pois a cultura digital está presente em basicamente todos os aspectos da nossa vida. Utilizar a tecnologia, no mundo de hoje, não é mais uma escolha individual<sup>2</sup>.

O contato extremo com a tecnologia faz com que seres humanos, sejam adultos ou crianças, estejam expostos a benefícios e riscos que sequer podem ser mensurados. Não apenas a imagem é envolvida no contexto digital, mas os dados pessoais das pessoas podem estar em constante exposição. Para tanto, entende-se por 'dado' a definição elaborada por Wolfgang Hoffmann-Riem<sup>3</sup>:

Os dados na literatura teórica são entendidos como sinais ou símbolos para mensagens que podem ser formalizadas e (aleatoriamente) reproduzidas e facilmente transportadas por meio de meios técnicos adequados. Os dados, enquanto tais, não têm significado. No entanto, podem ser portadores de informação, nomeadamente "informação codificada". O significado é-lhes atribuído quando estão envolvidos num processo de comunicação de informação por um remetente e de geração e informação pelo destinatário, ou seja, quando se tornam objeto de comunicação. Esta comunicação pode ocorrer entre humanos, mas também entre humanos e máquinas ou entre máquinas.

Aprofundando-se ao objeto deste estudo, neste trabalho abordar-se-ão os dados pessoais. De acordo com o art. 5º, I, da Lei Geral de Proteção de Dados Pessoais ("LGPD")<sup>4</sup> brasileira, dado pessoal é qualquer "informação relacionada a pessoa natural identificada ou identificável", ou seja, qualquer informação sobre uma pessoa que faça com que seja possível sua identificação. Dados pessoais podem ser ainda mais delicados quando se fala sobre dados pessoais sensíveis, que, nos termos do art. 5º, II, da mesma lei, seriam definidos como:

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou

---

<sup>1</sup> HENRIQUES, Isabella et al, 2021, p.379.

<sup>2</sup> FERNANDES, Elora, 2021, p. 200.

<sup>3</sup> HOFFMAN-RIEM, Wolfgang, 2018, p. 16.

<sup>4</sup> Lei nº 13.709, de 14 de agosto de 2018. Disponível em

<[http://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm)>

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dados pessoais são tratados por organizações massivamente, instantaneamente e diariamente. Corporações do mundo inteiro personificam produtos e serviços além de microsegmentarem seu marketing com base no tratamento de dados pessoais<sup>5</sup>. O setor público também utiliza dados pessoais para fins de segurança e monitoramento<sup>6</sup>. Tratar dados pessoais significa, ainda nos termos da LGPD, em seu art. 5º, X:

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

Nesse sentido, pessoas que são titulares de dados pessoais, ou seja, “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”, conforme preceitua o art. 5º, V, da LGPD, necessitam fornecê-los para que possam executar diversas ações na sociedade, pois a cultura digital dominou completamente as relações sociais e negociais<sup>7</sup>. Desde a assinatura de uma revista, a contratação de um cartão de crédito em uma instituição bancária e até a assinatura de um serviço de *streaming* ou cadastramento em uma rede social, dados pessoais são fornecidos para que a utilização dos serviços pretendidos seja alcançada.

Devido à importância que dados pessoais possuem no mundo hoje em dia, a sua característica como direito fundamental pode ser considerada como implícita ao art. 5.º, XII, da Constituição Federal de 1988<sup>89</sup>. Além disso, no momento em que este trabalho está sendo elaborado, aguarda sanção do Congresso Nacional o texto da Proposta de Emenda à Constituição (PEC) 17/2019, que tornou a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental. Ainda, o próprio STF, ao julgar a ADI 6387, considerou a proteção aos dados pessoais como um direito fundamental, como descreve<sup>10</sup>:

---

<sup>5</sup> HENRIQUES, Isabella et al, 2021, p.379.

<sup>6</sup> Idem.

<sup>7</sup> Idem.

<sup>8</sup> 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: (...)

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

<sup>9</sup> SARLET, Ingo Wolfgang, 2021, p. 90.

<sup>10</sup> Idem.

(...) o julgamento, pelo Plenário do STF, em 07.05.2020, que confirmou o deferimento, em sede de decisão monocrática proferida em 17.04.2020, pela relatora da ADIn 6387, Ministra Rosa Weber, de medida liminar suspendendo a eficácia da Medida Provisória n.º 954, que determinava às empresas de telefonia a fornecer ao IBGE os nomes, endereços e telefones de mais de cem milhões de brasileiros, mediante o argumento de que tal medida representaria uma restrição constitucionalmente ilegítima dos direitos à privacidade, intimidade e sigilo dos dados pessoais, porquanto inconsistente com as exigências da proporcionalidade e razoabilidade<sup>50</sup>. De acordo com a decisão, o direito fundamental à proteção de dados pessoais representa direito autônomo e com âmbito de proteção distinto ao do direito à privacidade.

Ressalta-se, nesse viés, que a ideia de proteção aos dados pessoais não é necessariamente focada em proteger os dados em si num sentido material, mas em proteger as pessoas titulares dos dados pessoais<sup>11</sup>.

A relevância que é dada à proteção aos dados pessoais está intimamente ligada ao conceito de privacidade. Inicialmente, privacidade era considerado “o direito de ser deixado só/em paz”<sup>12</sup>, mas, como preceitua Danilo Doneda, o que se entende por privacidade muda de acordo com o contexto e o tempo em que o tema é discutido. Assim, privacidade seria “uma noção cultural induzida no curso do tempo por condicionantes sociais, políticas e econômicas”<sup>13</sup>. Nesse sentido, com uma visão contemporânea sobre o tópico, traz-se a perspectiva de Stefano Rodotà<sup>14</sup>.

Assim, a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o Direito de manter o controle sobre as próprias informações.

Devido às mudanças nas relações sociais, o direito de manter controle sobre as próprias informações vem sendo preceituado em diversas legislações sobre proteção de dados pessoais ao redor do mundo. Na Lei Geral de Proteção de Dados brasileira, este direito é considerado um dos fundamentos da proteção aos dados pessoais no art. 2º, II, e é positivado a partir do exercício dos direitos do titular de dados pessoais encontrado nos incisos de seu artigo 18 (I - confirmação da existência de tratamento; II - acesso aos dados; III - correção dos dados; IV - anonimização; V - portabilidade; VI - eliminação; VII - informações de compartilhamento; VIII - informações sobre o não fornecimento de consentimento; e IX - revogação do consentimento). A privacidade em relação aos dados pessoais no contexto digital está diretamente conectada ao princípio da autodeterminação informativa, que seria “o

---

<sup>11</sup> HENRIQUES, Isabella et al, 2021, p. 380.

<sup>12</sup> WARREN, Samuel D.; BRANDEIS, Louis D., 1890 apud BIONI, Bruno Ricardo, 2019, p. 125.

<sup>13</sup> DONEDA, 2006, p. 114

<sup>14</sup> RODOTÁ, Stefano, 2008, p. 92.

direito de cada indivíduo poder controlar e determinar (ainda não de modo absoluto) o acesso e o uso de seus dados pessoais”<sup>15</sup>.

A autodeterminação informativa apresenta, dessa forma, uma conexão indissociável com a noção de dignidade<sup>16</sup>, pois garante autonomia para que o titular possa decidir sobre a utilização de seus dados pessoais. Mas não só, visa garantir que o titular saiba o que está acontecendo com as suas informações pessoais, o que encontra consonância com os princípios da finalidade e da transparência descritos nos incisos I e VI do art. 6º da LGPD:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(...)

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (...)

No entanto, quando se fala sobre crianças, em especial no ambiente digital, alguns cuidados especiais devem ser tomados, pois é um grupo em que sua vulnerabilidade é considerada um estado *a priori*<sup>17</sup>. Na sociedade da informação, sua hipervulnerabilidade está relacionada às etapas de seu desenvolvimento e alguns aspectos circunstanciais<sup>18</sup>, pois podem não conseguir compreender as dinâmicas complexas de causa e consequência que estão atreladas ao meio digital, mesmo que se apresentem habilidosos na utilização de tecnologias de informação e comunicação, já que são menos conscientes dos modelos de tecnologia e ameaças quanto ao processamento de seus dados<sup>19</sup>.

Essa vulnerabilidade é agravada por algumas condições deste público, como<sup>20</sup>:

(i) essas pessoas não possuem as mesmas experiências, condições e capacidades de adultos em razão de características físicas, cognitivas, motivacionais e sociais; (ii) o controle dessas características está fora do seu alcance e as crianças também podem não reconhecer sua vulnerabilidade; e (iii) esse contexto as deixa suscetíveis a danos que podem não atingir o público adulto.

---

<sup>15</sup> SARLET, Ingo Wolfgang, 2021, p. 76.

<sup>16</sup> Idem, p. 85 e 86.

<sup>17</sup> MARQUES; MIRAGEM, 2014, p. 131.

<sup>18</sup> EBERLIN, Fernando B. von T., 2020, p. 170.

<sup>19</sup> HENRIQUES, Isabella et al, 2021, p. 381.

<sup>20</sup> EBERLIN, Fernando B. von T., 2020, p. 165 apud Brenkert 1998, p. 13.

Vale ressaltar que os aspectos relacionados à vulnerabilidade de crianças e adolescentes serão diferentes a depender da fase de desenvolvimento que estão enfrentando na vida. Ainda<sup>21</sup>:

(...) por exemplo, explicam que as crianças de 03 a 07 anos possuem uma orientação egocêntrica e não compreendem pontos de vista diferentes, razão pela qual podem não distinguir as motivações persuasivas de uma publicidade. A impossibilidade de identificar uma mensagem como publicidade aumenta a vulnerabilidade dos consumidores de um modo geral, tanto que o CDC positiva os princípios da identificação da oferta publicitária<sup>74</sup>. Se as crianças de certa idade possuem uma incapacidade para identificar a publicidade, o fornecedor deveria cessar a mensagem direcionada a esse público ou alterá-la de modo a permitir (se é que isso seja possível) que a criança identifique que se trata de publicidade.

Apenas a partir dos 10-11 anos que crianças começam a entender que a publicidade possui um caráter persuasivo e não apenas informativo, por exemplo. Com menos de 05 anos, crianças apenas enxergam a publicidade como entretenimento<sup>22</sup>.

Já entre o público pré-adolescente, outras características irão impactar sua forma de ver o mundo, como descrito na pesquisa de Batat<sup>23</sup>:

(...) (i) a baixa autoestima em pessoas na puberdade (a partir de 12 ou 13 anos, decorrente de mudanças físicas e da insatisfação com sua aparência em razão das discrepâncias com o que entendem como ideal) é um fator que aumenta a sua vulnerabilidade; (ii) a aquisição de bens de consumo tende a aumentar a autoestima dos adolescentes); (iii) bens de consumo funcionam como símbolos materiais da personalidade e o materialismo é maior em adolescentes com baixa autoestima; (iv) pessoas entre 11 e 15 anos tem hábitos de consumo impulsivos, pois querem adquirir produtos e serviços (como jogos) antes de seus pares; (v) adolescentes possuem uma baixa autoconfiança revelada no fato de serem facilmente influenciados por fatores externos( por exemplo, antes de adquirirem produtos, verificam opiniões na internet e com os seus pares para terem maior segurança na realização da compra); e (vi) adolescentes são completamente dependentes da internet, especialmente quando estão fazendo suas lições de casa, se socializando, se divertindo ou consumindo.

Não à toa a Constituição Federal de 1988 incluiu em seu art. 227, mesmo que em caráter paternalista, a proteção à criança e ao adolescente de forma explícita.

O dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, 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.

---

<sup>21</sup> Idem, p. 168 apud La Ville e Tartas, 2010, p. 25.

<sup>22</sup> idem, p. 169 apud Young, 2010, p. 119.

<sup>23</sup> Idem, p. 169 apud Batat, 2010.



Norma esta que é refletida de maneira infraconstitucional nos seguintes dispositivos do Estatuto da Criança e do Adolescente (ECA ou Lei nº 8.069, de 13 de julho de 1990):

Art. 15. A criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como pessoas humanas em processo de desenvolvimento e como sujeitos de direitos civis, humanos e sociais garantidos na Constituição e nas leis.

Art. 16. O direito à liberdade compreende os seguintes aspectos:

I - ir, vir e estar nos logradouros públicos e espaços comunitários, ressalvadas as restrições legais;

II - opinião e expressão;

III - crença e culto religioso;

IV - brincar, praticar esportes e divertir-se;

V - participar da vida familiar e comunitária, sem discriminação;

VI - participar da vida política, na forma da lei;

VII - buscar refúgio, auxílio e orientação.

Art. 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, idéias e crenças, dos espaços e objetos pessoais.

Art. 18. É dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor. (...)

Art. 71. A criança e o adolescente têm direito à informação, cultura, lazer, esportes, diversões, espetáculos e produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento.

O cuidado especial disposto às crianças e adolescentes é importante devido à quantidade de pessoas deste público que acessam constante e diariamente a *internet*. Pode-se observar, por exemplo, dados da pesquisa TIC Kids Online Brasil 2019, elaborada pelo Comitê Gestor da Internet no Brasil (CGI.br), entre crianças e adolescentes de 9 a 17 anos, 89% teriam acessado a internet nos três meses que antecederam a pesquisa, sendo 95% destes por meio do telefone celular, 38% através de computadores, 43% pela televisão, enquanto 18% teriam utilizado o videogame<sup>24</sup>. Na sociedade da informação é fato que a *internet* é uma ferramenta fundamental para proporcionar às crianças garantia de acesso à informação, formas de expressão e

---

<sup>24</sup> HENRIQUES, Isabella et al, 2021, p. 381.

desenvolvimento de sua personalidade, considerando as atuais formas de interação social que se constroem nas redes<sup>25</sup>.

Assim, a legitimidade de crianças em relação ao direito de proteção aos seus dados pessoais deve ser medida não apenas pelos riscos decorrentes de interferências externas mal intencionadas, mas também no sentido de promover o desenvolvimento de sua autonomia e a criação de processos de decisão autônomos<sup>26</sup>. A privacidade se mostra, nessa seara, fundamental para garantir a proteção de crianças e adolescentes num sentido geral e para assegurar-lhes um pleno desenvolvimento social, cognitivo e biológico neste momento de estabelecimento de perspectivas críticas acerca de seus contextos e de criação de vínculos sociais e culturais com a sociedade e o entorno<sup>27</sup>.

Nesse sentido<sup>28</sup>, em relação ao tratamento dados de pessoais do público infantojuvenil, pode-se inferir que

O uso dos dados pessoais, com efeito, é capaz de impactar o próprio desenvolvimento da personalidade, na medida em que podem identificá-la, manipulá-la e, até mesmo, estigmatizá-la, além de ganharem especial relevância em um contexto de crescente desenvolvimento da tecnologia.”

Por isso, a LGPD trouxe hipóteses específicas em que esse tratamento pode ser realizado, conforme disposto em seu art. 14, *caput*, que assegura que o tratamento de dados pessoais de crianças e adolescentes deve ser executado sempre em seu melhor interesse, enquanto o § 1º dispõe que o tratamento de dados pessoais especificamente de crianças deve ser efetuado com o consentimento específico dado por pelo menos um dos pais ou responsável legal:

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.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem

---

<sup>25</sup> EBERLIN, Fernando B. von T., 2020, p. 165 apud DONEDA e ROSSINI, 2014, p. 39.

<sup>26</sup> EBERLIN, Fernando B. von T., 2020, p. 128.

<sup>27</sup> HENRIQUES, Isabella et al, 2021, p. 384.

<sup>28</sup> Idem, p. 392.

armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 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.”

Nesse viés, o melhor interesse visaria “proteger a pessoa incapaz, preservando a sua autonomia progressiva e garantindo o desenvolvimento saudável”<sup>29</sup>. Entende-se, portanto, que o melhor interesse no tratamento de dados de crianças e adolescentes seria alcançado<sup>30</sup>:

(...) somente por meio de práticas que promovam e protejam seus direitos previstos no sistema jurídico nacional e internacional com absoluta prioridade, abstendo-se de práticas violadoras e exploratórias da vulnerabilidade infantojuvenil, inclusive as comerciais.

No mesmo sentido, também em relação ao consentimento<sup>31</sup>:

Será considerado nulo de pleno direito o contrato, mesmo que realizado com consentimento<sup>33</sup> parental – específico e em destaque, tal qual previsto no art. 14, § 1.º, da LGPD –, para o tratamento de dados pessoais de crianças e adolescentes, que não atenda ao melhor interesse das próprias crianças e adolescentes envolvidos<sup>34</sup>

Ressalta-se que o consentimento é apenas uma das possíveis bases legais para que se realize o tratamento de dados pessoais de crianças e adolescentes. No próximo tópico, estudar-se-á com maior profundidade o que seriam essas bases legais.

---

<sup>29</sup> Idem, p. 157 apud DENSA, 2018, p. 42.

<sup>30</sup> HENRIQUES, Isabella et al, 2021, p. 394.

<sup>31</sup> Idem.

## **1.2. Bases legais para o tratamento de dados pessoais de crianças e adolescentes e estudo sobre melhor interesse**

A LGPD definiu em seu art. 6º uma série de princípios norteadores, além da boa-fé, que devem ser observados pelas pessoas físicas e jurídicas na realização do tratamento de dados pessoais. São eles:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Para que esses princípios sejam garantidos, a norma preceituou nos artigos 7º, 11 e 14 (com algumas exceções que estão dispostas no art. 4º da lei, que não será foco de estudo) hipóteses chamadas de bases legais em que o tratamento de dados pessoais pode ser fundamentado. Considera-se que o rol presente nesses artigos é

taxativo, mas que algumas hipóteses podem ser mais abertas a diferentes graus de subjetividade<sup>32</sup>.

No art. 7º, que dispõe sobre tratamento de dados pessoais de forma geral, definiu-se que o este apenas poderá ser realizado nas seguintes hipóteses: I - fornecimento de consentimento do titular; II - cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública para o tratamento e uso compartilhado necessários à execução de políticas públicas; IV - estudo por órgãos de pesquisa garantida a anonimização dos dados sempre que possível; V - execução de contrato ou de procedimento preliminares; VI - exercício regular de direitos em processo judicial, administrativo ou arbitral; VII - proteção da vida ou incolumidade física; VIII - tutela da saúde em procedimento realizado por profissionais de saúde exclusivamente; IX - legítimo interesse do controlador; e X - proteção do crédito.

Em relação aos dados sensíveis, que possuem suas bases legais de tratamento definidas no artigo 11, a regra geral é a do consentimento (inciso I), mas caso este não seja possível de ser alcançado, funcionarão as bases de, nos termos do inciso II: a) cumprimento de obrigação legal ou regulatória; b) pela administração pública para o tratamento e uso compartilhado necessários à execução de políticas públicas; c) estudo por órgãos de pesquisa garantida a anonimização dos dados sempre que possível; d) exercício regular de direitos em processo judicial, administrativo ou arbitral; e) proteção da vida ou incolumidade física; f) tutela da saúde em procedimento realizado por profissionais de saúde exclusivamente; e g) garantia de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

E, por fim, em relação ao tratamento de dados de crianças, o já citado artigo 14 definiu em seu parágrafo 1º que este deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal, tratamento semelhante ao atribuído aos dados sensíveis. Dessa forma, por se tratarem de dados sensíveis, as hipóteses do art. 11, II, da LGPD, também caberão<sup>33</sup>.

Diante dessa similitude de condições, é possível que se entenda que as outras hipóteses que dispõem sobre o tratamento de dados pessoais sensíveis, previstas no inciso II do art. 11 da LGPD – que não a do consentimento, que possui previsão específica no art. 14, § 1.º –, são válidas também para o tratamento de quaisquer dados pessoais de crianças e adolescentes, mesmo que não sejam considerados sensíveis nos termos da definição do art. 5.º, II, da LGPD, e contanto que haja observância ao melhor

---

<sup>32</sup> VIOLA, Mario e TEFFÉ, Chiara Spadaccini de, 2021, p. 236.

<sup>33</sup> HENRIQUES, Isabella et al, 2021, p. 397-398.

interesse dessas pessoas. Isso porque, no referido dispositivo, o legislador aumentou a proteção dos dados pessoais, por entender que dados pessoais sensíveis merecem maior cuidado, tal qual a criança e o adolescente por suas inerentes características.

Trazendo foco ao objeto do estudo - dados pessoais de crianças e adolescentes -, faz-se necessário algumas ponderações. O objetivo do consentimento fornecido pelos pais seria de garantir que seus dados pessoais não sejam tratados ou processados sem o devido consentimento de seus responsáveis e não de privá-los à utilização de ferramentas digitais<sup>34</sup>.

A LGPD considerou as crianças (pessoas de até 12 anos incompletos) como absolutamente incapazes de exercer o consentimento em relação ao tratamento de seus dados pessoais, de modo que este deve ser consentido por um dos pais ou responsável legal. Em relação aos adolescentes, que são incluídos no caput do artigo 14 no que tange a assertiva que determina que o tratamento de seus dados pessoais também será realizado em seu melhor interesse, foram deliberadamente excluídos do § 1º<sup>35</sup>:

E o que está por trás disso é justamente essa percepção de que deve ser considerada a autonomia do adolescente, cuja predominância é diretamente proporcional ao desenvolvimento de suas capacidades para assumir os encargos de sua vida na rede e fora dela a partir de uma atuação dialógica dos pais.

A situação foi definida de tal maneira para que seja refletida a realidade que ocorre no desenvolvimento de uma pessoa em nossa sociedade. Aos poucos, a depender da idade e do nível de maturidade, adolescentes começam a querer tomar suas próprias decisões e a não mais depender de seus pais ou responsáveis legais. Nesse sentido, sobre a participação dos adultos em relação às decisões nas vidas das pessoas em desenvolvimento<sup>36</sup>:

Tal participação na idade zero é total. São os pais que tomam todas as decisões relativas aos dados pessoais de seus filhos, quando estas dependem do consentimento, como a catalogação de seu crescimento por meio de aplicativos de acompanhamento da gravidez ou de seu cadastro em hospitais, escolas etc. Conforme a criança vai crescendo, ela passa a “sentir junto” com seus pais, manifestando também seus desejos e vontades, que devem ser respeitados dentro do possível. Finalmente, quando ingressam na adolescência, o papel dos pais começa a diminuir: o protagonismo no consentimento passa a ser cada vez mais dos adolescentes

---

<sup>34</sup> Idem.

<sup>35</sup> FERNANDES, Elora e MEDON, Filipe, 2021, p. 4.

<sup>36</sup> Idem.

Assim, desde que o melhor interesse seja preservado, os dados de adolescentes deveriam ser tratados a partir das bases dos art. 7º e 11<sup>37</sup>. Ainda sobre o tema<sup>38</sup>:

Ao analisar o art. 12.1 da CNUDC, Archard (2004, p. 65) explica que o direito de as crianças expressarem suas próprias visões depende da existência de uma capacidade madura, no sentido de formar os próprios pontos de vista. Nesse sentido, tal dispositivo não pode ser aplicado a todas as crianças. O autor, em seus estudos, não apontou uma faixa etária específica, mas sugere que há três tipos de crianças no âmbito da CNUDC, que são as muito jovens (de 0 a 06 anos), as crianças propriamente ditas (entre 06 e 12 anos) e as pessoas jovens (entre 12 e 18 anos). Enquanto pertencentes às duas primeiras categorias, claramente, não sejam capazes de formar opiniões próprias; aquelas consideradas jovens (12 a 18 anos), provavelmente tenham essa capacidade (ARCHARD, 2004, p. 65). Seguindo-se essa linha, pode-se afirmar que as crianças pertencentes à faixa etária entre 06 e 12 anos podem ser consideradas portadoras de opiniões próprias, obviamente, dependendo do nível de maturidade e da complexidade da situação à qual cada uma está exposta.

Refletindo esta perspectiva no ambiente digital<sup>39</sup>:

No ambiente digital, normalmente, a participação está associada ao direito da criança utilizar os meios de socialização, interação, divertimento e aprendizagem disponíveis, construindo, pelas suas próprias escolhas, os ambientes culturais, os círculos de amizades e, conseqüentemente, a sua socialização.<sup>31</sup> Nesse aspecto, todos os que exercem influências no desenvolvimento das crianças (pais, professores e familiares) são uma espécie de espelho para a socialização de cada uma delas, e devem contribuir para um estabelecimento equilibrado de seus próprios relacionamentos.<sup>32</sup>

Em vista que o consentimento será utilizado como legitimação para que terceiros utilizem dados pessoais de um titular como forma de manifestação de seus direitos de personalidade, este deve ser interpretado sempre na perspectiva mais restritiva. O agente que o recebeu não poderá utilizá-lo para outras finalidades que não as expressas e devidamente reconhecidas pelo titular, de modo que cumpra com os princípios da finalidade e da adequação. Ainda, para que o consentimento seja considerado válido e o princípio da transparência seja alcançado, as informações fornecidas ao titular sobre o tratamento de seus dados pessoais devem ser nítidas e inequívocas, devendo o controlador informar qualquer hipótese de mudança de finalidade e podendo o titular revogar o consentimento mediante sua manifestação expressa ou caso discorde das alterações<sup>40</sup>.

---

<sup>37</sup> Idem, p. 7.

<sup>38</sup> EBERLIN, Fernando B. von T., 2020, p. 152 apud Archard, 2004, p. 65.

<sup>39</sup> Idem, p. 153.

<sup>40</sup> VIOLA, Mario e TEFFÉ, Chiara Spadaccini de, 2021, p. 239-241.

Ressalta-se que o consentimento não deve ser a única base legal utilizada para tratamento de dados de crianças, pois a interpretação poderia inviabilizar e até mesmo atrapalhar situações em que seja necessário o tratamento destes dados visando seu melhor interesse<sup>41</sup>:

Desse modo, levando em consideração os princípios estabelecidos na LGPD e em todo o ordenamento jurídico brasileiro, parece ser possível advogar que, para tratar dados de crianças e adolescentes, poderiam ser aplicadas as bases legais previstas nos incisos I a VIII do art. 7º, da LGPD — desde que estejam sempre orientadas pelo melhor interesse. Além disso, deve-se considerar a base legal estabelecida no art. 14, § 3º e, especificamente em relação ao consentimento para tratamento de dados de crianças, deve-se aplicar a regra do art. 14, § 1º. Por fim, quando a hipótese envolver dados sensíveis de crianças e adolescentes, a conjunção será do art. 14 com o art. 11, da mesma normativa. Em todas as situações, no entanto, um Relatório de Impacto à Proteção de Dados Pessoais será essencial para avaliar como o melhor interesse será aplicado em cada caso, o que será delineado na próxima seção.

E, no mesmo sentido<sup>42</sup>:

Isso significa que o tratamento de dados de crianças e adolescentes só pode se dar exclusivamente com base no seu melhor interesse, ou seja, somente por meio de práticas que promovam e protejam seus direitos previstos no sistema jurídico nacional e internacional com absoluta prioridade, abstendo-se de práticas violadoras e exploratórias da vulnerabilidade infantojuvenil, inclusive as comerciais. Será considerado nulo de pleno direito o contrato, mesmo que realizado com consentimento<sup>33</sup> parental – específico e em destaque, tal qual previsto no art. 14, § 1º, da LGPD –, para o tratamento de dados pessoais de crianças e adolescentes, que não atenda ao melhor interesse das próprias crianças e adolescentes envolvidos<sup>34</sup>.

Pois bem, de volta ao trecho do *caput* do artigo 14 da LGPD que dispõe que o tratamento de dados de crianças e adolescentes deverá ser realizado em seu melhor interesse, surgem alguns questionamentos: o que seria esse “melhor interesse”? Como quantificá-lo? Será que os pais ou responsáveis legais são os únicos responsáveis por garanti-lo? Será que os pais ou responsáveis legais podem acabar por tomar decisões que vão contra o melhor interesse das crianças e adolescentes que estão sob sua responsabilidade?

Em uma interpretação mais abrangente, pode-se considerar que o conceito de melhor interesse estaria abarcado no Estatuto da Criança e do Adolescente e na Convenção sobre os Direitos da Criança (CNUDC) que foi adotada pela Assembleia Geral da ONU em 20 de novembro de 1989. Assim<sup>43</sup>:

O melhor interesse é o princípio que orienta o sopesamento dos direitos de provisão, participação e proteção das crianças,<sup>45</sup> o que tem sido muito discutido nas questões referentes à adoção (Especialmente internacional), ao

---

<sup>41</sup> FERNANDES, Elora e MEDON, Filipe, 2021, p. 11.

<sup>42</sup> HENRIQUES, Isabella et al, 2021, p.394.

<sup>43</sup> EBERLIN, Fernando B. von T., 2020, p. 157.



reconhecimento de paternidade, à guarda e à visitação. Contudo, a sua aplicação não se restringe a essas hipóteses, devendo o princípio ser utilizado em todas as situações nas quais os interesses da criança estejam envolvidos, inclusive em questões referentes ao ambiente digital.

Ainda, aprofundando-se na interpretação do tema e em paralelo ao já exposto<sup>44</sup>:

O Comitê sobre os Direitos da Criança, que tem como uma de suas funções a interpretação da Convenção, em seu Comentário Geral nº 14, interpretou o art. 3, 1, da normativa, que trata justamente sobre o melhor interesse. Segundo o Comitê, este princípio visa a assegurar a fruição plena e efetiva de todos os direitos reconhecidos na Convenção, bem como o desenvolvimento global da criança, de modo a garantir sua integridade física, psicológica, moral e espiritual e a promover sua dignidade. Trata-se de conceito complexo, que, preferencialmente, deve ser analisado caso a caso. Contudo, nas decisões coletivas, como as que emanam do art. 14, da LGPD, o Comitê entende que o melhor interesse deve ser avaliado e determinado à luz das circunstâncias do grupo específico ou das crianças em geral.

Por isso, o melhor interesse deve ser compreendido como um direito fundamental às crianças e adolescentes<sup>45</sup> e uma regra de interpretação para que atenda de forma objetiva a garantia dos direitos fundamentais. Sendo assim, no maior grau para preservação da dignidade da pessoa humana da criança.

Ou seja, sempre que houver a necessidade de tomada de decisão que afete uma criança ou um grupo de crianças deve ser escolhido o lado que satisfaça o que de fato será considerado o melhor interesse da criança em uma perspectiva objetiva. Para isso, sempre que houver um conflito de interesses ou impossibilidade de atendimento a direitos fundamentais colidentes será necessário um balanceamento para que seja garantida a primazia do melhor interesse, para que se procure buscar a garantia do interesse mais favorável à dignidade da criança de forma absoluta<sup>46</sup>.

Por se tratar de um termo relativamente amplo, surgem algumas dificuldades de aplicação, pois sua consolidação estará associada ao contexto social de vivência da criança e, no geral, se referirá ao melhor interesse *individual* de uma criança<sup>47</sup>. Por isso, para garantia deste preceito no contexto digital será necessário um processo cujo entendimento do tipo de mídia que crianças e adolescentes utilizam e a finalidade dessa utilização (entretenimento, educação, socialização) seja o primeiro passo para que pais e educadores não comprometam os direitos de acesso, informação, educação e proteção de seus filhos. Para isso, os responsáveis precisam conhecer

---

<sup>44</sup> FERNANDES, Elora e MEDON, Filipe, 2021, p. 8.

<sup>45</sup> Idem.

<sup>46</sup> HENRIQUES, Isabella et al, 2021, p.389.

<sup>47</sup> EBERLIN, Fernando B. von T., 2020, p. 157 apud JAMES; JAMES, 2004, p. 83.

os impactos e consequências possíveis da utilização de mídias digitais para que possam entender os benefícios e riscos associados à sua utilização<sup>48</sup>.

Assim, entende-se que o melhor interesse deve ser tratado casuisticamente<sup>49</sup>:

Segundo Tânia da Silva Pereira, “a aplicação do princípio do Best Interest permanece como um padrão, considerando, sobretudo, as necessidades da criança em detrimento dos interesses de seus pais, devendo realizar-se sempre uma análise do caso concreto”.<sup>465</sup> Portanto, é o caso concreto que estabelecerá o conteúdo do princípio, mas a diretriz é sempre no sentido de se buscar preservar o bem-estar da criança, de forma a proporcionar-lhe um crescimento biopsíquico saudável e tutelar adequadamente sua personalidade. Por isso, casuisticamente, é necessário elencar os elementos mais relevantes, determinar seu conteúdo concreto e ponderar sua importância em relação aos demais dados, a fim de se aquilatar os procedimentos com vistas a assegurar a implementação das garantias legais.<sup>466</sup>

Nesse viés, adentra-se no debate envolvendo casos em que os próprios pais falham em cumprir com o princípio do melhor interesse e podem ser os responsáveis por causar danos decorrentes do controle de acesso demasiado e da exposição excessiva de dados pessoais de seus filhos, que serão tratados no próximo capítulo.

## **2. Limites e mecanismos de controle no meio digital exercidos pelos pais e responsáveis legais em relação aos dados pessoais de seus filhos**

### **2.1. Nuances envolvendo o controle excessivo de acesso às redes e a superexposição promovidos pelos próprios pais ou responsáveis legais**

Quando se fala sobre limites e fiscalização de crianças e adolescentes que acessam serviços de tecnologia, surgem muitas controvérsias. Os responsáveis deveriam, em tese, sempre buscar basear suas decisões de acordo com o melhor interesse na perspectiva das crianças e adolescentes para que se tente preservar as garantias de seus direitos fundamentais e para que essas escolhas façam sentido com a preservação da saúde mental, emocional e do convívio social dos envolvidos. Assim observa-se a perspectiva jurisprudencial do STJ<sup>50</sup>:

---

<sup>48</sup> EBERLIN, Fernando B. von T., 2020, p. 158.

<sup>49</sup> TEIXEIRA, Ana Carolina Brochado e RETTORE, Anna Cristina de Carvalho, 2021, p. 262-263 apud Tânia da Silva Pereira.

<sup>50</sup> TEIXEIRA, Ana Carolina Brochado e RETTORE, Anna Cristina de Carvalho, 2021, p. 265 apud Tânia da Silva Pereira.

Importa notar, a partir do que expõe o Ministro, que o atendimento ao melhor interesse da criança e do adolescente se presta como vetor hermenêutico não apenas para a interpretação e aplicação de normas jurídicas, como também como orientação para a eleição de medidas concretas para suas vidas. O objetivo, ao fim e ao cabo, é que sejam feitas escolhas que coadunem com a preservação da saúde mental, da estrutura emocional e do convívio social desses indivíduos, alvos de proteção especial destinada pelo ordenamento. O Ministro, em outra oportunidade, destacou no mesmo sentido:

1. A proteção integral está intimamente ligada ao princípio do melhor interesse da criança e adolescente, pelo qual, no caso concreto, devem os aplicadores do direito buscar a solução que proporcione o maior benefício possível para o menor. Trata-se de princípio constitucional estabelecido pelo art. 227 da CF, com previsão nos arts. 4º e 100, parágrafo único, II, da Lei n. 8.069/1990, no qual se determina a hermenêutica que deve guiar a interpretação do exegeta.

2. O norte nessa seara deve buscar a máxima efetividade aos direitos fundamentais da criança e do adolescente (...).<sup>470</sup>

Porém, isso nem sempre ocorre. Adultos possuem ideias diferentes sobre os perigos do mundo e enxergam assuntos que permeiam a vida em sociedade a partir de suas próprias visões pessoais e, por isso, os cuidados e limitações que garantem aos seus filhos mudam de acordo com quem está sendo responsável por tomar as decisões.

A definição do que é proteção para uns pode significar cerceamento de liberdade para outros. Não é possível controlar de maneira universal a forma como pais e responsáveis legais vão agir em nome da proteção e do desenvolvimento de seus filhos. Defende-se, assim, que responsáveis devem buscar a garantia dos direitos de provisão<sup>51</sup>:

Os direitos de provisão são aqueles que garantem à criança o acesso a meios para o seu desenvolvimento. Pode-se incluir aqui o direito à vida, à provisão de alimentos, à educação, a bens materiais e quaisquer outros elementos que sejam necessários à infância. Na sociedade da informação, os direitos de provisão podem ser materializados com a viabilização do acesso das crianças ao ambiente digital, para que possam utilizar as ferramentas disponíveis para exercer seus direitos de participação (como aprender, se entreter e se socializar).<sup>24</sup>

No entanto, apesar de existirem diversos mecanismos e balizas legais de fonte, como o próprio Estatuto da Criança e do Adolescente, o assunto é delicado pois os responsáveis muitas vezes possuem dificuldade em enxergar seus excessos de criação. Nesse sentido, para fins de delineamento destes direitos, colaciona-se algumas das diretrizes do ECA que descrevem os direitos fundamentais das crianças e adolescentes:

---

<sup>51</sup> EBERLIN, Fernando B. von T., 2020, p. 150.

Art. 3º A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.

Parágrafo único. Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem. (incluído pela Lei nº 13.257, de 2016)

Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.

Parágrafo único. A garantia de prioridade compreende:

- a) primazia de receber proteção e socorro em quaisquer circunstâncias;
- b) precedência de atendimento nos serviços públicos ou de relevância pública;
- c) preferência na formulação e na execução das políticas sociais públicas;
- d) destinação privilegiada de recursos públicos nas áreas relacionadas com a proteção à infância e à juventude.

Art. 5º Nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais.

Art. 6º Na interpretação desta Lei levar-se-ão em conta os fins sociais a que ela se dirige, as exigências do bem comum, os direitos e deveres individuais e coletivos, e a condição peculiar da criança e do adolescente como pessoas em desenvolvimento.

Art. 7º A criança e o adolescente têm direito a proteção à vida e à saúde, mediante a efetivação de políticas sociais públicas que permitam o nascimento e o desenvolvimento sadio e harmonioso, em condições dignas de existência.

Assim, na medida em que faz parte do processo de desenvolvimento das crianças a redução do domínio dos pais, muitos jovens também buscam ambientes livres da presença de adultos<sup>52</sup>. No contexto digital, para tentar garantir a efetivação dos direitos acima descritos, responsáveis podem acabar por agir com excesso de cautela. A dificuldade que surge nesse espectro diz respeito ao balanceamento do

---

<sup>52</sup> EBERLIN, Fernando B. von T., 2020, p. 129.

princípio do melhor interesse à medida adequada de privacidade que é entendida pelos pais<sup>53</sup>.

Ainda, deve-se considerar que o melhor interesse é um conceito dinâmico. Por isso, colaciona-se o Comentário do Comitê sobre os Direitos da Criança<sup>54</sup>:

Em fevereiro de 2021, o Comitê sobre os Direitos da Criança publicou Comentário sobre a aplicabilidade dos direitos previstos na Convenção ao ambiente digital, no qual o Melhor Interesse da Criança é um princípio geral a guiar condutas, legislações e decisões acerca da interface da criança no ambiente virtual:

“O melhor interesse da criança é um conceito dinâmico que requer uma avaliação adequada ao contexto específico. O ambiente digital não foi originalmente desenvolvido para crianças, mas desempenha um papel significativo na vida das crianças. Estados Partes devem assegurar que, em todas as ações relativas ao fornecimento, regulação, design, gestão e uso do ambiente digital, o melhor interesse de cada criança seja uma consideração primordial.”<sup>486</sup>

Nessa seara, quando se fala sobre as decisões que serão tomadas pelos pais ou responsáveis legais, o art. 29 do Marco Civil da Internet (MCI) ou Lei nº 12.965, de 23 de abril de 2014, dispõe que o usuário possui livre escolha para utilizar o programa de computador para exercício de controle parental de conteúdo entendido por ele como impróprio a seus filhos, desde que respeitando os demais princípios do MCI e do ECA<sup>55</sup>. Na medida em que se analisa os diferentes tipos de realidade de criação de filhos no país, faz-se necessário ressaltar que o que é entendido como "conteúdo impróprio" e perigo nas redes digitais será diferente para cada tipo de família. Sobre os conflitos desse contexto<sup>56</sup>:

Os conflitos nessa área normalmente ocorrem em função dos controles que os pais e educadores exercem em relação ao acesso e à utilização de mídias digitais.<sup>47</sup> A restrição de acesso, já vista anteriormente, pode configurar a privação de direitos de provisão, e o controle excessivo sobre a atividade *on-line* dos filhos (filtros de navegação, ferramentas de rastreamento, verificações sistemáticas de trocas de mensagens, postagens e correspondências de crianças) pode violar alguns direitos de participação e/ou a privacidade.

Assim, um dos desafios à garantia da completude dos direitos de provisão no contexto digital para crianças e adolescentes surge na medida em que os pais se tornam os responsáveis por limitar seu próprio desenvolvimento social e por

---

<sup>53</sup> Idem.

<sup>54</sup> TEIXEIRA, Ana Carolina Brochado e RETTORE, Anna Cristina de Carvalho, 2021, p. 271-272.

<sup>55</sup> idem, p. 135 apud DENSA, 2018, p. 191.

<sup>56</sup> EBERLIN, Fernando B. von T., 2020, p. 157.

excederem os mecanismos de monitoramento. Para isso, são convencidos por estratégias sedutoras de empresas de monitoramento *on-line*<sup>57</sup>:

O *terceiro desafio* está ligado às estratégias sedutoras que as empresas utilizam para tentar convencer os pais a monitorarem seus filhos. De fato, há certo aproveitamento da compreensão da criança, como uma pessoa a ser protegida pelo mundo adulto, para que criem produtos e serviços que corroborem ainda mais com essa visão, resultando em ofertas de mecanismos que facilitam o controle dos pais sobre a atividade de seus filhos. 169 Quando bebês, as crianças são monitoradas por câmeras e babás eletrônicas capazes de medir seus batimentos cardíacos e funções vitais. Quando crescem e se tornam mais independentes, podem ficar sujeitas aos diversos acessórios que possibilitam a localização e rastreamento físico, oferecidos constantemente com a promessa de maior segurança e liberdade para a família. Esses dispositivos, como lembra Simpson (2014, p. 275), enfatizam um aspecto emancipador para as crianças (no sentido de viabilizar sua locomoção de maneira segura, já que os pais terão conhecimento a respeito de sua localização), mas, por outro lado, omitem possíveis restrições que possam decorrer do uso desse dispositivo.

Alguns exemplos de aplicativos nesta linha são o Life360 e o Google Family Link. O aplicativo chamado Life360 permite que toda a família fique conectada entre si, prometendo possibilidades de comunicação, verificação da localização dos demais membros da família e notificação das autoridades, em caso de acidentes ou problemas de segurança (LIFE360, 2018). Simpson (2014, p. 276), ao analisar esse aplicativo, sustenta que as promessas referentes à segurança da família são ilusórias, já que o aplicativo não pode, por si só, efetivamente proteger uma pessoa, mas apenas permitir que um pai, por exemplo, notifique às autoridades de que uma criança não pode ser localizada ou que está em perigo.<sup>170</sup> O Google Family Link, por seu turno, é um aplicativo que permite aos pais monitorar toda a atividade de seus filhos *on-line*, assim como a sua localização, desde que ela esteja com o dispositivo. De acordo com informações constantes do *site* da empresa (GOOGLE, 2018b), o dispositivo permite identificar toda a atividade da criança em um celular, gerenciar os aplicativos que elas baixam e utilizam, além de estimular o uso de aplicativos “recomendados por professores” que os pais podem “adicionar diretamente ao dispositivo da criança”. Além disso, é possível que os pais determinem o tempo de uso de um celular e estabeleçam a hora para dormir, bem como bloqueiem o dispositivo (GOOGLE, 2018b). O Google ainda alerta que a criança “poderá compartilhar informações, como fotos, vídeos, áudios e locais, publicamente e com outras pessoas”, as quais “podem ser indexadas por mecanismos de pesquisa como a Pesquisa Google” (GOOGLE, 2018a).

No entanto, deve-se indagar a real necessidade de proteção das crianças a este nível de controle, pois esses aparelhos trazem apenas a promessa de “paz” em vista que a criança estará “amarrada” ou fiscalizada por aparelhos eletrônicos<sup>58</sup>. Afinal, de fato, a criança que possui estes aplicativos instalados em seu celular está sendo realmente protegida ou apenas monitorada?

---

<sup>57</sup> Idem, p. 132

<sup>58</sup> EBERLIN, Fernando B. von T., 2020, p. 133 apud Marx e Steeves, 2019, p. 217.

Nesse viés, psicólogos acreditam que algum tipo de exposição a riscos seria fundamental para que crianças aprendam a se adaptar<sup>59</sup>, pois é importante que a criança desenvolva a capacidade de lidar com situações de risco por si mesma, vide que monitoramentos excessivos podem prejudicar esse desenvolvimento:

Os riscos, por si só, não são inerentemente ruins para as crianças. Como explica o relatório produzido pela UNICEF (2017, p. 74), psicólogos acreditam que alguma exposição das crianças ao risco é fundamental para que elas aprendam a se adaptar, mas a tolerância em relação ao risco aceitável para elas depende da sociedade, da cultura, das comunidades e das famílias individuais envolvidas. Nessa mesma linha, Staksrud (2013, p. 62) explica que há evidências de que os riscos durante a infância podem ser positivos para o desenvolvimento da criança, uma vez que essa ideia também se aplica aos riscos *on-line*. Para a autora, os riscos *on-line* não representam automaticamente danos à infância, por ser a forma pelo qual a criança sabe lidar com o risco e, a partir disso, constrói uma barreira relativamente segura (STAKSRUD, 2013, p. 58).

Por outro lado, pais e responsáveis legais podem acabar por compartilhar excessivamente os dados pessoais de crianças na internet. Responsáveis muitas vezes não possuem um nível de consciência adequado sobre os meios digitais que os torne capazes de lidar com os perigos deste contexto, não entendendo a importância que deve se ter ao lidar com dados pessoais de crianças e adolescentes. Essa falta de consciência pode ser lesiva e atrapalhar a construção de identidade pessoal de um filho e causar danos à longo prazo, como *bulliying*, *cyberbullying* e restrição em colocações no mercado de trabalho por exposições que podem ser encontradas por empresas, quando na realidade o papel dos pais deveria ser de orientar e proteger<sup>60</sup>.

Assim, surge outra questão envolvendo a proteção de dados de crianças, que está relacionado à exposição excessiva de suas informações pessoais<sup>61</sup>:

O *segundo desafio* relacionado ao tema da proteção de dados e da privacidade de crianças, é a exposição excessiva de suas informações pessoais, que pode dificultar a sua inserção social. Informações médicas, dados sobre crianças que cometem crimes e infrações, dados sobre abusadores de crianças, informações sobre desempenho escolar, processos de adoção e guarda e tantas outras devem ser protegidas,<sup>161</sup> já que a sua exposição descontrolada pode gerar consequências importantes na vida da criança quando adulta, impactando suas possibilidades e comportamento.<sup>162</sup> Também deve haver algum controle sobre as situações de exposição pública de fatos de caráter privado (como vídeos e fotos colocados na internet por terceiros), em que não existe nenhum tipo de interesse público e muito menos intenção da criança de dar publicidade aos fatos.<sup>163</sup>

---

<sup>59</sup> Idem, p. 134.

<sup>60</sup> MEDON, Filipe, 2021, p. 355

<sup>61</sup> EBERLIN, Fernando B. von T., 2020, p. 130.

Este tipo de atitude cria um conflito entre o direito de liberdade de expressão dos pais, o direito-dever dos mesmos de cuidar de seus filhos com base no melhor interesse e o direito à privacidade das crianças<sup>62</sup>. A situação é chamada de *oversharenting*<sup>63</sup>:

Da junção das palavras de língua inglesa *share* (compartilhar) e *parenting* (cuidar, exercer a autoridade parental) vem o neologismo que dá nome a este fenômeno,<sup>14</sup> que consiste, em apertada síntese, “no hábito de pais ou responsáveis legais postarem informações, fotos e dados dos menores que estão sob a sua tutela em aplicações de internet”.<sup>15-16</sup> O termo chegou a ser definido pelo Dicionário Collins como “a prática de um pai/mãe de usar regularmente as mídias sociais para comunicar grande quantidade de informação detalhada acerca de sua criança.”<sup>17</sup> Trata-se, portanto, de exercício disfuncional da liberdade de expressão e da autoridade parental dos genitores, que acabam minando direitos da personalidade de seus filhos nas redes sociais.

Vale trazer os dados de uma pesquisa realizado pela Avast com mais de 500 pais e pais brasileiros em fevereiro de 2020<sup>64</sup>, em que

(...) 33% dos entrevistados informaram já ter publicado uma foto do seu filho menor de idade, sem pedir sua permissão e sem nenhum tipo de restrição que impeça a identificação da criança.

Nesse sentido, levanta-se<sup>65</sup> um importante ponto relacionado ao princípio da autodeterminação informativa da criança.

Essa tensão entre a privacidade da criança, o seu melhor interesse e a liberdade de expressão dos pais pode causar conflitos entre pais e filhos no futuro, podendo-se imaginar um potencial direito de as crianças, na idade adulta, exigirem que seja apagada das redes sociais e demais aplicações de internet toda a informação a seu respeito transmitida e armazenada ao longo da vida (não só pelos pais, mas também por terceiros como o colégio, amigos e familiares), sob o fundamento de que tais dados não foram transmitidos pelo seu titular e a sua manutenção em bases de dados, a contragosto,<sup>168</sup> seria um desrespeito ao princípio da autodeterminação informativa. A UNICEF (2017, p. 92) também aponta que o “*sharenting*” pode interferir no bem-estar da criança a longo prazo, em especial na criação de sua própria identidade e na procura por emprego.

O fenômeno da superexposição de crianças e adolescentes pode repercutir de diversas maneiras negativas nas vidas de crianças e adolescentes e afetar seus direitos de personalidade como a privacidade, a imagem, a honra e a proteção de sua intimidade e seus dados pessoais<sup>66</sup>. Algoritmos predatórios que armazenam padrões de comportamento a partir de dados pessoais fornecidos pelos responsáveis ou pelas próprias crianças podem parecer irrelevantes, mas poderão servir como uma forma

---

<sup>62</sup> Idem, p. 131.

<sup>63</sup> MEDON, Filipe, 2021, p. 354-355.

<sup>64</sup> MEDON, Filipe, 2021, p. 31.

<sup>65</sup> EBERLIN Fernando B. von T., 2020, p. 132.

<sup>66</sup> MEDON, Filipe, 2021, p. 31.



de manipulação das decisões sobre as crianças<sup>67</sup>, o que se agrava em casos de crianças que possuem rastros digitais desde os seus primeiros anos de vida, caso que vem sendo extremamente comum no Brasil, principalmente por influenciadores digitais, que criam perfis nas redes sociais para seus filhos enquanto ainda estão na gestação, compartilhando assim dados sensíveis e de saúde de forma indevida. Dados estes que podem resultar, por exemplo, em um valor mais alto para a contratação de um plano de saúde, visto que qualquer pessoa poderia acessar os dados de saúde da criança que teriam sido compartilhados nas redes sociais.

Os riscos podem ser ainda maiores quando se avalia a questão envolvendo a garantia da integridade física de crianças. Colaciona-se a descrição de um caso do Brasil, em que o vídeo de uma criança de biquíni ultrapassou mais de 400 mil visualizações<sup>68</sup>:

Veja-se, nesse sentido, caso ocorrido no Brasil em que uma mãe que foi surpreendida por sua filha ao descobrir que o vídeo postado pela criança no YouTube em que ela aparecia de biquíni, brincando com uma amiga, ultrapassou a marca de 400 mil visualizações, devido a uma suposta configuração da plataforma que acabaria, segundo pesquisadores de Harvard, indicando o vídeo para pedófilos, que demonstram interesse em vídeos com conteúdo sexual. Os algoritmos da plataforma, compreendendo as preferências dos usuários que assistem a vídeos eróticos, passam a recomendar<sup>41</sup> “vídeos de mulheres mais jovens e, em seguida, para mulheres que posam provocativamente em roupas de criança. Eventualmente, alguns usuários podem receber vídeos de meninas de 5 ou 6 anos usando roupas de banho ou se vestindo.”<sup>42</sup>

Outro caso bem recente que vem ganhando notoriedade no país é o da bebê Alice, de 2 anos, que participou de um comercial para o Banco Itaú contracenando com ninguém menos que a atriz Fernanda Montenegro, mundialmente conhecida. O caso foi abordado de forma ilustrativa e resumida no início do capítulo 1 deste estudo. Basicamente, os pais da criança, que residem com ela em Londres, descobriram que a sua filha de pouca idade conseguia pronunciar palavras diversas com bastante eloquência e decidiram gravar e postar vídeos em que a criança falava algumas “palavras difíceis”.

Os vídeos se tornaram viral rapidamente. Hoje, no momento em que este estudo é realizado, o instagram de sua mãe possui 3,4 (três milhões e quatrocentos mil) seguidores. Com o passar do tempo, começaram a surgir vídeos relacionados à

---

<sup>67</sup> MEDON, Filipe, 2021, p. 358.

<sup>68</sup> Idem, p. 359.

marcas em que a criança falava essas “palavras difíceis” em tom publicitário, de modo a divulgar os produtos dos mais diferentes tipos de empresas.

Porém, após a grande repercussão do comercial com o banco, uma enxurrada de memes surgiu nas redes sociais associando a imagem da criança com qualquer tipo de tema (humor, crítica social, política, religião etc.). A mãe da criança, nesse sentido, gravou uma sequência de vídeos e os disponibilizou em sua conta informando que não teria autorizado a utilização da imagem de sua filha para memes e “não concorda em associar a imagem da Alice com fins políticos ou religiosos, por exemplo”. Assim, reitera que o uso da imagem da menina também não estaria autorizado para empresas e instituições, campanhas e vendas de produtos, com exceção às empresas em que há contrato comercial, que estariam autorizadas a utilizar a imagem de sua filha dentro dos termos dos contratos.

Por fim, solicitou “bom senso” na hora de postar memes sobre a criança. Ora, o mesmo bom senso que foi utilizado para vincular a imagem dela a um dos maiores bancos do mundo e uma das maiores atrizes do país em rede nacional em uma campanha publicitária?

Aqui, cabe um retrocesso à análise do melhor interesse da criança. Ressalta-se que não será analisada a perspectiva econômica da situação. Se a criação de memes tornou-se algo intrínseco à sociedade digital, não seria possível prever que provavelmente a imagem da criança se tornaria um viral? Será que o melhor interesse desta criança vem sendo respeitado ao ser colocada para participar de diferentes tipos de campanhas comerciais? Fato é que este indivíduo, com 2 anos de idade, desconhece os efeitos da repercussão que comerciais deste porte possuem. E, provavelmente, não tem dimensão do quão famosa é.

Agora, esta criança terá seu desenvolvimento totalmente atrelado ao fato de ter sido um meme aos 2 anos de idade. Será que ela vai gostar disso quando crescer e começar a compreender a grandiosidade desta exposição a qual foi submetida? As perguntas aqui delineadas não possuem respostas definidas e foram formuladas para gerar pensamento crítico sobre a situação.

O caso narrado assemelha-se com a história da norte-americana Avery Jackson, que teve seu crescimento e desenvolvimento totalmente atrelado ao fato de ter se entendido como uma pessoa transgênero aos sete anos de idade<sup>69</sup>.

---

<sup>69</sup> TEPEDINO, Gustavo e MEDON, Filipe, 2021, p. 180-181.

Para se ter a dimensão da importância do tema, veja-se a título de exemplo, o caso da transgênero norte-americana Avery Jackson, que foi capa da revista National Geographic aos sete anos de idade ao lado de letras garrafais que diziam “Gender Revolution”, ou “revolução no gênero”. Após ter sido entrevistada pelo programa Profissão Repórter da TV Globo em 2014, a menina voltou a ser procurada pelos repórteres no ano de 2018, quando depois de alguns anos demonstrando publicamente seu orgulho por ser trans, passou a rejeitar o rótulo, não querendo aparecer na reportagem da TV Globo. Segundo a mãe, Debi Jackson, ouvida pela reportagem nos primeiros anos, Avery “se sentiu orgulhosa de representar todos os trans, mas depois as pessoas começaram a dizer: ‘nossa, daqui a 30 anos todo mundo ainda vai lembrar da menina trans na capa da revista’.”<sup>7</sup> Foi então que, segundo a mãe, a filha “começou a pensar que daqui a 30 anos ela não quer ser ‘a menina trans’, ela só quer viver a vida dela. Ela não queria que trans fosse a definição sobre quem é ela para o resto da vida.”<sup>8</sup>

As consequências desse tipo de exposição podem ser ainda maiores quando a criança é exposta a situações vexatórias ou humilhantes. Narra-se, assim, o caso da “Bel para Meninas”<sup>70</sup>:

Durante o período de quarentena, ganhou a mídia o caso “Bel Para Meninas”, relativo ao canal no YouTube de uma criança de 13 anos.<sup>23</sup> Com mais de 7 milhões de inscritos, a mãe da menina Bel registrava o dia a dia das filhas, como tantos outros pais têm feitos em canais semelhantes ao redor do mundo, especialmente no período de quarentena. A repercussão do caso, no entanto, se deu por conta de exposições vexatórias da imagem da criança nos vídeos. Há cenas em que “a mãe faz a filha lamber uma mistura de leite com bacalhau, comer um sabonete como se fosse picolé e quebra um ovo na cabeça da menina.”<sup>24</sup>

O assunto, que já vinha causando polêmica há algum tempo, gerou a *hashtag* #SalveBelParaMeninas, que virou *trending topic* no Twitter, após circular na rede uma série de vídeos em que a menor mostra-se visivelmente constrangida a realizar tais atos vexatórios. A mãe ainda é acusada de infantilizar a menina nos vídeos do canal, que gera renda para toda a família:<sup>25</sup> “só o livro Segredos da Bel para Meninas, lançado em 2016, vendeu mais de 100 000 exemplares.”<sup>26</sup> Não tardou para que o caso chegasse ao Judiciário e os vídeos acabassem sendo retirados do ar durante algum tempo, após decisão judicial. Segundo a reportagem da Revista Veja, após inúmeras denúncias, o Conselho Tutelar fez duas visitas à residência da família e elaborou um parecer para o Ministério Público. O relatório cita as expressões “exposição vexatória e degradante”.<sup>27</sup>

Essa postura por pais e responsáveis legais revela a existência de uma falta de consciência sobre os perigos dos ambientes digitais, pois há irresponsabilidade e negligência no exercício da parentalidade. Dessa forma, os responsáveis que atuam nessa exposição deixam de considerar “a importância de seus papéis no ambiente tecnológico”<sup>71</sup>. Assim, traz-se à tona a essencialidade que a proteção aos dados pessoais de crianças possui para a garantia de um desenvolvimento biopsíquico e social adequado para crianças e adolescentes<sup>72</sup>.

---

<sup>70</sup> Idem, p. 184-185.

<sup>71</sup> Idem.

<sup>72</sup> HENRIQUES, Isabella et al, 2021, p.384-385.

A privacidade e, mais especialmente, a proteção dos dados pessoais – que supõe mais do que a interdição de acesso a informações pessoais, mas sim o acesso condicionado e limitado à vontade do sujeito titular dos dados – são essenciais para a formação da personalidade e, portanto, é fundamental que sejam asseguradas, especialmente no período da infância e da adolescência, ao longo do desenvolvimento social, cognitivo e biológico. A proteção de dados pessoais, na perspectiva da autodeterminação informativa, é indispensável na infância e na adolescência para a configuração de sujeitos plenos, capazes de estabelecer vínculos sociais e culturais com a sociedade e o entorno, e igualmente aptos a desenvolver perspectivas críticas acerca do contexto em que vivem.

A garantia da proteção de dados pessoais de crianças e adolescentes, além de possuir uma relevância relativamente maior em relação aos demais entes da sociedade, é mais complexa porque, enquanto pessoas em estágio peculiar de desenvolvimento biopsíquico e social, crianças e adolescentes estão começando a desenvolver a compreensão da amplitude do tratamento de dados pessoais e a capacidade de tomar as decisões sobre autorizar, ou não, o uso de informações e dados pessoais.

Nesse sentido, importante ressaltar os riscos que a superexposição e o processamento indevido de dados pessoais de crianças e adolescentes podem trazer para o desenvolvimento de um indivíduo deste grupo<sup>73</sup>.

Especificamente com relação aos dados pessoais, Pedro Hartung, Isabella Henriques e Marina Pita destacam os múltiplos impactos e problemas sociais para o bem-estar individual e social que podem advir do processamento de dados de crianças e adolescentes, a saber: “(i) ameaça à integridade física, psíquica e moral por contatos maliciosos e de terceiros; (ii) hiperexposição de dados pessoais e discriminação; (iii) a modulação e manipulação de comportamento; e (iv) a microsegmentação da prática abusiva e ilegal da publicidade infantil”<sup>63</sup> que passa a ser mais direcionada para as crianças a partir dos perfis de consumo gerados pelo tratamento de seus dados coletados.

Ainda, crianças e adolescentes podem ser vítimas de (i) antipatia de seus seguidores ao criar-se uma narrativa em que a criança é “malcriada”, por exemplo; (ii) *bullying* e *cyberbullying* na escola, já que podem se tornar motivo de piada; (iii) riscos envolvendo sua integridade física, pois em muitos casos compartilha-se onde os filhos estudam, gostos e hábitos; e ausência de controle sobre a renda obtida com publicidade eventualmente feita, que pode ser facilmente desviada pelos pais para outros interesses que não o melhor da criança<sup>74</sup>.

Relevante ressaltar que se busca criticar o fenômeno da **superexposição**, pois em determinada medida, algum tipo de exposição em redes sociais pode ser considerado aceitável e até saudável, já que é algo indissociável da sociedade atual. Nesse sentido<sup>75</sup>:

---

<sup>73</sup> MEDON, Filipe, 2021, 363-364.

<sup>74</sup> Idem, p. 365.

<sup>75</sup> TEPEDINO, Gustavo e MEDON, Filipe, 2021, p. 188.

Vale dizer, o compartilhamento pode ser positivo para os pais<sup>32</sup>, à comunidade e também às crianças. Nesse compasso, veja-se, por exemplo, as campanhas públicas no Brasil que divulgam a imagem de crianças rejeitadas para adoção: aqui, entende-se que o compartilhamento das imagens estaria funcionalizado a um bem maior, que é a busca por um lar para a criança a ser adotada. Por esse motivo, parte da doutrina chega a dizer que o fenômeno que se busca combater não seria exatamente o *sharenting*, mas o *over-sharenting*,<sup>33</sup> na medida em que a utilização da palavra *sharenting* poderia carregar a conotação negativa de que toda forma de compartilhamento é ruim, quando, em verdade, o que se busca coibir é o excesso irrefletido e prejudicial. O problema não seria a exposição, mas a superexposição. Dito diversamente, os problemas surgem quando se causam embaraço e riscos para a saúde e a segurança das crianças, que passam a crescer com a noção limitada de privacidade, parecendo-lhes normal que toda a sua vida seja exposta aos olhos do público. Isso contribui, para reforçar a suspeita de que a ideia de privacidade estaria desaparecendo.<sup>34</sup>

Desse modo, tem-se dois problemas encontrados em contextos opostos envolvendo o tratamento de dados pessoais: controle excessivo dos pais em relação às redes sociais e a superexposição em redes sociais promovida pelos próprios pais. Surge a questão: como encontrar um meio termo para a garantia do melhor interesse da criança e do adolescente? Colocando-se essas questões em perspectiva<sup>76</sup>:

Nessa linha, Veronese e Silva colocam os dois lados do problema, que são “assegurar o acesso de crianças e adolescentes ao lazer e à cultura” e, por outro lado, exercer o necessário controle para fazer isso “em consonância com a etapa de maturação física, psicológica e emocional desses seres em desenvolvimento, posto que a inobservância das normas de prevenção acarretará a responsabilização da pessoa física ou jurídica, segundo dispõe o art. 73, do Estatuto.

Assim, sustenta-se que os dois lados da moeda coexistem. Crianças e adolescentes devem ser protegidos contra superexposição, exploração e manipulação, mas precisam ter a possibilidade de estender seus direitos de personalidade para exercer e alcançar o poder de autodeterminação informativa e, conseqüentemente, de autonomia<sup>77</sup>, sem que haja controle e monitoramento excessivo por seus responsáveis. Além disso, importante reforçar que a socialização *on-line* é benéfica para crianças pois auxilia na aquisição de conhecimento e na manutenção de conexões com contatos sociais, o que conseqüentemente favorece na redução do sentimento de solidão e promove responsabilidade social<sup>78</sup>.

Nesse viés, questiona-se até que ponto crianças e adolescentes conseguirão exercer sua autodeterminação informativa e obter controle de suas narrativas previamente elaboradas por seus pais ou responsáveis legais. Seria possível exercer

---

<sup>76</sup> EBERLIN, Fernando B. von T 2020, p. 160 apud VERONESE; SILVIA, 2009, p. 35.

<sup>77</sup> EBERLIN, Fernando B. von T 2020, p. 157 apud BUCKINGHAM, 2012, p. 49.

<sup>78</sup> EBERLIN, Fernando B. von T., 2020, p. 154 apud Betts e Spenser, 2016, p. 20.

o direito de apagar todos os dados e imagens que já foram previamente compartilhados com o consentimento de seus pais? E, na prática, caso esse direito seja exercido, o que de fato mudaria?

Sabe-se que é extremamente difícil remover algo por completo da internet na sociedade digital. É impossível controlar se alguém salvou uma imagem em seu próprio telefone celular ou subiu para uma pasta secreta. E, mesmo que ocorra a remoção por completo, os assuntos e pessoas que “caem na boca do povo” geralmente tendem a não ser esquecidas tão facilmente.

A partir dessa perspectiva, realizar-se-á análise sobre o direito ao esquecimento na perspectiva de crianças e adolescentes com base na temática da superexposição.

## **2.2. – Direito ao esquecimento na perspectiva do tratamento de dados pessoais de crianças e adolescentes**

A partir do momento em que pais e responsáveis legais começam a compartilhar imagens de seus filhos em redes sociais, inicia-se a consolidação do processo de identificação de quem é aquela pessoa pelos algoritmos digitais. Pode-se dizer, assim, via de exemplo, que desde o momento da primeira postagem da imagem de uma criança ou da postagem de uma foto do primeiro ultrassom de um feto vinculada a uma conta em rede social, começarão a ser produzidos rastros digitais desse futuro ser vivo.

Em um raciocínio lógico, se uma mãe ou pai postam a foto de uma criança dizendo que é seu filho com seu nome, esta criança naturalmente se tornou uma pessoa identificável e, por isso, seus dados pessoais já estarão sendo tratados por redes de computadores. É impossível fugir deste processamento de dados pessoais.

Agora, imaginando-se a seguinte situação: aquela criança de 2 anos que participou de um comercial com o banco alcançou os 12 anos de idade tendo sua imagem massivamente compartilhada por seus pais. Ela começa a se incomodar profundamente com a situação e solicita aos pais que apaguem das redes sociais todas as postagens e contas vinculadas à sua pessoa. Num mundo imaginário e sem colocar em perspectiva as questões contratuais com empresas que utilizam sua imagem para promoção de marcas, imagine-se que os pais prontamente aceitaram a

solicitação. Em seguida, solicitam aos provedores de rede que também procedessem com o apagamento dos dados pessoais de sua filha de todos os seus armazenamentos. Será que, mesmo com o auxílio dos responsáveis e com a procedência da exclusão pelos provedores - repita-se, num mundo imaginário -, essa criança conseguiria alcançar o *direito de ser esquecida*? Afinal, o que seria este direito ao esquecimento? É possível garanti-lo às crianças e adolescentes que tiveram seus dados pessoais e imagens compartilhados pelos pais em uma idade em que não poderiam manifestar seu próprio consentimento? Do que adianta “ser esquecido” pelas redes online se pelo menos uma pessoa tiver sua foto salva em seu dispositivo pessoal?

O direito ao esquecimento pode ser interpretado como o direito de ter seus dados pessoais referentes à determinada situação apagados da internet ou não veiculados em mídias de informação. Nesse sentido<sup>79</sup>:

O direito ao esquecimento, ou o direito a ser esquecido<sup>1</sup>, origina-se na proteção da intimidade e da vida privada e tem sido invocado, sobretudo no mundo digital, como direito ao apagamento de dados pessoais no contexto da internet, mas também no contexto da mídia em geral, como direito à não veiculação de informação desprovida de atualidade e relevância para o público, mas ofensiva ao interessado.

Este direito é previsto no Regulamento Geral de Proteção de Dados (RGPD ou Regulamento UE 2016/679 ou GDPR, como é mais conhecido devido à sua nomenclatura em inglês - General Data Protection Regulation) em seu artigo 17. Ele surgiu em 2009 a partir de uma demanda envolvendo o *leading case* de Mario Costeja, que teve negado seu pedido de exclusão da informação sobre a existência de uma dívida antiga que já havia sido paga. Num primeiro momento, seu pedido foi direcionado ao jornal que havia publicado a matéria sobre a dívida, e depois, ao Google, onde pretendia ter os dados pessoais referentes à essa matéria apagados. O caso chegou ao “Tribunal de Justiça da União Europeia, que reconheceu expressamente o direito ao esquecimento”<sup>80</sup>, com base na Diretiva 95/46/CE, que futuramente seria revogada para que este direito fosse contemplado na supracitada GDPR.

Vale esclarecer que, em relação ao Google, o titular pleiteava a aplicação de um direito à desindexação, que é contemplado pelo próprio direito ao esquecimento,

---

<sup>79</sup> CUEVA, Ricardo Villas Bôas, 2020, p. 1122.

<sup>80</sup> Idem, p. 1123.

mas não atinge as publicações em si, mas a eliminação de referências que façam tornar a pessoa identificável. Nesse viés<sup>81</sup>:

O caso envolveu a aplicação de um direito à desindexação, ou seja, a possibilidade de se pleitear a retirada de certos resultados (conteúdos ou páginas) relativos a uma pessoa específica de determinada pesquisa, em razão de o conteúdo apresentado ser prejudicial ao seu convívio em sociedade, expor fato ou característica que não mais se coaduna com a identidade construída pela pessoa ou apresente informação equivocada ou inverídica. A desindexação não atinge a publicação em si, pois não importa em remoção de conteúdo de página na web, mas sim importa na eliminação de referências a partir de pesquisas feitas com base em determinadas palavras-chave.

No Brasil, porém, o direito ao esquecimento não é previsto especificamente em nenhuma norma, seja no Marco Civil da Internet ou na própria Lei Geral de Proteção aos Dados Pessoais, que, pasmem, foi inspirada na GDPR. O artigo 18 da LGPD, em seu IV, apesar de prever os direitos de ‘anonimização’, ‘bloqueio’ ou ‘eliminação’ de dados do titular, não compreende o direito ao esquecimento em sua completude, pois os termos citados carregam outros significados<sup>82</sup>.

A **anonimização** é definida como a “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (art. 5.º, XI, da LGPD). Os dados anonimizados não são considerados dados pessoais, exceto se a anonimização for revertida exclusivamente por meios próprios ou se, com esforços razoáveis, puder ser revertida (art. 12 da LGPD).

Já o **bloqueio** indica a “suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados” (art. 5.º, XIII). Curiosamente, além de ser um direito do titular, oponível ao controlador, o bloqueio é também uma das sanções administrativas aplicáveis pela autoridade nacional (art. 52, V, da LGPD), o que provavelmente exigirá regulamentação que explicita o sentido e o alcance do direito ao bloqueio, que não tem paralelo no direito europeu. Talvez a forma mais próxima seja o direito à limitação do tratamento, previsto no art. 18 do RGPD, que pode ser resumido como o direito à restrição temporária do tratamento ou da utilização dos dados em certas hipóteses especificadas na norma, entre elas a situação em que “o tratamento for ilícito e o titular dos dados se opuser ao pagamento dos dados pessoais e solicitar, em contrapartida, a limitação de sua utilização” (art. 18, 1, b, do RGPD), o que desde logo permite inferir que tal direito não se confunde com o direito ao apagamento de dados pessoais.

A **eliminação**, por seu turno, é a “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado” (art. 5.º, XIV da LGPD). Resta saber, portanto, se o direito à eliminação de dados pessoais previsto na lei brasileira corresponde ao direito ao apagamento de dados pessoais definido no RGPD. Não parece haver semelhança entre os institutos, pois o inciso IV do art. 18 da LGPD alude à “eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei”, enquanto o direito ao apagamento dos dados pessoais “diz respeito unicamente à possibilidade de

---

<sup>81</sup> MARTINS, Guilherme Magalhães, 2021, p. 24.

<sup>82</sup> CUEVA, Ricardo Villas Bôas, 2020, p. 1135-1136.



eliminação de dados nessas circunstâncias, já que os dados pessoais, por evidente, devem sempre ser necessários, adequados e lícitos”.<sup>22</sup> (grifou-se)

Trata-se, então, de um caso grave de omissão legislativa, onde não houve preocupação em garantir mecanismos adequados para alcance do direito ao esquecimento e, conseqüentemente, garantiu-se a prevalência da liberdade de expressão e informação sobre os direitos da personalidade<sup>83</sup>. No entanto, importante ressaltar que a defesa do direito ao esquecimento não deve ser lida como algo absoluto. Não é porque alguém almeja ter apagado informações suas que já foram públicas em algum momento que este desejo deve ser cumprido por mera liberalidade do indivíduo, o assunto envolvendo este tema deve ser analisado casuisticamente. Nesse viés, trazem-se hipóteses para a garantia do direito ao esquecimento<sup>84</sup>.

Para Cíntia Rosa Pereira Lima, o direito ao esquecimento pressupõe que: **a) o fato tenha ocorrido em tempo remoto; b) tal fato não tenha mais utilidade pública ou social; c) não se pretenda alterar a verdade factual; e d) não sejam produzidos efeitos com relação às instituições de cunho jornalístico, literário ou científico**. Assim, um jornal não pode ser condenado a suprimir notícia veiculada no passado, mas um provedor de busca na internet pode ser levado a remover conteúdo ofensivo, desde que presentes os pressupostos supraelencados.<sup>23</sup>

O direito ao esquecimento não pode ser entendido como um direito absoluto. Algumas das limitações à sua aplicação são o interesse público, o direito e a liberdade de informação, o direito à memória e a vedação da censura e a liberdade de expressão. (grifou-se)

Assim, defende-se que, em relação às crianças e adolescentes, além da necessidade de terem mais voz sobre como seus dados e sua imagem estão sendo utilizados por seus responsáveis, o direito ao esquecimento seria um mecanismo útil para garantia do direito à autodeterminação informativa, pois seria uma maneira do indivíduo de “recuperar o controle sobre os fatos e dados que dizem respeito” à sua vida. Defende-se, assim<sup>85</sup>:

Nessa linha, aduz-se que os pais atuam a um só tempo como os *gatekeepers* e os *gate openers* dos dados dos filhos, na terminologia utilizada por Stacey Steinberg<sup>62</sup> isto é, a eles, em decorrência do exercício da autoridade parental, é dado o poder de decisão sobre as questões de privacidade dos filhos, incubindo a supervisão e o controle, além do próprio consentimento, que deles se exige por força do §1º do artigo 14 da LGPD.<sup>63</sup> Mas ao mesmo tempo, os pais também franqueiam o acesso aos dados que lhes cabe controlar, “abrindo esse portão”, quando divulgam os dados dos filhos. Para tutelar as vítimas dos excessos de tais divulgações, para além de propor maior autonomia para as crianças e adolescentes, que passariam eventualmente a ter suas vozes ouvidas na forma de um poder de veto em face de seus pais, de acordo com seu crescimento e maturidade, Steinberg defende a aplicação do direito ao esquecimento como forma de recuperar o

---

<sup>83</sup> Idem, p. 1139-1140.

<sup>84</sup> Idem, p. 1136.

<sup>85</sup> TEPEDINO, Gustavo e MEDON, Filipe, 2021, p. 192-193.

controle sobre os fatos e dados que dizem respeito à vida daquela pessoa.<sup>64</sup> Em tal perspectiva, tem-se sustentado a atribuição do direito ao esquecimento em nome da autodeterminação informativa.<sup>54</sup>

E, por isso, para a garantia da funcionalização do princípio de que o tratamento de dados pessoais de crianças e adolescentes ser realizado em seu melhor interesse, sustenta-se que o poder exercido pelos pais e responsáveis legais não deve ser absoluto. Há de se ter responsabilidade ao “abrir e fechar” os portões de dados pessoais. Ainda<sup>86</sup>:

Por certo, a autoridade parental não pode ser exercida de modo absoluto, devendo os pais antes funcionalizar o seu exercício ao melhor interesse dos filhos, questionando-se a todo o tempo se a publicação de suas informações na *Internet*, por tenderem à perpetuidade, deve ser efetivamente realizada. Essa perspectiva preventiva associa-se, portanto, à responsabilidade dos próprios titulares da autoridade parental quanto à sua função da formação da personalidade dos filhos. De todo modo, em situações patológicas, ao interessado, que não participou da formulação de sua história de vida tal qual apresentada às redes sociais, há de ser garantida uma última chance de, ao se tornar adulto, tutelar a sua própria privacidade e assumir a gestão de sua identidade pessoal.

Por fim, resgata-se o já citado trecho do art. 227 da Constituição Federal de 1988 que diz que o dever de prover os direitos lá dispostos às crianças e adolescentes será “da família, da sociedade e do Estado”. Apesar de os responsáveis exercerem grande influência sobre como os dados pessoais de seus filhos serão tratados, a culpa sobre erros e excessos não pode cair exclusivamente em cima deles. A sociedade e o Estado devem atuar ativamente na promoção de mecanismos que garantam o acesso digno à internet e à autodeterminação informativa. Ademais, sua atuação deve ser voltada à prevenção de situações como as descritas neste capítulo.

Assim, a partir de agora, o próximo capítulo buscará entender as nuances envolvendo os aspectos e desafios regulatórios relacionados ao tratamento de dados pessoais do grupo infantojuvenil. Para além disso, a utilização da “privacidade por *design*” será avaliada como sendo ou não um mecanismo viável para a busca pelo princípio do melhor interesse.

---

<sup>86</sup> Idem, p. 195.

### **3 – Desafios e perspectivas regulatórias para o tratamento de dados pessoais de crianças e adolescentes: um olhar para a privacidade por design**

#### **3.1. – Perspectivas regulatórias para o tratamento de dados pessoais de crianças e adolescentes**

Delineados os conceitos envolvendo o tratamento de dados pessoais de crianças e adolescentes e expostas algumas das problemáticas que surgem a partir da falta de conscientização existente no contexto digital, parte-se para a análise de perspectivas regulatórias para o alcance do melhor interesse. Afinal, a LGPD é suficiente para garantir a segurança necessária aos dados pessoais de crianças e adolescentes? Seria possível buscar referências no cenário internacional? Há algum tipo de solução que seja vislumbrável para que se evitem problemas maiores no futuro?

As tecnologias existentes que dominam as relações sociais atuais não foram pensadas tendo como base a segurança dos dados pessoais. Basta que se pense um pouco nos exemplos dos aplicativos que são mais comumente utilizados pelas pessoas. Todos são elaborados tendo como foco a escalabilidade (ou seja, de modo que estejam em constante crescimento e aprimoramento), a acessibilidade (ou seja, de modo que alcancem o maior número de indivíduos) e a rentabilidade (ou seja, de modo que todo o investimento realizado na aplicação seja financeiramente rentável e proporcione lucro aos seus desenvolvedores e investidores). Para que seja possível alcançar estes ideais, são necessários a coleta e o processamento massivo de dados pessoais, o que gera um ciclo vicioso permeado por algoritmos que criam estereótipos e prejudicam principalmente os mais vulneráveis<sup>87</sup>.

Nesse sentido, é fato que a internet em si não foi pensada tendo como base o princípio da segurança. Muito menos, a internet e as tecnologias que dela partiram não foram sequer desenhadas considerando pessoas com necessidades especiais e vulnerabilidades, como crianças e adolescentes, que estão na fase de

---

<sup>87</sup> FERNANDES, Elora, 2021. p. 202

desenvolvimento de suas personalidades e de entendimento sobre os riscos que existem no mundo<sup>88</sup>. No mesmo viés<sup>89</sup>:

O processamento de enormes quantidades de dados pessoais através do uso de técnicas de mineração de dados que se seguem a partir deste novo cenário tornou-se um assunto de interesse amplo e atual. Este tratamento de dados afeta todos os usuários da web, mas é de especial importância quando se trata de grupos vulneráveis e principalmente de menores, devido à falta de assertividade e compreensão dos riscos e consequências posteriores ao tratamento dos seus dados pessoais. Na verdade, geralmente nem mesmo os pais entendem a forma pela qual é realizado o tratamento dos dados dos seus filhos.<sup>832</sup>

Assim, o público infantojuvenil, grande utilizador da internet e representante de grande parte do segmento do consumo, se torna alvo fácil de empresas, que desenvolvem suas estratégias de marketing e de negócios a partir da segmentação e da análise dos hábitos de consumo deste grupo e, conseqüentemente, de suas famílias<sup>90</sup>. Cria-se, então, uma falsa ideia de que responsáveis e crianças possuem controle sobre suas próprias decisões e narrativas, em contrapartida que se evita a responsabilização de empresas e algoritmos<sup>91</sup>.

É válido lembrar que crianças e adolescentes necessitam de ambientes em que haja um nível adequado de privacidade interpessoal e que seja possível aprender com erros e acertos para que tenham um desenvolvimento psicossocial pleno. Nesse sentido<sup>92</sup>:

Mas, para além da proteção dos dados de crianças e adolescentes, entendida como uma esfera objetiva, a falta de espaços em que se detém controle da chamada privacidade interpessoal<sup>345</sup> também gera riscos, relacionados ao conteúdo, contato e conduta, descritos acima. Assim, além de a privacidade e a proteção de dados serem um fim em si mesmo, também são meios para a concretização de outros direitos.

O fato de crianças e adolescentes estarem em desenvolvimento demanda um ambiente adequado para erros e acertos, a fim de que possam recomeçar suas vidas sem que tudo o que disseram ou fizeram fique registrado indefinidamente. Eles ainda estão compreendendo quem são, quais são seus gostos, como se diferenciam de suas famílias, quais suas afinidades políticas e sociais e precisam da possibilidade de mudança. A forma como a internet funciona hoje, bem como os modelos de negócios baseados na exploração de dados — e, por isso, de pessoas — torna isso quase impossível, o que faz com que modificar a arquitetura do próprio meio possa ser uma solução eficaz.

---

<sup>88</sup> idem, p. 200

<sup>89</sup> VIOLA, Mario e VARGAS, Vanessa, 2021, p. 456

<sup>90</sup> idem, p. 460.

<sup>91</sup> FERNANDES, Elora, 2021. p. 201.

<sup>92</sup> idem, p. 202-203.

Por isso e pelos demais motivos já apresentados durante todo este estudo, entende-se que as legislações atuais presentes no Brasil não são suficientes para garantir o alcance do princípio da autodeterminação informativa e para resguardar a proteção integral aos dados pessoais de crianças e adolescentes visando seu melhor interesse. Assim, se faz necessário “uma regulamentação da matéria pela Autoridade Nacional de Proteção de Dados (ANPD)”<sup>93</sup>.

Ademais, como já citado anteriormente, não cabe aos pais e aos responsáveis legais todo o peso sobre como lidar com os dados pessoais de seus filhos. Afinal, apesar do consentimento fornecido por estes ser muito importante para diversos aspectos que envolvem a vida das crianças e adolescentes, nem sempre será suficiente ou sequer verificado que realmente tenha partido dos responsáveis. Por isso, defende-se que o consentimento não deve ser a única medida possível para a tomada de decisões em relação ao tratamento de dados pessoais de crianças e adolescentes<sup>94</sup>.

Ainda que se considere que em algumas situações o consentimento parental seja o melhor caminho, especialmente para aquelas situações nas quais a criança ainda não possui o discernimento suficiente para a tomada de decisões, ele não pode ser a única medida possível, e deve ser acompanhada de uma maior conscientização tanto de pais quanto de crianças com relação aos riscos e oportunidades gerados pela utilização da internet, e, também, de mecanismos para assegurar um maior grau de proteção dos dados pessoais no ambiente virtual, como, por exemplo, a mudança nas configurações de privacidade padrão das redes sociais.<sup>878</sup> Além disso, deve ser considerada o que a Convenção sobre os direitos da criança chamou de “evolução de sua capacidade”, devendo ser concedida maior autonomia para as crianças à medida que demonstrem maiores condições e discernimento e que possam tomar decisões que lhes afetem.

Em algumas hipóteses, inclusive, reconhece-se a possibilidade de dispensa do consentimento<sup>95</sup>, como no caso do tratamento de dados de crianças e adolescentes para serviços preventivos e de conscientização ou até em casos de que a saúde e segurança da criança depende de determinado tipo de tratamento que foge da necessidade de aprovação dos responsáveis. Ademais, como já defendido anteriormente, é necessário algum tipo de garantia de privacidade das crianças e adolescentes em relação aos seus pais<sup>96</sup>.

Assim, a ideia de apenas contar com a intervenção dos pais “opõe-se à ideia da participação das crianças no processo de tomada de decisão que lhes diz respeito – uma ideia ancorada na Convenção das Nações Unidas sobre os

---

<sup>93</sup> idem, p. 205.

<sup>94</sup> VIOLA, Mario e VARGAS, Vanessa, 2021, p. 470

<sup>95</sup> idem, p. 471.

<sup>96</sup> idem, p. 474-475.

Direitos da Criança”.<sup>889</sup> Isso porque para os pais consentirem com o processamento dos dados pessoais dos seus filhos teriam de intervir nos espaços privados das crianças, tais como contas de jogos, contas de redes sociais e assim por diante, fazendo com que as crianças pudessem sofrer restrições no acesso à informação, bem como à liberdade de expressão, já que sabendo que seus pais têm acesso ao que acessam e dizem online provavelmente lhes inibiria. Imaginem situações nas quais os filhos buscam informações sobre saúde sexual e métodos contraceptivos, ou ainda quando manifestam opiniões políticas sobre determinado tema. Provavelmente não buscariam tais informações ou manifestariam certa opinião se seus pais estivessem monitorando o que fazem.

Consequentemente, garantir a privacidade das crianças online tem, na maioria dos casos, um impacto positivo no exercício dos outros direitos que acabamos de mencionar, o que significa que as iniciativas nessa direção também devem ter em mente os possíveis conflitos que terão para garantir o pleno exercício desses direitos e ser “consistente com a evolução das capacidades das crianças [e fornecer] orientação apropriada no exercício de seus direitos”<sup>890</sup>. O debate ainda está aberto e não existe uma solução definitiva para a questão. O que é certo é que deve ser dada maior relevância para a capacidade evolutiva da criança sob uma ótica não apenas de proteção contra riscos, mas, também, de empoderamento dessa mesma criança para o exercício de direitos (liberdade de expressão, acesso à informação, privacidade) para assegurar uma maior participação na tomada de decisões que lhe afetem. De qualquer modo, já contar com uma lei geral de proteção de dados que em alguma medida se preocupa com as particularidades de crianças e adolescentes já é um passo enorme, especialmente porque até há alguns anos sequer tínhamos uma lei desse tipo.

Apenas com a finalidade de trazer maior profundidade ao assunto, fala-se também sobre a existência de uma espécie de “hipertrofia do consentimento”<sup>97</sup>.

Em relação à proteção de dados pessoais, o consentimento sempre atuou como uma das principais bases legais para o tratamento de dados. Bioni fala, inclusive, de uma “hipertrofia do consentimento junto ao restante do corpo normativo de proteção de dados pessoais, o que é diagnosticado por um desenvolvimento incompleto dos seus outros ‘membros’ [...]”.<sup>359</sup> No caso de crianças e adolescentes, essa foi a única base legal para a qual a LGPD trouxe, explicitamente, regras específicas, em seu art. 14, §1º (além, claro, de criar aquelas presentes no art. 14, §3º). Nesse sentido, sendo ele um veículo importante da autodeterminação informativa e do controle dos dados pessoais, é preciso discutir seu papel real de concretização de autonomia e proteção de crianças e adolescentes.

Por isso, ao analisar-se a figura do consentimento na sociedade digital a partir de uma perspectiva realista não demora para que se perceba que a validação sobre a manifestação ter sido “livre” é bem difícil de ser avaliada. Na economia atual, muitas vezes não há a opção de recusar o tratamento de dados pessoais em determinadas plataformas, pois o uso de dados pessoais “está intrinsecamente ligado ao modelo de negócio predominante”<sup>98</sup>. Mais que isso, os sistemas e plataformas foram desenhados

---

<sup>97</sup> FERNANDES, Elora, 2021. p. 208.

<sup>98</sup> idem, p. 211

também para agregar estes dados pessoais e estão se aprimorando para cada vez mais coletar dados sensíveis, o que pode resultar em consequências mais graves para pessoas vulneráveis<sup>99</sup>.

Outra situação emblemática é a coleta de dados de diversas pessoas de forma agregada, como ocorre hoje com os artefatos inteligentes conectados à internet (Internet das Coisas). Assistentes virtuais, por exemplo, coletam dados de toda a família de forma conjunta, o que dificulta a individualização dos dados de crianças e adolescentes para uma melhor proteção. Justamente por não serem direcionadas a este público, essas tecnologias acabam não seguindo legislações específicas para a proteção de seus direitos<sup>389</sup> e não utilizam como base legal o consentimento para tratamento de seus dados em específico.

Ao agregar esses dados, as empresas de tecnologia têm ainda não só a possibilidade de tratar dados contextuais da família, como situação socioeconômica, valores familiares e hábitos, mas também os dados biométricos de crianças e adolescentes, como a sua voz. Os dados contextuais são chave para o funcionamento de Inteligência Artificial<sup>390</sup> no modelo de negócios atual, mas isso pode ter consequências graves nas vidas de crianças e adolescentes, caso sejam utilizados para se realizar afirmações falsas, discriminar ou cercear determinado direito.<sup>391</sup> Isso é especialmente grave quando essas assunções são feitas com base em dados de sua família como um todo, o que pode gerar um engessamento social e agravar desigualdades socioeconômicas.

Nesse sentido, para que se alcance um mínimo de proteção em relação aos dados pessoais não só de mas principalmente crianças e adolescentes defende-se que a arquitetura das plataformas digitais e da internet em si deve ser pensada tendo como base a ideia de segurança a esses dados. Ou seja, ao se pensar na construção de uma plataforma, em primeiro lugar deve ser colocado em pauta como funcionarão os mecanismos para proteção aos dados pessoais dela. Assim, é necessário que haja a regulação do design das tecnologias em que se privilegie a governança preventiva de dados<sup>100</sup>. Nesse viés<sup>101</sup>:

Em outras palavras, seria necessário incluir na arquitetura da tecnologia ferramentas e instrumentos de proteção da privacidade. Esses componentes fariam parte do próprio design da tecnologia. Em síntese, a metodologia conhecida como *privacy by design* abrange a ideia “de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviço, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais”.<sup>20</sup>

Para isso, será estudado o conceito da privacidade por design ou, como é mundialmente conhecido em inglês, o *privacy by design (PbD)*.

---

<sup>99</sup> idem, p. 221-222.

<sup>100</sup> idem, p. 207-208.

<sup>101</sup> LEMOS, Ronaldo e BRANCO, Sérgio, 2020, p. 813

### 3.2. – Privacidade por design como a possível solução de um problema estrutural

A ideia de se pensar a privacidade a partir do design não é nova e inclusive está presente em diversas legislações sobre proteção aos dados pessoais no mundo. Este conceito é consolidado na Lei Geral de Proteção aos Dados Pessoais a partir de seu artigo 46:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

A GDPR, na Europa, também incorporou o conceito em seu artigo 25<sup>102</sup>.

Em seu art. 25, o GDPR incorporou o conceito de privacy by design e de privacy by default (que, na tradução oficial para o português, aparecem como “proteção desde a concepção” e “por defeito”):<sup>30</sup>

Artigo 25.º Proteção de dados desde a concepção e por defeito 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. 3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.ºs 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.º.

---

<sup>102</sup> idem, p. 817-818



Nessa perspectiva, entende-se que este ideal preceitua a inclusão de ferramentas e instrumentos de proteção à privacidade como parte do próprio design da plataforma. A relevância desta percepção tem a ver com a influência que o design possui na vida dos seres humanos, pois a forma como algo é desenhado afeta diretamente o comportamento das pessoas e, nesse sentido, “os sinais emitidos pelo design afetam o relacionamento do humano com a tecnologia e também o cálculo de risco elaborado”<sup>103</sup>. Mais que isso, acredita-se que o ser humano é facilmente manipulável pelo design das ferramentas que utiliza e, por isso, existiria uma relação intrínseca entre design e poder. Entretanto, o design também teria o poder de melhorar a vida em sociedade<sup>104</sup>.

Ao se entender que as tecnologias estão geralmente permeadas com valores utilizados por seus desenvolvedores, ou seja, não são neutras, percebe-se que nelas podem existir diversos mecanismos que beneficiam o serviço online em detrimento do titular de dados pessoais ao utilizarem técnicas que visam enganar o usuário final. Mesmo assim, há certa dificuldade em mapear de forma fixa quais técnicas são utilizadas para favorecer empresas. Por isso, estes atributos que visam desorientar os titulares de dados pessoais foram nomeados como “*dark patterns*” (em tradução literal “padrões sombrios”)<sup>105</sup>.

Para fins de exemplificação, os *dark patterns* podem ser classificados a partir de como modificam a arquitetura da escolha do usuário, sejam (i) modificando o espaço de decisão ou (ii) manipulando o fluxo de informações. Abaixo, exemplifica-se a tabela explicativa sobre os atributos das *dark patterns* traduzida por Elora Fernandes<sup>106</sup>.

Padrões sombrios que modificam o espaço de decisão podem ser (i.a) assimétricos, quando geram cargas desiguais nas escolhas disponíveis ao usuário, (i.b) restritivos, quando eliminam certas escolhas que deveriam estar disponíveis para os usuários, (i.c) oferecer tratamento díspar, quando geram desvantagem e tratam grupos de usuários de maneiras diferentes de outros grupos e (i.d) ocultos, quando escondem mecanismos de influência dos usuários. Padrões sombrios que manipulam o fluxo de informações podem (ii.a) ser enganosos, quando induzem a falsas crenças

---

<sup>103</sup> FERNANDES, Elora, 2021. p. 223.

<sup>104</sup> idem, p. 224.

<sup>105</sup> idem, p. 227.

<sup>106</sup> idem, p. 229

nos usuários por meio de declarações falsas, enganosas ou omissas ou *(ii.b)* esconder informações, quando obscurecem ou atrasam a apresentação de informações necessárias aos usuários.

Em contraponto a este tipo de arquitetura nociva ao usuário, foram criados princípios norteadores para o alcance da privacidade por *design*, que foram elaborados a partir do artigo “Privacy by design: the definitive workshop” publicado pela Ph. D Ann Cavoukian. Abaixo, descrevem-se os com tradução interpretativa do autor deste estudo para o português<sup>107</sup>.

O princípio da *(i) Atuação proativa e preventiva, não reativa e remediadora* consiste na antecipação dos eventos que possam afetar a privacidade antes que estes ocorram. Pode ser alcançado por meio da atribuição de responsabilidades concretas para que cada membro da organização que cuida da arquitetura esteja ciente de suas tarefas com relação à privacidade e do desenvolvimento de métodos sistemáticos baseados em indicadores para a detecção precoce de processos e práticas deficientes na garantia da privacidade.

O princípio da *(ii) Privacidade como configuração padrão* consiste no estabelecimento de configuração padrão para que seja fornecido ao usuário utilizador do produto o mais alto nível de privacidade possível. Os dados pessoais devem ser protegidos automaticamente, por padrão, em qualquer sistema a ser desenvolvido. Para isso, algumas medidas devem ser trabalhadas como *(a)* a limitação do uso de dados pessoais à finalidade para os quais foram coletados, *(b)* a restrição de acesso aos dados às partes envolvidas no tratamento de acordo com a necessidade, *(c)* a definição de prazos estritos de retenção com mecanismos operacionais que garantam posterior exclusão e *(d)* a criação de barreiras tecnológicas e procedimentais para a conexão não autorizada de diferentes fontes de dados.

O princípio da *(iii) Privacidade de fato incorporada ao design* consiste na integração da privacidade como um conceito a ser aplicado no desenvolvimento de sistemas desde os estágios de conceito. Para garantia de que a privacidade seja considerada nos estágios iniciais de design, deve-se *(a)* considerá-la como um requisito essencial dentro do ciclo de vida de sistemas e serviços, *(b)* realizar análises de risco e avaliações de impacto da proteção de dados como parte integrante de qualquer nova iniciativa de tratamento de dados e *(c)* documentar todas as decisões

---

<sup>107</sup> CAVOUKIAN, Ann, 2011.

que que forem adotadas.

O princípio da *(iv) Funcionalidade completa: soma positiva, não soma zero* consiste na busca de soluções eficazes e eficientes tanto a nível empresarial quanto de privacidade. Muitas vezes, a privacidade é entendida como sendo adquirida à custa de outras funções, como usabilidade, benefício comercial e funcionalidade. O PbD busca uma abordagem de equilíbrio entre os diferentes interesses, que pode ser trabalhada a partir *(a)* do estabelecimento de canais de comunicação, colaboração e consulta aos diferentes agentes participantes no desenvolvimento de novos produtos, de forma que os interesses divergentes possam ser discutidos e *(b)* a partir da busca de novas soluções de operacionalidade que não ameacem a privacidade.

O princípio da *(v) Segurança de ponta-a-ponta: proteção total do ciclo de vida* consiste na garantia da privacidade dos dados durante todo seu ciclo de vida, ou seja, a integração da privacidade em todas as etapas do processamento de dados (coleta, registro, classificação, conservação, consulta, distribuição, limitação, exclusão) a partir de exaustiva análise caso a caso. Para isso, podem ser utilizadas *(a)* técnicas de pseudonimização, *(b)* classificação e organização das operações de tratamento de dados com base nos perfis os acessam, *(c)* criptografia padrão para que o “estado” dos dados, quando vazados ou roubados, seja ilegível e *(d)* destruição segura e garantida da informação no final do seu ciclo de vida.

O princípio da *(vi) Visibilidade e transparência* consiste na garantia da transparência sobre os processos de tratamento de dados a partir da demonstração da existência da privacidade. A promoção da transparência requer a adoção de medidas como *(a)* a publicização de políticas de privacidade e proteção de dados, *(b)* a elaboração e publicação de cláusulas de informação concisas, claras e compreensíveis que sejam facilmente acessíveis e permitam que os titulares dos dados possam entender a que riscos estão expostos, bem como exercer seus direitos e *(c)* compartilhamento do contato do controlador de dados.

E, por fim, o princípio do *(vii) Respeito à privacidade do usuário* consiste na concepção de projetos centrados no usuário, em que qualquer medida adotada vise a garantia de sua privacidade, antecipando suas necessidades. Para isso, podem ser envolvidas *(a)* a implementação de configurações de privacidade “robustas” por padrão, em que os usuários são informados das consequências sobre o tratamento de seus dados, *(b)* a disponibilização de informações adequadas que conduzam a um consentimento informado, livre, específico e inequívoco, *(c)* a utilização de

mecanismos que permitam aos titulares exercerem seus direitos em matéria de proteção de dados.

Princípios são excelentes pontos de partida para causar reflexão e movimentar mudanças, mas é necessário ir além. Confiar que os agentes que movem a sociedade digital utilizarão apenas princípios no desenvolvimento de seus produtos digitais seria de uma ingenuidade tremenda. Por isso, é fundamental que o Estado possua uma participação mais ativa na promoção da conscientização e da educação digital. Defende-se, inclusive, que a educação digital deveria ser uma disciplina presente nos currículos escolares desde os primeiros anos de vida.

Não só isso, o Estado deve atuar por meio de seus órgãos na regulamentação da privacidade por design para a proteção do tratamento realizado aos dados pessoais de crianças e adolescentes. Esta regulamentação, no entanto, para que faça sentido, deve ser estudada e desenvolvida de acordo com as etapas de desenvolvimento do público infantojuvenil<sup>108</sup>.

Em primeiro lugar, confiar no envolvimento dos pais “contradiz os últimos dados empíricos que mostram que as crianças, em certa medida, estão cientes das ameaças à privacidade e têm as mesmas preocupações com o roubo de identidade e a exploração de dados como adultos.”<sup>884</sup> Além disso, as crianças também devem poder agir de acordo com suas capacidades em evolução, conforme previsto no art. 12 da Convenção sobre os direitos da criança.<sup>885</sup> Isso fica claro em uma pesquisa publicada pelo UNICEF Office of Research – Innocenti, que destaca que “A maioria das crianças mais velhas relatam saber como gerenciar suas configurações de privacidade online, uma indicação fundamental de suas habilidades digitais e de segurança.”<sup>886</sup>

Um grande modelo a ser observado é o da *UK Data Protection Act*, a lei de proteção de dados pessoais do Reino Unido, que determinou que o *Information Commissioner’s Office (ICO)*, a autoridade de proteção de dados pessoais do mesmo país, elaborasse um código de práticas específicas contendo “padrões de design tecnologicamente neutros e adequados às diferentes idades de crianças”<sup>109</sup>.

O principal objetivo do código não é o de proteger crianças do ambiente digital, mas sim de protegê-las dentro dele. Ele apresenta 15 padrões de design cumulativos e interligados para fornecer proteção integrada, permitindo que crianças explorem, aprendam e joguem online de maneira segura. Além disso, todo o código é baseado nos princípios estabelecidos pela Convenção sobre os Direitos da Criança e busca respeitar os direitos e deveres dos pais, assim como a capacidade em desenvolvimento da criança de tomar suas próprias decisões.<sup>421</sup>

(...)

---

<sup>108</sup> VIOLA, Mario e VARGAS, Vanessa, 2021, p. 473.

<sup>109</sup> FERNANDES, Elora, 2021. p. 236-239.

Dentre os padrões estabelecidos pelo código pode-se citar a necessidade de se elaborar avaliações de impacto para a proteção de dados de crianças e adolescentes; o não uso dos dados para finalidades prejudiciais; a determinação de configurações padrão sempre mais protetivas; a vedação a priori do compartilhamento de dados e do profiling, entre outros.

(...)

Ademais, também determina que delimitar uma idade de acesso a um serviço não poderia ser utilizado como pretexto para o não cumprimento das normas previstas. Assim, nos casos em que o serviço não deve ser utilizado por crianças abaixo de certa idade, devem ser tomadas medidas para garantir que os mecanismos de verificação de idade sejam eficazes. Se isso não puder ser feito pela organização, ela deve garantir que as medidas de proteção estejam em vigor para todos os usuários.<sup>426</sup>

(...)

Ressalta-se, ainda, o entendimento da DPC de que as organizações não devem realizar o profiling de crianças, tomar decisões automatizadas em relação a elas ou utilizar seus dados pessoais para fins de publicidade, a menos que possam demonstrar claramente como e por que isso é de seu melhor interesse. A fim de evitar qualquer dúvida, a DPC salienta que não considera que seja de seu melhor interesse anúncios ou sugestões automáticas para outros jogos, serviços, produtos, vídeos etc.<sup>427</sup> Por fim, a regulamentação apresenta diversos padrões de design que podem ser utilizados para concretizar os fundamentos.

Nesse sentido, buscam-se, em primeiro lugar, as considerações acerca dos estágios de desenvolvimento das crianças e adolescentes delineados pela ICO, que podem eventualmente ser utilizados pela ANPD num futuro processo de regulamentação do tema. Para isso, utiliza-se como base a tabela comparativa brilhantemente traduzida e elaborada pelo ITS (Instituto de Tecnologia e Sociedade do Rlo) em parceria com o Instituto Alana<sup>110</sup>.

Em relação à crianças na faixa etária entre 0 e 5 anos, que estão na fase de pré-alfabetização e alfabetização fundamental, recomenda-se a utilização de um design cuja arquitetura seja de alta privacidade por padrão, de modo que sejam incluídos *nudges*<sup>111</sup> que estimulem o bem-estar e seja possível realizar intervalos na utilização da aplicação (a possibilidade de dar pausa em um jogo on-line, por exemplo”). Nessa faixa etária, crianças provavelmente não possuem capacidade cognitiva de seguir regras que não sejam simples ou intuitivas e geralmente são supervisionadas por adultos a maior parte do tempo. Ainda, não possuem condições

---

<sup>110</sup> NUNES, Beatriz Laus Marinho (tradução) e MORENA, Carolina Braz (revisão). ITS e Instituto Alana.

<sup>111</sup> *Nudge* é “qualquer tentativa de influenciar o julgamento, escolha ou comportamento das pessoas de uma forma previsível, que é (1) possibilitada em virtude de limites cognitivos, vieses, rotinas e hábitos na tomada de decisão individual ou social, que impõem barreiras para que as pessoas ajam racionalmente em seu próprio autointeresse; e que (2) funcionam valendo-se desses limites, vieses, rotinas, e hábitos”. HANSEN, Pelle Guldborg, 2016, p. 155-175.

de consentir sozinhas para o uso de seus dados pessoais. Por isso, devem ser consideradas também intervenções como notificações parentais e a não possibilidade de alteração da configuração padrão.<sup>112</sup>

Para crianças entre as idades 6 e 9 anos, que estão nos principais anos do ensino fundamental, sugere-se que a arquitetura também seja de alta privacidade por padrão e que caso haja tentativa de mudar alguma configuração, os responsáveis legais sejam envolvidos. Essas crianças geralmente utilizam dispositivos para jogar online e assistir vídeos, além de começarem a possuir a necessidade de interagir com colegas de forma virtual ou utilizar meios digitais para realizar tarefas advindas da escola. Nesse sentido, também se incentiva a inclusão de *nudges* de bem-estar e o fornecimento de explicações simples em relação ao tratamento de dados pessoais, de modo que soem como regras<sup>113</sup>.

Crianças entre 10 e 12 anos estão passando por uma fase de transição escolar, mas pela idade ainda se sugere que a arquitetura seja de alta privacidade por padrão e que em caso de tentativa de mudanças os responsáveis legais sejam envolvidos. No entanto, é necessário que se estimule a tomada de decisões conscientes e que essas regras relacionadas à autoridade dos pais sejam consideradas de forma casuística, visto que é uma faixa etária em que há maior desenvolvimento de autoidentidade e de relacionamentos. Também há a necessidade de se incentivar a inclusão de *nudges* de bem-estar<sup>114</sup>.

Na faixa etária entre 13 e 15 anos, onde inicia-se a adolescência, as recomendações em relação à arquitetura são semelhantes às das crianças entre 10 e 12 anos. No entanto, pode ocorrer um distanciamento dos valores culturais de seus pais e conseqüentemente há a busca de aplicações que são desconhecidas por estes, o que dificulta que crianças os procurem em casos de problemas online. Nesse sentido, além da inclusão de *nudges* de bem-estar, recomenda-se o incentivo à tomada de decisões conscientes e a explicação sobre funcionalidades e riscos das plataformas aos adolescentes<sup>115</sup>.

Por fim, na faixa etária entre 16 e 17 anos, adolescentes estão se aproximando da maioridade e por isso geralmente já possuem capacidade técnica e desenvolveram

---

<sup>112</sup> NUNES, Beatriz Laus Marinho (tradução) e MORENA, Carolina Braz (revisão). ITS e Instituto Alana, p. 105 e 128.

<sup>113</sup> idem, p. 105 e 129.

<sup>114</sup> idem, p. 105 e 130.

<sup>115</sup> idem, p. 106 e 131.

habilidades e estratégias online para lidar com algumas situações. No entanto, há a possibilidade da tomada de decisões impulsivas em vista de ainda estarem desenvolvendo sua capacidade cognitiva e emocional, sendo o apoio dos pais visto como uma opção. Assim, é importante que, além de ser necessário o desenvolvimento de arquitetura de alta privacidade por padrão, haja outras fontes de apoio para que possam lidar com as questões online. Por isso, o ICO recomenda que o consentimento seja provido pelos próprios adolescentes e que haja também a inclusão de *nudges* de bem-estar<sup>116</sup>.

Assim, para o alcance dos padrões estabelecidos, o Estado precisa criar mecanismos regulatórios que estimulem as práticas acima. Nesse sentido, há a necessidade do estabelecimento de uma agenda regulatória pela ANPD para que haja a regulação do artigo 14 da lei e sejam criadas regras mais específicas para o tratamento de dados pessoais de crianças e adolescentes no país<sup>117</sup>. Para tanto, com base nos escritos de Elora Fernandes, recomenda-se que sejam regulados alguns aspectos essenciais da lei na perspectiva do design das arquiteturas, que serão descritos abaixo.

Como abordado no capítulo 1 deste estudo, as bases legais estipuladas para crianças e adolescentes não são totalmente adequadas e não se enquadram na realidade de como as relações sociais ocorrem, por isso é importante que sejam regulamentadas a utilização de outras bases legais para o tratamento de crianças e adolescentes que não seja o consentimento. A medida garantirá mais segurança jurídica no meio digital pois, na prática, é impossível que o consentimento abarque todo o espectro de tratamento de dados dessas pessoas, principalmente em relação aos adolescentes<sup>118</sup>.

Também já delineado, o estabelecimento de alta privacidade por padrão deve ser um aspecto a ser regulado, de modo que se alcance o previsto no art. 14, §4º, da LGPD. Assim, devem ser estabelecidos os parâmetros mais protetivos possíveis para crianças e adolescentes que visem a busca de seu melhor interesse, de modo que se garantam os princípios dispostos no art. 6º, da mesma lei<sup>119</sup>.

---

<sup>116</sup> *idem*, p. 106 e 131.

<sup>117</sup> ELORA, Fernandes, 2021, p. 242.

<sup>118</sup> *Idem*, p. 243-244

<sup>119</sup> *Idem*.

Outro ponto que a ANPD necessita desenvolver a regulamentação sobre seriam relacionados aos aspectos necessários para a elaboração de relatório de impacto, pois é um instrumento necessário para a avaliação de riscos que podem impactar crianças e adolescentes no desenvolvimento de novas tecnologias. Na LGPD, este documento é previsto nos art. 5º, XVII, art. 10, § 3º e art. 38<sup>120</sup>.

Mais um foco fundamental deveria ser a elaboração de regulamentação para parâmetros técnicos envolvendo segurança da informação para o tratamento de dados pessoais de crianças e adolescentes. Alguns exemplos “seriam o uso de criptografia,<sup>436</sup> a separação de seus dados em relação aos dados de adultos, o processamento de dados no próprio aparelho e não na nuvem”<sup>121</sup>.

Nesse sentido, quando um aplicativo estabelece a proibição de seu uso por crianças e adolescentes, deveriam ser estabelecidos mecanismos reais que garantam que este não seja acessado<sup>122</sup>. Por isso, a ANPD deve regular este assunto. Não basta que a proibição seja descrita apenas nos termos de uso, pois em situações práticas se mostra uma medida totalmente ineficaz, já que os próprios adultos mal leem em termos de uso. Ademais, cabe ressaltar que<sup>123</sup>:

Crianças e adolescentes não devem ser simplesmente banidos da utilização do produto ou serviço ou terem sua experiência prejudicada, devendo, sempre que possível, ser criados espaços que estejam de acordo com o seu melhor interesse.

No mesmo viés, também é necessária a regulamentação de limites de idade para coleta de dados de crianças. Assim, aplicativos que realizam a implementação de mecanismos de verificação de idade poderiam se basear em aspectos concretos para a real verificação de quem está utilizando o aplicativo ou para a validação do consentimento quando este for solicitado<sup>124</sup>.

O tratamento de dados relacionados às decisões automatizadas ou perfilamento é um item de extrema importância que necessita de maior aprofundamento regulatório, principalmente quando observado através da perspectiva dos dados de crianças e adolescentes. Idealmente, a menos que para o alcance de seus melhores interesses, crianças e adolescentes não deveriam ter seus dados tratados para perfilamento ou decisões automatizadas. Uma medida que pode auxiliar

---

<sup>120</sup> Idem, p. 244-245.

<sup>121</sup> Idem, p. 245.

<sup>122</sup> Idem, p. 246-247.

<sup>123</sup> Idem.

<sup>124</sup> Idem, p. 247.



neste ponto é a criação de mecanismos de design que evitem ao máximo a criação de perfis por crianças, por exemplo. Também, outro ponto relevante neste viés seria o desenvolvimento de regulamentação específica para o tratamento de dados pessoais sensíveis de crianças e adolescentes<sup>125</sup>.

Como já mencionado, a utilização de técnicas de *nudge* de bem-estar, a evitação de designs enganosos (exemplo: interface com existência de cadeados para transmitirem uma ideia de segurança) e a utilização de linguagem acessível e com transparência são mecanismos mecanismo que auxiliam crianças e adolescentes a terem um melhor aproveitamento e desenvolvimento no ambiente digital e podem ser regulamentadas pela Autoridade<sup>126</sup>. Exemplos relevantes de *nudges* seriam:

A proibição de designs e tratamento de dados para manter usuários engajados com a tecnologia o maior tempo possível (exemplos seriam os chamados loops de recompensa, feeds infinitos ou rolagem de tela contínua, notificações abusivas e recursos de reprodução automática).<sup>443</sup>

Outro aspecto importante para regulamentação seria relacionado ao exercício dos direitos dos titulares previstos no art. 18 da LGPD. Nesse sentido, devem ser delineados as formas que crianças e adolescentes poderão exercer seus direitos diretamente ou acompanhados de acordo com a sua fase de desenvolvimento<sup>127</sup>.

Também, os contextos envolvendo compartilhamento de dados com terceiros devem ser vislumbrados na agenda regulatória da ANPD. Em relação às crianças, recomenda-se que se adote uma postura conservadora e se evite o compartilhamento de seus dados em qualquer hipótese, “a menos que seja essencial para a concretização de seu melhor interesse”<sup>128</sup>.

Por fim, a regulamentação sobre os limites e deveres envolvendo controle parental é um dos assuntos mais importantes na seara do tratamento de dados de crianças e adolescentes. Como já defendido, é necessário que haja espaços privados em relação aos pais “para o desenvolvimento saudável da personalidade, da criatividade e da autonomia”. Para isso, os ambientes devem ser seguros para que sejam utilizados por crianças e adolescentes. Esta medida é ideal para o alcance da privacidade interpessoal<sup>129</sup>.

---

<sup>125</sup> Idem, p. 248-250.

<sup>126</sup> Idem, p. 249-250.

<sup>127</sup> Idem, p. 252-253.

<sup>128</sup> Idem, p. 252.

<sup>129</sup> Idem, p. 251.

Assim, para que as sugestões acima sejam possíveis, a ANPD deve atuar de forma constante na esfera educacional de modo que se promova a educação digital desde os primeiros anos de vida. Esta educação deve ser promovida para adultos também, que muitas vezes não compreendem como funcionam algumas tecnologias e acabam pecando pela falta de informação. A regulamentação sobre o tema necessita ser realizada de forma transparente e principalmente incluindo a opinião de crianças e adolescentes<sup>130</sup>.

Assim, é essencial que a regulamentação desse tema seja feita de forma democrática, aberta e transparente, com consultas públicas e tomadas de subsídio de todos os setores, mas, em especial, fazendo valer o direito de participação de crianças e adolescentes, os mais afetados neste processo, assim como foi feito no recente e festejado Comentário nº 25, do Comitê sobre os Direitos da Criança. Para além disso, é preciso que a atuação da ANPD incentive essa participação em todo o processo de elaboração de tecnologias e também novos modelos de negócios que estejam alinhados à promoção dos direitos de crianças e adolescentes.

Essas medidas são importantes para que se alcancem os princípios da autodeterminação informativa e do melhor interesse. Apesar de serem buscados exemplos internacionais, ressalta-se que devem ser levadas em consideração as especificidades presentes no contexto social brasileiro quando na elaboração de políticas públicas envolvendo meios digitais, pois os valores e questões socioculturais presentes no país são fatores relevantes a serem observados e fazem diferença em como as situações serão vividas na prática.

## **CONSIDERAÇÕES FINAIS**

O presente estudo buscou, em um primeiro momento, entender quais seriam os aspectos gerais sobre a proteção de dados pessoais de crianças e adolescentes. Para isso, foram delineados os conceitos de dado e especificamente de dado pessoal com base na Lei Geral de Proteção de Dados brasileira.

Seguindo, foi trazido à baila a importância que a proteção aos dados pessoais incorporou na sociedade atual, sendo considerada inclusive como um direito fundamental, estando intrinsecamente ligada ao conceito de privacidade e ao princípio da autodeterminação informativa. Este último, que é positivado na LGPD a partir do

---

<sup>130</sup> idem, p. 253-254

exercício dos direitos do titular de dados pessoais e sendo indissociável para a noção de dignidade da pessoa humana.

Assim, procurou-se avaliar as vulnerabilidades de crianças e adolescentes dentro do contexto de existência digital e alguns dos mecanismos de proteção a este grupo que se encontram no arcabouço legislativo brasileiro, como a Constituição Federal e o Estatuto da Criança e do Adolescente. Então, foram considerados alguns dados estatísticos relevantes sobre os níveis de utilização da Internet por crianças e adolescentes no Brasil.

Nesse viés, entendeu-se que a legitimidade de crianças e adolescentes em relação ao direito de proteção aos seus dados pessoais seria válida não apenas para precaução em relação aos riscos existentes no mundo digital, mas também para exercício de sua autonomia e desenvolvimento social, cognitivo e biológico. E, nessa perspectiva, a LGPD teria elaborado hipóteses específicas em que seus dados poderiam ser tratados, com vistas sempre ao princípio do melhor interesse.

Por conseguinte, foram analisadas as bases legais presentes na norma citada que possibilitam a ocorrência do tratamento de dados pessoais de indivíduos em geral e mais especificamente de crianças e adolescentes. Assim, foi apresentada a diferenciação que é realizada em relação aos dados de adolescentes para os de crianças, que tem a ver com as etapas do desenvolvimento de uma pessoa na sociedade e no início de tomada de decisões conscientes independentes de seus responsáveis legais.

Em sequência, questionou-se a utilização do consentimento como a única base legal para o tratamento de dados de crianças, pois seria uma interpretação que poderia inviabilizar algumas situações. Ainda, também foi questionada o que seria a busca pelo “melhor interesse” e como de fato aplicar este conceito para as relações sociais e comerciais envolvendo dados do público infantojuvenil.

Para tanto, foi entendido que o melhor interesse deveria ser compreendido como um direito fundamental às crianças e adolescentes e uma regra de interpretação que atenda de forma objetiva a garantia de direitos fundamentais no maior grau possível para preservação da dignidade das crianças e adolescentes. Devendo, assim, ser avaliado casuisticamente.

Após, adentrou-se no estudo de casos envolvendo situações em que os próprios pais ou responsáveis legais poderiam ser os responsáveis por causar danos decorrentes da sua forma de controlar o acesso e a exposição de seus filhos na

internet. De tal maneira, foram levantadas algumas controvérsias relacionadas ao uso de tecnologias e mídias digitais por crianças e adolescentes.

Foi observado que muitos jovens buscam ambientes digitais livres da presença de adultos e que isso faria parte de seus processos de desenvolvimento. No entanto, seria um contraponto em relação aos possíveis excessos de cautela que os adultos poderiam ter para com seus filhos, surgindo assim certa dificuldade para que haja um balanceamento sobre o melhor interesse em relação ao que os pais entendem como proteção. Nesse sentido, questionou-se a real necessidade de um nível de controle tão extremo em nome de uma proteção prometida por aplicações digitais.

Assim, foi considerado que um certo nível de exposição a riscos poderia ser favorável para que crianças aprendam a se adaptar e a lidar com situações arriscadas. Concluiu-se, assim, que um monitoramento excessivo pode ser prejudicial ao desenvolvimento infantil.

Por outro lado, foi constatado pais e responsáveis legais muitas vezes não possuem um nível de consciência adequado sobre os meios digitais e, por isso, podem acabar seguindo o caminho contrário: o da superexposição dos dados pessoais de seus filhos na internet. Este fenômeno, conhecido como *oversharenting*, pode repercutir de diversas maneiras negativas na vida de crianças e adolescentes, afetando seus direitos de personalidade.

O estudo avaliou casos concretos que demonstram algumas das consequências que esse tipo de atitude pode causar em suas vidas. Especificamente, refletiu-se sobre o recente caso da criança de 2 anos que participou de um comercial patrocinado por um dos maiores bancos do mundo. Concluiu-se, então, que esta superexposição pode fazer com que crianças e adolescentes sejam vítimas de *bullying* e *cyberbullying*, riscos envolvendo sua integridade física, antipatia de seus seguidores e até atrapalhar no futuro na tentativa de ingressar no mercado de trabalho. Sustentou-se, assim, que devem ser buscadas medidas que visem assegurar o exercício da autonomia do público infantojuvenil para que esta possa participar das decisões ou ter ciência sobre como seus dados estão sendo compartilhados.

Após, adentrou-se na perspectiva do direito ao esquecimento para crianças e adolescentes. Foram analisados os aspectos envolvendo este direito no Brasil e na Europa e concluiu-se que seria um instrumento válido e necessário para que crianças

e adolescentes tivessem garantidos para si o princípio da autodeterminação informativa. Defendeu-se, assim, a utilização deste mecanismo no país.

Por fim, foram trazidas as nuances envolvendo os aspectos e desafios regulatórios relacionados ao tratamento de dados pessoais de crianças e adolescentes. Assim, foi considerado que a internet não foi pensada tendo como base o princípio da segurança e que as tecnologias que dela se desenvolveram não foram elaboradas na perspectiva de grupos vulneráveis, como os estudados nesta monografia. Dessa forma, chegou-se à conclusão de que as legislações presentes no país não seriam suficientes para resguardar a proteção dos dados pessoais de crianças e adolescentes e para a garantia do princípio da autodeterminação informativa. Ainda, que a culpa sobre o tratamento dos dados do grupo estudado não deveria recair apenas sobre os responsáveis legais, mas em conjunto com Estado e os agentes privados que atuam na sociedade em geral.

Por isso, defendeu-se que a Agência Nacional de Proteção de Dados deve proceder com a regulamentação do art. 14 da LGPD, que dispõe sobre o tratamento de dados pessoais de crianças e adolescentes. Para que esta medida seja efetiva, defendeu-se que se deve partir da ideia de regulação da arquitetura das plataformas digitais a partir da privacidade por design.

A privacidade por design está presente no art. 46 da LGPD e a sua regulamentação auxiliaria com que fossem neutralizados alguns valores permeados pelos desenvolvedores das plataformas. Como exemplo, foram trazidos os padrões sombrios que deveriam ser evitados no desenho das aplicações e os princípios norteadores do *privacy by design* que deveriam ser utilizados como base para a regulamentação.

Não só isso, entendeu-se que para que haja efetividade na concretização desta ideia, a ANPD deveria instituir uma agenda regulatória para tratar sobre os assuntos envolvendo o *design* das arquiteturas e tratar de temas como: bases legais, alta privacidade por padrão, relatório de impacto, parâmetros técnicos de segurança da informação, proibição do uso de aplicativos por crianças e adolescentes, limites de idade para coleta de dados, verificação de idade, decisões automatizadas ou perfilamento, tratamento de dados sensíveis, utilização técnicas de *nudge*, utilização de linguagem transparente e acessível, exercício do direito dos titulares, compartilhamento de dados por terceiros e controle parental.

Ao final, defendeu-se que a implementação desta regulamentação deve ser realizada respeitando o contexto sociocultural brasileiro e juntamente com atuação na esfera educacional de modo que a educação digital seja promovida desde os primeiros anos de vida. Pretendeu-se, assim, que essas medidas auxiliem no alcance dos princípios da autodeterminação informativa e do melhor interesse para crianças e adolescentes.

## **BIBLIOGRAFIA**

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

BRASIL. Lei nº 8.069, de 13 de julho de 1990, **Estatuto da Criança e do Adolescente**. Brasília, DF, 1990.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília, DF, 2014.

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

CAVOUKIAN, Ann, Ph.D. **Privacy by Design: The 7 Foundational Principles**. Creation of a Global Privacy Standard (November 2006) Information and Privacy Commissioner of Ontario: Ontario, 2011.

CUEVA, Ricardo Villas Bôas, **Proteção de dados pessoais e direito ao esquecimento**. In: DONEDA, Danilo et al (Coords.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

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

EBERLIN, Fernando B. von T. **Direitos da criança na sociedade da informação: ambiente digital, privacidade e dados pessoais**. São Paulo: Thomson Reuters Brasil, 2020.

FERNANDES, Elora. **Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANPD**. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). Privacidade e proteção de dados de crianças e adolescentes. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

\_\_\_\_\_, Elora; MEDON, Filipe. **Proteção de crianças e adolescentes na LGPD: Desafios interpretativos**. Rio de Janeiro: Revista eletrônica da PGE-RJ, v. 4, n. 2, maio/ago., 2021.

HANSEN, Pelle Guldborg. **The definition of nudge and libertarian paternalismo: does the hand fit the glove?** Europa: European Journal of Risk Regulation, p. 155-174, 2016.

HENRIQUES, Isabella; HARTUNG, Pedro; PITA, Marina. **A proteção de dados pessoais de crianças e adolescentes**. In: DONEDA, Danilo et al (Coords.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

HOFFMAN-RIEM, Wolfgang. **Big data e inteligência artificial: desafios para o direito**. In: Journal of Institutional Studies 2, v. 6, p. 431-506, maio/ago. 2020.

LEMOS, Ronaldo; BRANCO, Sérgio. **Privacy by Design: Conceito, fundamentos e aplicabilidade na LGPD**. In: DONEDA, Danilo et al (Coords.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2014.

MARTINS, Guilherme Magalhães. **O direito ao esquecimento como direito fundamental**. Civilistica.com, Rio de Janeiro, a. 10, n 3, 2021. Disponível em:

<<http://civilistica.com/o-direito-aoesquecimento-como-direito/>>. Data de acesso 04/01/2022.

MEDON, Filipe. **(Over)sharenting: a superexposição da imagem e dos dados da criança na internet e o papel da autoridade parental**. Indaiatuba: Editora Foco Jurídico Ltda, 2021.

NUNES, Beatriz Laus Marinho (tradução); MORENA, Carolina Braz (revisão). **Design apropriado para a idade: código de práticas para serviços on-line**. Age-Appropriate Design Code elaborado pelo Information Commissioner's Office (ICO) do Reino Unido. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro e Alana com apoio do Governo do Reino Unido. 2021. E-book.

RODOTÁ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.  
SARLET, Ingo Wolfgang. Fundamentos Constitucionais: **O direito fundamental à proteção de dados**. In: DONEDA, Danilo et al (Coords.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

TEIXEIRA, Ana Carolina Brochado; RETTORE. **O princípio do melhor interesse no ambiente digital**. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). Privacidade e proteção de dados de crianças e adolescentes. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

TEPEDINO, Gustavo; MEDON, Filipe. **A superexposição de crianças por seus pais na internet e o direito ao esquecimento**. Indaiatuba: Editora Foco Jurídico Ltda, 2021.

União Europeia. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation)**. Jornal Oficial da União Europeia: Estrasburgo, 2016.



VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11.** In: DONEDA, Danilo et al (Coords.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

\_\_\_\_\_, Mario; VARGAS, Vanessa. **Desafios para a tutela da privacidade infantil na era digital: FERPA, COPPA, GDPR e Lei Geral de Proteção de Dados.** In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). Privacidade e proteção de dados de crianças e adolescentes. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, [s.1.], v., n. 5, p. 193-220, 15 dez. 1890.