Privacy by Design e a proteção dos dados pessoais dos adolescentes

Zélia Maria Martins Guilherme[1]
Orientador: Gustavo Pereira Leite Ribeiro[2]

Resumo: Hoje, adolescentes estão constantemente conectados ao ambiente digital. No entanto, nota-se que o espaço virtual não foi pensado e desenhado para considerar os interesses desses sujeitos. O presente trabalho busca demonstrar que as empresas de tecnologia devem se valer da metodologia da *Privacy by Design* para garantir o direito à proteção de dados dos adolescentes no ambiente virtual, tendo em vista suas capacidades e condição peculiar de desenvolvimento. Essa ferramenta possui como objetivo incorporar a proteção de dados em todo o ciclo de vida de determinado serviço ou produto. Além disso, busca-se capacitar os indivíduos para desempenhar um papel ativo no gerenciamento de seus dados. Para alcançar o objetivo proposto, o texto foi dividido em três partes. Inicialmente, delimitou-se o sentido e o alcance do direito à proteção de dados pessoais do adolescente. Em sequência, discutiu-se a insuficiência do artigo 14, §1º, da Lei Geral de Proteção de Dados (LGPD), ao utilizar o consentimento dado pelo adolescente como instrumento de proteção dos dados pessoais desses sujeitos. No último tópico, apresentou-se as origens da *Privacy by Design*, bem como os princípios norteadores dessa metodologia. Por fim, discutiu-se sobre a necessidade de envolvimento dos adolescentes na proteção de seus dados pessoais.

Palavras-chaves: Proteção de Dados; Adolescentes; *Privacy by Design*.

Abstract: Today, adolescents are constantly connected to the digital environment. However, it is noted that the virtual environment was not thought and designed to consider the interests of these individuals. The present work seeks to demonstrate that technology companies should use the Privacy by Design methodology to guarantee adolescents' right to data protection in the virtual environment, given their capacities and peculiar developmental condition. This tool aims to incorporate data protection throughout the life cycle of a given service or product. In addition, it seeks to empower individuals to play an active role in managing their data. To achieve the proposed objective, the article is divided into three parts. Initially, the meaning and scope of the

[1] Graduanda em Direito pela Universidade Federal de Lavras. Integrante do Programa de Educação Tutorial Institucional da Universidade Federal de Lavras (PETI/UFLA). Integrante do Laboratório de Bioética e Direito (LABB/CNPq).
[2] Mestre (2004) e Doutor (2010) em Direito Privado pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas). Professor Associado de Direito Civil na Universidade Federal de Lavras (UFLA). Líder do grupo de pesquisa Laboratório de Bioética e Direito (LABB/CNPq) e do Programa de Educação Tutorial Institucional da Universidade Federal de Lavras (PETI/UFLA).

right to the protection of adolescents' data was delimited. Next, was discussed the insufficiency of Article 14, paragraph 1, of the General Data Protection Law (LGPD) when using the consent given by the adolescent as an instrument to protect the personal data of these individuals. In the last topic, the origins of Privacy by Design were presented, as well as the guiding principles of this methodology. Finally, the need to involve adolescents in the protection of their personal data was discussed.

Keywords: Data Protection; Adolescents; Privacy by Design.

Introdução

A pesquisa TIC Kids Online Brasil, divulgada no ano de 2021, revelou que, entre crianças e adolescentes, o uso de redes sociais é uma das atividades *online* que mais cresceu. Em 2021, 78% dos usuários de Internet, com idades entre 9 e 17 anos, acessaram esse tipo de plataforma, o que representou um aumento de 10% em relação a 2019 (68%). Além disso, revelou também que 83% das crianças e adolescentes, de igual faixa etária, utilizaram a Internet mais de uma vez ao dia.[3]

Seja por meio da apresentação de pesquisas, seja pela própria observação do cotidiano, evidencia-se que os adolescentes estão totalmente inseridos no ambiente virtual, de modo que se torna necessária a discussão acerca da proteção de seus dados pessoais. Isso porque, a capacidade de coleta de dados pelas empresas tem se tornado cada vez mais eficiente e complexa. A partir dos dados colhidos, essas instituições conseguem analisar o comportamento e os hábitos dos indivíduos, bem como utilizar essas informações de diversas formas.

[3] TIC Kids Online Brasil 2021: 78% das crianças e adolescentes conectados usam redes sociais. *Cetic.br*, São Paulo, 16 ago. 2022. Disponível em: https://bit.ly/3ksqdKQ.

Ao mesmo tempo em que cresce a utilização da internet por adolescentes, desponta também a preocupação quanto aos riscos a que esses sujeitos podem ser expostos no ambiente virtual. No entanto, para além de protegê-los desses riscos, importa pensar nas formas a partir das quais essa parcela da população terá assegurada a efetividade de seu direito à proteção de dados, tendo em vista sua condição peculiar de desenvolvimento.

No Brasil, a Lei Geral de Proteção de Dados, a fim de conferir maior proteção aos dados de crianças e adolescentes, destinou no Capítulo II, referente ao tratamento de dados pessoais, a Seção III, que disciplina acerca do tratamento de dados pessoais de crianças e adolescentes. Nessa, trouxe especificamente o art. 14, o qual dispõe acerca das regras de proteção de dados desses sujeitos. O legislador prevê em seu *caput* que o referido tratamento de dados deverá ser realizado a partir do seu melhor interesse.

Contudo, a LGPD tem apresentado incongruências quanto ao tratamento de dados de crianças e adolescentes, especialmente de adolescentes. Isso porque, o art. 14, § 1º, LGPD, dispõe que o tratamento de dados de crianças só poderá ser realizado por meio do consentimento de um dos pais ou responsável legal, não incluindo, aqui, os adolescentes, como fez o *caput* do dispositivo. Assim, ao não restringir aos pais o consentimento para o uso dos dados de adolescentes, interpreta-se que o legislador teria compreendido que tais sujeitos possuem capacidade para, de forma autônoma, manifestar sua vontade.

Apesar da evolução percebida, ao reconhecer o direito do adolescente de exercer, de forma autônoma, o controle de seus dados pessoais, o artigo 14, § 1º, LGPD, ainda se mostra insuficiente. Isso porque, o principal mecanismo para assegurar a proteção dos dados pessoais desses sujeitos tem sido o consentimento. Contudo, no ambiente virtual, a efetivação de um consentimento válido, sobretudo de adolescentes, torna-se uma tarefa muito mais complexa, já que não resta assegurado que os titulares dos dados, de fato, concordaram com o conteúdo aderido.

A partir deste cenário, o presente trabalho possui como objetivo demonstrar que as empresas de tecnologia devem se valer da metodologia da *Privacy by Design* para garantir o direito à proteção de dados dos adolescentes no ambiente virtual, à luz de suas capacidades e condição peculiar de desenvolvimento. Mais do que protegê-los, torna-se necessário prepará-los para lidar com os riscos e benefícios do ambiente virtual.

Para adequada compreensão da temática, este trabalho foi divido em três partes. Inicialmente, delimita-se o sentido e alcance do direito à proteção dos dados pessoais dos adolescentes. Isso, com objetivo de compreendê-lo enquanto um direito que possibilita ao titular ter controle de seus dados pessoais. Assim, ao adolescente deve ser oportunizado, enquanto sujeito com absoluta prioridade no ordenamento jurídico brasileiro, o direito de exercê-lo de acordo com suas particularidades.

O segundo tópico busca demonstrar a insuficiência da Lei Geral de Proteção de Dados ao utilizar, em seu art. 14, § 1º, LGPD, o consentimento dado pelo adolescente como instrumento protetivo de seus dados pessoais. Isso porque, o consentimento no ambiente virtual tem sido obtido por meio das políticas de privacidade, estruturadas nos moldes de "tudo ou nada". Ou a pessoa aceita, em um único momento, autorizar a utilização de seus dados, ou terá seu acesso a determinado serviço ou produto impedido. Dessa maneira, não há garantia de que tais indivíduos terão o controle de seus dados.

Em resposta ao problema, o terceiro tópico apresenta a metodologia da *Privacy by Design* enquanto expediente adequado para garantir a proteção de dados pessoais do adolescente. Criada por Ann Cavoukian, a *Privacy by Design* possui como cerne a operacionalização de sete princípios fundantes. Uma vez aplicados de forma sólida e sistemática, o consentimento obtido no ambiente virtual se mostra um meio de proteção mais autêntico, uma vez que passa a atender todos os critérios exigidos pela LGPD. Nasce, assim, um melhor caminho para garantir que os adolescentes terão um envolvimento saudável no ambiente virtual, já que a salvaguarda de sua autonomia só é possível quando há apoio, informação e orientação.

1 O sentido e o alcance do direito à proteção dos dados dos adolescentes na sociedade de informação

A proteção de dados pessoais é um tema da agenda contemporânea, no Brasil e no mundo.[4] A discussão em relação à disciplina vem sendo construída há, ao menos, cinco décadas. De tal forma, a Lei de Proteção de Dados da Alemanha, em 1970, foi considerada pioneira por desenvolver um modelo normativo autônomo para a proteção de dados pessoais.[5]

[4] DATA protection laws of the world. Disponível em: https://encurtador.com.br/dkJU3.
[5] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 22.

Hoje, a disciplina já alcançou certo grau de harmonização em diversos países. De acordo com estimativas, o perfil dessa matéria está presente de forma concreta em mais de 140 países.[6] Isso significa que os seus principais institutos e ferramentas fazem parte da maioria das legislações de proteção de dados existentes, de modo a proporcionar estruturas semelhantes.[7]

A necessidade do desenvolvimento de legislações sobre o tema se dá, principalmente, à luz do avanço tecnológico e da massificação do uso das tecnologias da informação e comunicação. Dentre as inovações tecnológicas, a Internet, em especial, mudou a maneira a partir da qual as pessoas se relacionam entre si, fazem negócios e divertem-se. Fazer compras, descansar, estudar, viajar, ir ao nutricionista, assistir a filmes, se divertir com os amigos ou até mesmo namorar: nada é como antes. Isto é, tudo pode passar pela rede e, consequentemente, algum dado será utilizado para o fornecimento de determinado serviço ou produto.[8]

Como explica Stefano Rodotà, a atual capacidade de coleta de informações dos meios interativos é altamente complexa e eficiente, bem como institui uma comunicação direta entre os gestores de serviços e os usuários. A partir da concessão dos dados pelos seus titulares, as empresas conseguem analisar comportamento, hábitos e interesses dos indivíduos, utilizando-os para o aperfeiçoamento de seu produto, além da venda a terceiros. Assim, sem perceber, o indivíduo fornece dados que serão utilizados para persuadi-lo.[9]

Vale ressaltar que não é apenas o setor privado que se vale do tratamento de dados[10] para melhorar sua eficiência. O setor público também os utiliza, seja para fins de segurança e monitoramento, seja para a realização de censos ou desenvolvimento de políticas públicas.[11] Fato é que, hoje, a sociedade é movida a dados. A partir desse cenário, o

---

[6] GREENLEAF, Graham; COTTIER, Bertil. 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business Internacional Report*, [s.l.], v. 163, [s.n], p. 1-5, maio, 2020. Disponível em: https://encurtador.com.br/gloxS.

[7] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 22.

[8] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 213.

[9] RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 62.

[10] Utiliza-se tratamento de dados pessoais para designar as operações técnicas realizadas com os dados pessoais, de modo automatizado ou não, com a finalidade de se transformar dado pessoal em informação.

[11] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 213.

presente trabalho pretende identificar o que significa, na contemporaneidade, proteção de dados pessoais.

No entanto, para se falar em proteção de dados, é necessário compreender os conceitos jurídicos de dado e informação, visto que, na maioria das vezes, ambos são utilizados como sinônimo, embora não sejam. Segundo Bruno Bioni, dado é o estado primitivo da informação, pois sozinho não consegue exprimir nenhum tipo de conhecimento sobre o sujeito. Em suas palavras, "dados são simplesmente *fatos brutos* que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação".[12] Isso possibilita que os dados, após processados e convertidos em informação, passem a ser utilizados para comércio, marketing, vendas, elaborações de políticas públicas e demais atuações.

Quanto ao conceito de dados pessoais, destaca-se que são os fatos, comunicações e ações que se referem às circunstâncias pessoais de um indivíduo, identificado ou identificável. Como discutido, a informação é sempre o resultado de uma ação interpretativa. Nesse sentido, um dado pode ser qualificado como pessoal quando informações capazes de revelar a identidade de determinada pessoa puderem ser extraídas dele.[13] Alguns exemplos de dados pessoais são: qualificação pessoal do sujeito, como nome completo, endereço, telefone e número do CPF; características pessoais, como altura, raça, cor dos olhos e tipo de cabelo; e outras informações como dados genéticos.

Devido a esse caráter pessoal, a disciplina jurídica se preocupa com a proteção do sujeito e com a circulação dos seus dados pessoais, considerando o uso que a sociedade de informação faz deles. No entanto, em diversos momentos da história, a proteção de dados pessoais apresentou uma roupagem diferente da que se revela hoje.

Desde a década de 1970, já existiam iniciativas legislativas para a proteção de dados. As primeiras leis sobre a temática propunham-se a regular um cenário no qual centros de tratamento de dados, de grande porte, concentravam a coleta e a gestão de dados pessoais. Proteger dados, nessa época, significava obter a concessão de autorizações para a criação destes bancos de dados e de seu controle, *a posteriori,* por órgãos públicos. A relação estabelecida era, primordialmente, entre titulares de dados e Estado, já que este

---

[12] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 55, grifo do autor.
[13] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 169.

era o destinatário principal (se não o único) destas normas.[14] Contudo, rapidamente essas leis tornaram-se ultrapassadas, diante da multiplicação de centros de processamento e, consequentemente, da impossibilidade de se garantir um controle efetivo.

Leis posteriores surgiram na segunda metade da década de 70. As técnicas utilizadas para proteger dados pessoais passaram a não ser dirigidas diretamente à tecnologia, como a proibição ou não da criação de determinado banco de dados. Nessa época, proteger dados pessoais significava fornecer instrumentos para o cidadão identificar o uso indevido de seus dados pessoais e propor sua tutela após determinada violação.[15]

Hoje, mais do que a interdição de acesso aos dados pessoais, busca-se garantir aos indivíduos uma liberdade de controle sobre os dados que lhes dizem respeito. Nesse sentido, proteger dados pessoais significa atribuir ao sujeito a garantia de controlar quando, como, onde e por quem seus dados poderão ser utilizados. Isso porque, os serviços tecnológicos estão cada vez mais sofisticados e as empresas, públicas e privadas, se tornam detentoras de uma quantidade relevante de dados pessoais. Como consequência, os indivíduos perdem o controle da disseminação de seus dados e ficam sujeitos ao uso deles por prestadores de serviços que sequer conhecem.

Como explica Stefano Rodotà, o direito de controlar a maneira pela qual terceiros utilizam os dados pessoais – logo, protegê-los – surge como uma ferramenta essencial para se garantir o livre desenvolvimento da personalidade.[16] Um dado atrelado à esfera de uma pessoa caracteriza-se como uma projeção, extensão ou dimensão do seu titular.[17] O seu uso indiscriminado é capaz de objetificar pessoas, afetar o desenvolvimento da personalidade, promover manipulação e gerar discriminações.[18] Assim, ao garantir aos indivíduos o poder de autonomia sobre seus dados, a própria pessoa estabelecerá os limites e a forma como deseja ser apresentada à sociedade.

No Brasil, a proteção dos dados pessoais tem se mostrado presente, embora até agosto de 2018 o ordenamento brasileiro não dispusesse de lei específica para garanti-la. Sua tutela amparava-se em dispositivos da Constituição Federal da República, como a

---

[14] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2020. p. 166.
[15] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2020. p. 167.
[16] RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 17.
[17] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2020. p. 55.
[18] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 222.

inviolabilidade da intimidade e da vida privada[19], a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas"[20] e a ação de *habeas data*[21]. Além disso, o próprio Código Civil[22], bem como o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e a Lei do Cadastro Positivo são diplomas que, em alguma medida, apresentam disposições sobre a matéria. Contudo, esse arcabouço regulatório não foi suficiente para solucionar muitas questões relativas à proteção de dados, já que não oferecia garantias às partes - o que, além de gerar insegurança jurídica, tornava o país menos competitivo no contexto de uma sociedade movida a dados pessoais.[23]

À luz da importância dos dados na atual conjuntura, no Brasil e no mundo, a recente Emenda Constitucional nº 115/2022 incluiu, no rol dos direitos fundamentais do art. 5º da Constituição, o inciso LXXIX, segundo o qual: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Além disso, a Emenda acrescentou ao art. 21 o inciso XXVI, o qual determina que compete à União "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei". Adicionou também, no art. 22, o inciso XXX, que dispõe ser competência privativa da União legislar sobre "proteção e tratamento de dados pessoais".

Além da garantia constitucional apresentada, a proteção de dados pessoais incumbe à Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), cuja vigência se iniciou em setembro de 2020. Em busca de conferir maior proteção aos dados das pessoas, o legislador estabeleceu regras para o uso, coleta, armazenamento e compartilhamento de dados pessoais. O objetivo foi sedimentar a compreensão de que os dados não são de titularidade de quem os coleta, mas da pessoa natural a que se referem.[24]

---

[19] Art. 5º, X. "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".
[20] Art. 5º, XII. "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".
[21] Art. 5º, LXXII. "conceder-se-á "habeas-data": a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".
[22] Art. 21. "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."
[23] TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. In: MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélago, 2020. p. 160.
[24] Tal constatação é possível de ser verificada a partir da leitura do art. 5, V, da LGPD, que dispõe: "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

O art. 2º, II, da Lei Geral de Proteção de Dados, elenca a autodeterminação informativa como um dos seus principais fundamentos. Com esse princípio, pretende-se viabilizar ao titular dos dados pessoais o direito de exercer controle de seus dados.[25] No entanto, se o exercício do controle sobre seus próprios dados já é difícil para indivíduos adultos, pode ser ainda mais complexo quando exercido por adolescentes. Apesar de ser uma situação que requer maiores cuidados, o que não se deve esquecer é que os dados pessoais desses sujeitos também são colhidos e utilizados no âmbito público e privado. Evidentemente, isso torna necessária a preocupação direcionada à proteção dessa parcela da população.

A LGPD, para lidar com tal situação, apresenta em seu Capítulo II, referente ao tratamento de dados pessoais, a Seção III, que disciplina acerca do tratamento de dados pessoais de crianças e adolescentes. Especificamente, em seu art. 14[26], o legislador estabelece que o tratamento de dados desses sujeitos deverá ser realizado em seu melhor interesse, ou seja, somente pode ocorrer por meio de práticas que promovam e protejam seus direitos previstos no sistema jurídico nacional e internacional, com absoluta prioridade. Vale ressaltar que o Estatuto da Criança e do Adolescente, promulgado em julho de 1990, no art. 2º, dispõe que se considera criança a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

Acerca da tutela jurídica dos adolescentes, a Constituição Federal determina, em seu art. 227, que é dever da família, da sociedade e do Estado assegurar a proteção dos seus direitos fundamentais com absoluta prioridade.[27] Mais especificamente, o Estatuto da Criança e do Adolescente adota a proteção integral dessa parcela da população ao

---

[25] BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *Cadernos Adenauer*, Rio de Janeiro, v. 3, n. 1, p. 113-135, 2019. p. 118.

[26] 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 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.

[27] Art. 227. "É 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."

determinar que a condição peculiar de desenvolvimento das crianças e dos adolescentes deve sempre ser levada em consideração para a aplicação da lei.[28]

A chamada doutrina da proteção integral foi consolidada pela Convenção Internacional sobre os Direitos da Criança[29], de 1989, e internalizada no Brasil, em 1990. Essa teoria busca compreender a posição ocupada pelas crianças e adolescentes no mundo jurídico, afirmando que eles "não são adultos mais jovens, mas são seres diferentes, que, embora estejam em fase de crescimento e de formação, são portadores de projetos de vida próprios".[30]

Assim, a coleta e o tratamento dos dados de adolescentes requerem uma proteção especial, voltada às suas peculiaridades. Apesar de eles, atualmente, estarem em contato constante com a tecnologia, e serem até mesmo chamados de nativos digitais, por vezes os adolescentes não conseguem compreender as complexas dinâmicas atreladas ao impacto do uso de seus dados pessoais.[31]

O que se pretende, neste trabalho, é defender que, embora a Lei Geral de Proteção de Dados tenha destinado o seu art. 14, exclusivamente, para dispor sobre o tratamento de dados pessoais de criança e adolescentes, este ainda se mostra insuficiente para garantir a proteção de seus dados. Isso porque, o consentimento é a principal ferramenta apresentada pela Lei para garantir o controle dos dados pessoais desses sujeitos. Contudo, no ambiente virtual, a obtenção de um consentimento válido dos adolescentes torna-se uma tarefa complexa, já que não assegura que os titulares, de fato, tenham controle de seus dados.[32]

2 A função do consentimento

A regulação jurídica em torno da proteção dos dados pessoais está amparada no direito que cada indivíduo deve ter de controlar livremente a circulação e a utilização de seus

[28] 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.
[29] Vale ressaltar que a Convenção sobre os Direito da Criança considera crianças os indivíduos de até 18 anos de idade, ou seja, na definição da legislação brasileira, refere-se a crianças e adolescentes.
[30] MENEZES, Joyceane Bezerra de; MORAES, Maria Celina Bodin de. Autoridade parental e privacidade do filho menor: o desafio de cuidar para emancipar. *Revista Novos Estudos Jurídicos*, Itajaí, v. 20, n. 2, p. 501-532 jul. 2015. Disponível em: https://encurtador.com.br/msLT7. p. 507-508.
[31] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 202.
[32] EBELIN, Fernando Büscher von Teschenhausen. *Direitos da criança na sociedade da informação*. São Paulo: Revista dos Tribunais, 2020. p. 249.

dados na sociedade, de modo a preservar seu livre desenvolvimento da personalidade.[33] Assim, cabe ao Estado por meio de legislações promover ferramentas adequadas para que o cidadão consiga exercer tal direito.

Diante do objetivo de garantir aos indivíduos maior controle de seus dados pessoais, a figura do consentimento ganha especial relevância após a segunda geração de leis de proteção de dados, em meados da década de 80. A preocupação desloca-se das bases de dados estatais, as quais tinham como objetivo estabelecer normas rígidas que domassem o uso da tecnologia, para a proteção da esfera privada dos sujeitos. Com isso, o fluxo dos dados pessoais, antes controlado pelo Estado, agora cabe ao próprio cidadão, que, por meio do consentimento, realiza suas escolhas em relação à coleta, uso e compartilhamento de seus dados.[34]

A Lei Geral de Proteção de Dados não adotou postura muito diferente quanto à garantia do controle dos dados pelos seus titulares. Em seu art. 7º, I, a Lei elenca o consentimento como a primeira base legal para legitimar o tratamento de dados pessoais. No entanto, ainda que represente uma figura relevante em relação à proteção dos dados, enfatiza-se que o consentimento não é a única hipótese apresentada, para o tratamento de dados, no art. 7º[35], da LGPD. Apesar disso, ainda é a mais recorrente quando o assunto é assegurar o controle dos dados pessoais.

A Lei Geral de Proteção de Dados, em seu art. 5º, XII, conceitua o consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Essas adjetivações apontam que deve haver um processo de tomada de decisão, no qual o titular, por si só,

---

[33] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 60.

[34] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 114.

[35] Art. 7º. "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente [...]."

não é capaz de atingir sem a cooperação da contraparte que processa seus dados.[36] Dessa maneira, cada adjetivo constitui um elemento obrigatório para que o consentimento seja considerado válido e legítimo.

Por livre, compreende-se que o titular de dados deve manifestar uma ação espontânea, que não seja objeto de coação física ou moral. Deve-se verificar qual é o poder de escolha do cidadão para a realização ou não do tratamento de seus dados pessoais efetuado pelas empresas.[37] Por exemplo, ao tentar adentrar em determinada rede social, se o sujeito não autorizar a utilização de algum dado, como seu CPF, ele conseguirá utilizá-la normalmente ou terá seu acesso interrompido? Foi oferecida ao indivíduo a opção da não utilização dos seus dados? Essas são perguntas importantes para analisar se o consentimento pode ser adjetivado ou não como livre.

A necessidade de que o consentimento seja informado, para LGPD, decorre do fato de que o titular dos dados deve ter ao seu dispor as informações necessárias e suficientes para avaliar a situação e a forma a partir das quais seus dados serão tratados. O objetivo, aqui, é que o indivíduo tenha completa consciência sobre o destino de seus dados pessoais, de modo que a tomada de decisão, entre autorizar ou não sua utilização, seja considerada válida. As informações a serem fornecidas incluem: a quem o dado se destina; para qual finalidade será utilizado e por quanto tempo; quem terá acesso ou não aos seus dados, se eles poderão ser transmitidos a terceiros,[38] dentre outras necessárias para que o titular dos dados possa, de fato, consentir.

Além disso, a manifestação de vontade deverá ser inequívoca ou expressa. De acordo com o princípio da finalidade da LGPD, toda atividade de tratamento de dados deve ser baseada em um propósito específico e explícito. Consequentemente, todo consentimento deve ter um direcionamento, já que não se consente no vazio e de forma genérica. O ato de concordância, para qualquer atividade que utilize dados pessoais, deve ser possível de comprovação, sendo vedada a sua extração da omissão ou silêncio do titular.[39]

---

[36] BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: BIONI, Bruno Ricardo et al (coord.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 167.
[37] FRAJHOF, Isabella Zalcberg; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. In: MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 70.
[38] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2020. p. 299.
[39] BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: BIONI, Bruno Ricardo et al (coord.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 168.

Com isso, o consentimento no campo da proteção de dados refere-se a um processo que deve contar com a efetiva participação dos titulares dos dados, de modo que estes tenham liberdade de escolha para a construção e delimitação de sua esfera privada.[40] Vale ressaltar, ainda, que o consentimento figura como instrumento legitimador para que terceiros utilizem os dados pessoais, nos parâmetros estabelecidos pelo próprio titular. Ou seja, é um instrumento jurídico que torna legal uma conduta que, sem o consentimento, seria considerada ilegal.[41]

2.1 O modelo de proteção dos dados pessoais de crianças e adolescentes

Com relação à proteção de dados das crianças (pessoas até doze anos de idade incompletos), a LGPD optou pela adoção do modelo de consentimento parental como forma de efetivar tal proteção. Em seu art. 14, § 1º, o legislador estabelece que o tratamento de dados das crianças deverá ser realizado com o consentimento específico e em destaque, dado por pelo menos um dos pais ou representante legal.

Vale ressaltar que o consentimento parental, independentemente de ser realizado por mães, pais ou responsáveis legais, possui as mesmas exigências estabelecidas no art. 5º, XII, da LGPD, quais sejam: manifestação livre, informada e inequívoca para uma finalidade determinada. Acrescidas da necessidade de que o consentimento seja, também, específico e em destaque. Dessa forma, qualquer manifestação de vontade dada pelo sujeito fora dos requisitos legais, ou pela própria criança, não poderá ser admitida.[42]

Apesar de tais disposições, o legislador não menciona o adolescente (pessoas com idade entre doze e dezoito anos) no art. 14, § 1º, da LGPD. O enunciado normativo não deixa claro se o consentimento desses sujeitos deverá ser manifestado diretamente por eles, sem assistência ou representação. Com isso, abre-se a possibilidade para a interpretação de que, no caso dos adolescentes, não haveria necessidade de consentimento parental, podendo manifestá-lo pessoalmente.

---

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

[41] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil - RBDCivil,* Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. p. 93. Disponível em: https://encurtador.com.br/qzIJ5.

[42] TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. In: MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 164.

Isso porque, o instituto da representação foi criado para atender às situações de caráter patrimonial. Nessas relações, mostra-se possível dissociar o detentor do direito daquele que será responsável por exercê-lo em nome do titular. Nas situações existenciais, nas quais a proteção de dados está inserida, os atributos do exercício e da titularidade do direito devem estar sempre concentrados na mesma pessoa. Assim, retirar a capacidade do indivíduo de exercer pessoalmente o seu direito significa suprimir o próprio direito.[43]

Essa interpretação também se coaduna com o disposto no art. 17[44], do Estatuto da Criança e do Adolescente, que assegura a esses sujeitos o respeito à sua identidade e autonomia. Além disso, a Convenção Internacional sobre os Direitos das Crianças apresenta, em seu art. 12[45], dispõe acerca do dever de os Estados Partes assegurarem à criança, de acordo com suas capacidades, o direito de participação sobre todos os assuntos que lhe dizem respeito. Desse modo, deve ser oportunizada, ao adolescente, a possibilidade de exercício do seu direito à proteção de dados pessoais.

2.2 A ineficácia do consentimento nas manifestações de vontade dos adolescentes no ambiente virtual

Já não é novidade para ninguém que crianças e adolescentes estão, constantemente, conectados ao ambiente virtual. Apesar de apresentarem habilidades de uso das novas tecnologias de informação e comunicação, por vezes, não possuem condições de compreender as consequências e ameaças atreladas ao processamento de seus dados pessoais. Isso decorre do fato de que esses indivíduos vivenciam um período peculiar de desenvolvimento, tanto físico quanto cognitivo, psicológico e social.[46]

Nesse sentido, busca-se discutir a insuficiência do consentimento da forma como é obtido, enquanto instrumento para assegurar que os adolescentes tenham seu direito à proteção de dados pessoais efetivado. Para que o consentimento seja considerado válido

---

[43] TEPEDINO, Gustavo; OLIVA, Milena Donato. *Fundamentos do Direito Civil*: teoria geral do direito civil. Rio de Janeiro: Forense, 2022. p. 113.

[44] 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."

[45] Art. 12. "1. Os Estados Partes assegurarão à criança que estiver capacitada a formular seus próprios juízos o direito de expressar suas opiniões livremente sobre todos os assuntos relacionados com a criança, levando-se devidamente em consideração essas opiniões, em função da idade e maturidade da criança; 2. Com tal propósito, se proporcionará à criança, em particular, a oportunidade de ser ouvida em todo processo judicial ou administrativo que afete a mesma, quer diretamente quer por intermédio de um representante ou órgão apropriado, em conformidade com as regras processuais da legislação nacional."

[46] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020. p. 202.

e atinja o seu principal objetivo, precisa ser livre, informado e inequívoco, de modo que, para o cumprimento de cada adjetivo, seja observado um grau elevado de participação do titular.

No entanto, tem-se o que Bruno Bioni identifica como hipertrofia do consentimento. Segundo o autor, para cada adjetivo que compõe o seu conceito, deveriam existir mecanismos e ferramentas que os operacionalizassem, de maneira a dar concretude ao prometido controle dos dados pessoais.[47] Por exemplo, sabe-se que o consentimento deve ser livre. Nesse sentido, o corpo normativo de proteção de dados deveria apresentar ferramentas e diretrizes para que agentes públicos e privados pudessem concretizar tal exigência. Contudo, não é o que acontece. As adjetivações acabam figurando como *slogans*, sem aplicabilidade prática.

Apesar disso, o consentimento continua figurando como elemento obrigatório para que empresas, públicas e privadas, possam tratar os dados pessoais dos indivíduos. Desse modo, a alternativa adotada por tais entes para lidar com a demanda regulatória, no contexto virtual, tem sido a utilização das políticas de privacidade. Por meio dessa técnica contratual, os interessados em tratar dados pessoais conseguem colher o consentimento necessário dos titulares dos dados, legitimando sua conduta.[48]

No entanto, as políticas de privacidade têm representado "um descaso normativo com relação às formas pelas quais o consentimento deveria ser operacionalizado".[49] Isso porque, observa-se que a adoção dessa dinâmica retira dos usuários o poder de controle para expor suas preferências em relação à utilização de seus dados pessoais. Na maioria das vezes em que os indivíduos se deparam com a necessidade de autorizar a utilização dos seus dados, para usufruir de determinado serviço ou produto, acabam por fazê-lo diante da impossibilidade de se discutir as cláusulas ali elencadas. Assim, ou a pessoa aceita as condições estabelecidas ou ficará impossibilita de usufruir dos bens ou serviços disponíveis no ambiente virtual.[50]

---

[47] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 166.
[48] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 166.
[49] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 166.
[50] FRAJHOF, Isabella Zalcberg; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. In: MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 67.

A título de exemplo, um estudo empírico realizado pela *Global Privacy Enforcemente Network*, após a análise de mais de 1.200 aplicativos móveis de todo o mundo, concluiu que: i) 85% falham em prestar uma informação adequada sobre a coleta, o uso e o compartilhamento dos dados pessoais; ii) mais de 59% são de difícil compreensão para extração de informações básicas a respeito da utilização dos dados pessoais; iii) 1/3 coleta dados pessoais excessivos e; iv) 43% têm uma interface inadequada, seja porque a tela ou as letras são muito pequenas, seja porque traz longos textos que demandam a leitura de inúmeras páginas.

O documentário "Sujeito a Termos e Condições"[51] apresenta um interessante caso sobre a utilização das políticas de privacidade, o qual se correlaciona com os dados apresentados anteriormente. Em 2009, por um dia, *Gestation*, uma empresa britânica, colocou a seguinte cláusula em seus termos: "Ao fazer uma compra neste site, você nos concede o direito intransferível agora e para sempre, de propriedade da sua alma". Nesse único dia, sete mil clientes concordaram com a condição estabelecida.[52]

Apesar dos resultados causarem certo susto, observa-se que não é novidade o fato de que quase ninguém lê os termos de uso antes de aceitá-los. E isso também tem uma explicação: um estudo realizado pelas pesquisadoras da *Carnegie Mellon University* chegou ao resultado de que os usuários despenderiam, ao menos, 201 horas por ano para que pudessem ler todos os termos de uso dos *websites* que acessam. Esse número de horas poderia ser aumentado exponencialmente, já que a metodologia da pesquisa não incluiu as políticas de privacidade dos aplicativos móveis, tampouco dos parceiros comerciais que embutem publicidades nas plataformas.[53]

Uma pesquisa na Universidade de *Stanford* também chegou ao resultado de que 97% dos usuários pulam direto para o "li e concordo" das políticas de privacidade. Ou seja, de cada 100 indivíduos cadastrados, apenas 3 realizam a leitura. Contudo, apesar de terem lido, não é possível afirmar que esses indivíduos, verdadeiramente, sabem o que a plataforma pode ou não fazer com seus dados pessoais.[54] Todas essas constatações são

---

[51] PROFESSOR CARLOS AUGUSTO. *Terms and Conditions May Apply*. 2013. 1 vídeo (1h16m). Disponível em: https://encurtador.com.br/BNOUX. Acesso em: 24 jun. 2023.
[52] PROFESSOR CARLOS AUGUSTO. *Terms and Conditions May Apply*. 2013. 1 vídeo (1h16m). Disponível em: https://encurtador.com.br/BNOUX. Acesso em: 24 jun. 2023.
[53] MCDONALD, Aleecie M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. *Journal of Law and Policy for the Informations Society*, United Kingdom, v. 4, p. 1-22, 2008. Disponível em: https://encurtador.com.br/BDFN8.
[54] ROMERO, Luiz. Não li e concordo. *SuperInteressante*, São Paulo, 27 mar. 2018. Disponível em: https://encurtador.com.br/afuWX.

um reflexo do que Danilo Doneda chama de "paradoxo da privacidade".[55] Isso porque, o consentimento deveria ser um instrumento para garantir a participação dos titulares nas questões que envolvam seus dados e, consequentemente, assegurá-los controle. Ocorre que a atual estrutura desse direito exige que o indivíduo, primeiro, concorde em revelar seus dados para, somente depois, se valer da tutela.[56]

Esse cenário, já difícil para adultos, mostra-se ainda mais complexo para adolescentes. A adolescência é vista como um período de desenvolvimento, que se inicia aos doze anos de idade, no qual a capacidade cognitiva tende a ficar mais aguçada. [57] Assim, o seu comportamento impulsivo é bastante frequente. Nessa esteira, a rede de controle cognitivo responsável pelas funções executivas, como planejamento e autorregulação, tende a se desenvolver plenamente apenas na idade adulta. Assim, essa parcela da população acaba por identificar, em certos momentos, que recompensas imediatas parecem ter mais importância do que ganhos posteriores.[58] Por isso, estaria menos propensa a ler as políticas de privacidade, já que não enxerga um ganho imediato com tal ação.

Dessa maneira, a utilização das políticas de privacidade, estruturadas nos moldes de "tudo ou nada", para a obtenção do consentimento dos adolescentes, não garante a estes o direito à proteção de dados pessoais. Enquanto indivíduos em desenvolvimento e dotados de proteção absoluta pelo ordenamento jurídico brasileiro, devem ter a capacidade de usufruírem do ambiente virtual, de maneira que possam ser incluídos com conhecimento e repertório necessários.[59] Assim, "um clique não é suficiente para averiguar o pleno conhecimento do usuário em relação ao que ele está de fato concordando", bem como os possíveis riscos e benefícios dessa escolha.[60]

---

[55] Embora o autor utilize privacidade para intitular "parodoxo da privacidade", a ideia central empregada gira em torno do conceito e dos fundamentos da proteção dos dados pessoais.
[56] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2020. p. 294.
[57] HOF, Simone Van der. I agree... Or do I? A rigthts-bases analysis of the law on children' consente in the digital world. *Wisconsis International Law Journal,* [s.l.], v. 34, n. 2, p. 410-445, 2016. p. 126.
[58] MACEDO, Davi Manzini; PETERSEN, Circe Salcides; KOLLER, Silvia Helena. Desenvolvimento cognitivo, socioemocional e físico na adolescência e as terapias cognitivas contemporâneas. In*:* NEUFELD, Carmem Beatriz. *Terapia Cognitivo-Comportamental para adolescentes*: uma perspectiva transdiagnóstica e desenvolvimental. Porto Alegre: Artmed, 2017. p. 21.
[59] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020, p. 215.
[60] FRAJHOF, Isabella Zalcberg; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. In: MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 68.

3 *Privacy by Design*: análise de ferramentas para a proteção e participação dos adolescentes no ambiente virtual

A proteção de dados pessoais dos adolescentes, por meio do consentimento, como se extraí da interpretação do art. 14, § 1º, da Lei Geral de Proteção de Dados, mostra-se insuficiente. Com isso, busca-se discutir ferramentas que possam auxiliar esses sujeitos no exercício do controle de seus dados pessoais. Como resposta, o presente trabalho apresenta a metodologia da *Privacy by Design* enquanto ferramenta apta a criar uma melhor experiência ao usuário, de modo a garantir que o consentimento seja livre, informado e inequívoco.

Embora ainda exista uma certa ideia no imaginário das pessoas de que, de fato, a proteção em relação aos dados pessoais, após o advento das novas tecnologias, seja algo inalcançável, observa-se que essa não é a realidade na seara regulatória. Desde o início da década de 90, com a expansão mundial da Internet e, consequentemente, a circulação de informações pessoais de forma mais rápida, viu-se a necessidade de uma releitura dos institutos referentes à proteção de dados pessoais. Passou-se a discutir e defender a utilização de diferentes técnicas de regulação, de forma a permitir o desenvolvimento de um cenário mais propício à proteção dos dados pessoais frente às novas tecnologias.[61] Surge, então, a ideia da *Privacy by Design*.

Embora seja verdadeiro afirmar que a *Privacy by Design* tenha recebido um maior nível de atenção após a formulação e entrada em vigor, em 25 de maio de 2018, do *General Data Protection Regulation (GDPR)*[62], pela União Europeia, o instituto não é recente.

---

[61] MORASSUTTI, Bruno Schimitt. *Regulação de tecnologia e arquitetura de sistema:* um estudo sobre o privacy by design e a transparência aplicada a algoritmos computacionais. 2019. 182 p. Dissertação (Mestrado) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2019. p. 71.

[62] Na parte normativa do diploma do artigo 25, denominado *data protection by design and by default,* dedica os incisos 1 e 2 ao tema: 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects; 2. The controller shall implement appropriate technical and organisationalmeasures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. Original em inglês. Tradução livre: "1. Levando em conta o estado da arte, o custo da implementação e a natureza, abrangência, contexto e propósitos do processamento, bem como os riscos variáveis e a gravidade representados pelo processamento de dados para os direitos e liberdades de pessoas naturais, o controlador deverá, tanto ao tempo da determinação dos meios de processamento e ao tempo do próprio processamento, implementar medidas técnicas e organizacionais apropriadas, tal como a pseudonimização, que sejam projetadas para implementar princípios de proteção de dados, como

Seu estudo e aplicação têm origem desde a década de 80, anos antes de a proposta ser apresentada com tal nomenclatura. Cientistas da computação, preocupados com os possíveis impactos da disseminação de computadores, já defendiam a construção de modelos tecnológicos para a proteção dos dados pessoais.[63]

A consolidação sobre o tema sobreveio com a metodologia da *Privacy by Design,* proposta por Ann Cavoukian, então Comissária do *Information and Privacy Commissioner,* da província canadense de Ontário entre 1997 e 2014. A autora, nos anos de 1990, defendeu que estabelecer requisitos técnicos para a proteção de dados não é suficiente. Por exemplo, o fato de as empresas de tecnologia permitirem o anonimato para que os indivíduos naveguem nas plataformas digitais ou a criptografia que assegura a confidencialidade das comunicações não são, por si só, ferramentas que garantem a proteção dos dados pessoais.

Sua proposta é que a garantia do direito à proteção de dados deve ser trabalhada pelas empresas, públicas ou privadas, desde o início do desenvolvimento de determinado produto ou serviço, até seu efetivo funcionamento. Ou seja, o objetivo de promover o controle dos dados pessoais deve orientar as escolhas que os agentes responsáveis pelo tratamento de dados fazem. Assim, poderão adicionar em seus sistemas tecnologias e ferramentas que facilitem tal controle.

Vale destacar que Ann Cavoukian não apresenta um conceito delimitado sobre a metodologia da *Privacy by Design*. Ao invés disso, constrói sete princípios que devem ser observados por qualquer ente desenvolvedor de sistemas, os quais utilizem dados pessoais para o seu funcionamento. Isso porque, a metodologia, na concepção da autora, deve variar conforme a organização, tecnologia, público-alvo da empresa, dentre outros aspectos. Embora não exista uma única forma de implementação, observa-se que, na operacionalização dos princípios, torna-se fundamental a adoção de uma abordagem holística. O processo deve desafiar os programadores e engenheiros a pensarem criativamente sobre todos os requisitos de um sistema. De modo similar, os líderes

minimização de dados, de maneira efetiva e para integrar as garantias necessárias no processamento de modo a atingir as exigências desta regulação proteger os direitos dos titulares de dados. 2. O controlador deverá implementar medidas técnicas e organizacionais apropriadas para assegurar que, por padrão, apenas dados pessoas que sejam necessários para cada propósito específico do processamento sejam processados. Esta obrigação se aplica ao montante de dados pessoais coletados, à extensão de seu processamento, ao período de sua manutenção e à sua acessibilidade. Em particular, tais medidas devem assegurar que por padrão dados pessoais não sejam acessíveis sem a intervenção do indivíduo a um número indefinido de pessoas naturais."

[63] INTERNET ACTIVITIES BOARD. *Request for comments 1087:* ethics and the internet. [s.l]: Internet activities board, jan. 1898. Disponível em: https://bit.ly/3AiJzq3. Acesso em: 21 abr. 2023.

dessas organizações devem inovar, testar e descobrir o que funciona melhor para o seu ambiente e contexto.[64]

3.1 Princípios da *Privacy by Design*

O cerne da metodologia da *Privacy by Design* reside na aplicação dos sete princípios elaborados por Ann Cavoukian, os quais buscam assegurar que a proteção de dados pessoais seja o elemento central de qualquer produto ou serviço. Vale ressaltar que a operacionalização dos princípios depende de uma colaboração mútua: deve haver alta participação das empresas, ao oferecem aos sujeitos ferramentas necessárias para o controle dos seus dados pessoais, e dos titulares dos dados no engajamento em tais mecanismos.

3.1.1 *Proactive not Reactive; Preventative not Remedial*

O primeiro princípio é o *Proactive not Reactive; Preventative not Remedial*. Busca-se criar medidas que antecipem e previnam quaisquer incidentes de segurança que possam afetar a proteção dos dados pessoais. Ou seja, não se espera a concretização do dano para atuar com soluções. Os entes responsáveis, desde o início da concepção de determinado serviço ou produto, já devem criar ferramentas para minimizar ao máximo eventos danosos que impactem os direitos dos titulares dos dados.[65]
Sabe-se que todo serviço ou sistema digital é produto de uma série de decisões de *design* que moldam a experiência dos usuários. Assim, para a aplicação do princípio *Proactive not Reactive; Preventative not Remedial*, faz-se necessário que as empresas conheçam os riscos a que podem ser acometidos os adolescentes na internet, de modo a prevenirem eventuais danos. Na literatura, tem sido discutida a divisão dos riscos que envolvem esses sujeitos: os "4Cs".

O primeiro risco é o de conteúdo (*Content Risks*). Ocorre quando os adolescentes se envolvem ou são expostos a conteúdos potencialmente nocivos para sua idade. No geral, tratam-se de conteúdos violentos, de ódio, racistas ou discriminatórios, bem como sexuais, pornográficos ou que endossam comportamentos de riscos ou prejudiciais à saúde, como anorexia, automutilação e suicídio. Tais materiais podem ser produzidos

[64] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 9.
[65] CAVOUKIAN, Ann. *Operationalizing Privacy by Design:* a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 14.

em massa ou gerados pelos próprios usuários de determinada plataforma - incluindo os adolescentes - de modo a serem compartilhados em grande escala ou não.[66]

Há também o risco de contato (*Contact Risks*). Acontece quando o adolescente experimenta ou é alvo de uma interação potencialmente prejudicial para sua idade. O contato, na maioria das vezes, é iniciado por adultos, os quais podem ser conhecidos ou não do adolescente. A título de exemplificação, destacam-se o assédio, incluindo o sexual, a perseguição, o comportamento de ódio, o aliciamento sexual, a sextorção (que consiste em uma ameaça a partir da qual o agressor se utiliza de imagens íntimas da vítima para obrigá-la a fazer algo), dentre outros exemplos.[67]

O terceiro é o risco de conduta (*Conduct Risks*). Normalmente, esses riscos resultam das interações entre os próprios adolescentes, embora não necessariamente esses indivíduos tenham a mesma idade. Ocorre quando tais sujeitos participam ou são vítimas de condutas, potencialmente nocivas, como *bullying, sexting,* pornografia de vingança, ameaças e intimidações pelos seus pares.[68]

Por fim, tem-se o risco de contrato (*Contract Risks*). Dá-se quando os adolescentes são partes ou explorados por contratos celebrados no ambiente virtual, potencialmente prejudiciais, como jogos de azar, marketing direcionado ou inadequado para sua idade. Essas situações podem ser mediadas por meio do tratamento automatizado de dados, bem como por contratos celebrados por outras partes que envolvam um adolescente.[69]

Esses são alguns exemplos das possíveis consequências que os adolescentes podem sofrer no ambiente virtual. No entanto, a partir da compreensão de que são titulares de direitos, bem como destinatários de absoluta prioridade no ordenamento jurídico brasileiro, torna-se fundamental garantir ferramentas que possam prepará-los para lidar com tais situações. Isso porque, o objetivo deve ser proteger os adolescentes na internet, e não da internet.

---

[66] LIVINGSTONE, Sônia; MARIYA, Stoilova. The 4Cs: Classifying Online Risk to Children. CO:RE – Children Online. *Social Science Open Access Repository*, [s.v], [s.n], p. 1-14, 2021. Disponível em: https://encurtador.com.br/gySTW. p. 6-11.

[67] LIVINGSTONE, Sônia; MARIYA, Stoilova. The 4Cs: Classifying Online Risk to Children. CO:RE – Children Online. *Social Science Open Access Repository*, [s.v], [s.n], p. 1-14, 2021. Disponível em: https://encurtador.com.br/gySTW. p. 6-11.

[68] LIVINGSTONE, Sônia; MARIYA, Stoilova. The 4Cs: Classifying Online Risk to Children. CO:RE – Children Online. *Social Science Open Access Repository*, [s.v], [s.n], p. 1-14, 2021. Disponível em: https://encurtador.com.br/gySTW. p. 6-11.

[69] LIVINGSTONE, Sônia; MARIYA, Stoilova. The 4Cs: Classifying Online Risk to Children. CO:RE – Children Online. *Social Science Open Access Repository*, [s.v], [s.n], p. 1-14, 2021. Disponível em: https://encurtador.com.br/gySTW. p. 6-11.

3.1.2 *Privacy as the Default Setting*

A *Privacy as the Default Setting* é outro princípio, cujo objetivo é proporcionar que todo sistema tenha, de forma automática, a proteção de dados pessoais como padrão. Isso porque, em regra, a proteção do sujeito, no ambiente virtual, só se inicia após o aceite das políticas de privacidade. O que se busca é assegurar que, mesmo que o usuário não adote nenhuma preferência quanto à utilização dos seus dados, o sistema ou produto devem garantir que a proteção dos dados seja assegurada.[70] Para a aplicação desse princípio, as empresas devem se valer da compreensão de que, uma vez que não há manifestação de vontade do indivíduo, os dados não deverão ser utilizados ou compartilhados com terceiros.

Na aplicação da *Privacy as the Defautl Setting*, caso o adolescente opte por acessar a plataforma do *Twitter* e, em um primeiro momento, não autorize o uso dos seus dados, a empresa não deverá fazê-lo sem antes obter o consentimento livre, específico e inequívoco do titular. O objetivo, portanto, é garantir que este tenha controle dos seus dados. Quando não há manifestação de vontade do adolescente, protegê-lo significa impedir a circulação dos seus dados.

3.1.3 *Privacy Embedded into Design*

A *Privacy Embedded into Design* determina que a proteção de dados deve ser contemplada na arquitetura de determinado sistema, produto ou serviço. A garantia do controle dos dados não pode ser considerada com um mero complemento ao produto, como acontece com o consentimento que só surge no momento em que o usuário pretende usufruir de algum sistema. Desse modo, a autorização para que terceiros utilizem os dados pessoais deve ocorrer de forma específica.[71]

A autora cita alguns exemplos para que desenvolvedores de plataformas digitais possam seguir, quais sejam: i) criação de ferramentas de comunicação, em tempo real, que permitam ao usuário ser notificado sobre como seus dados estão sendo recolhidos, por quem e caso ocorra algum tipo violação; ii) fornecimento de uma plataforma simples e de fácil compreensão para que os indivíduos possam exercer esse controle e; iii) criação

[70] CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles - implementation and mapping of fair information practices. *Information and privacy commissioner of Ontario*, Canadá, v. 5. 2009. p. 2-3.
[71] CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles - implementation and mapping of fair information practices. *Information and privacy commissioner of Ontario*, Canadá, v. 5. 2009. p. 7.

de mecanismos que minimizem o acesso da plataforma aos dados, de modo que seja utilizado apenas o necessário para o funcionamento do sistema.[72]

Hoje, o direito de controle dos dados pessoais mostra-se essencial para formação da personalidade e, portanto, torna-se fundamental assegurá-lo no período da adolescência. O objetivo é fazer com que os adolescentes se tornem sujeitos plenos, capazes de estabelecer vínculos sociais e culturais, igualmente aptos a desenvolverem um posicionamento crítico em relação ao contexto no qual estão inseridos, bem como a eventuais riscos presentes no ambiente virtual.[73]

Assim, a operacionalização *Privacy Embedded into Design*, no contexto de envolvimento dos adolescentes no ambiente virtual, permite a participação ativa desses sujeitos. Enquanto indivíduos em desenvolvimento, é necessária a criação de mecanismos adequados para que o adolescente possa consentir de forma específica para a utilização de seus dados. Tais ferramentas devem capacitar os adolescentes, além de possibilitar que consigam errar e acertar, a fim de criarem sua própria identidade. [74]

3.1.4 *Full Functionality – Positive-Sum, not Zero-Sum*

O *Full Functionality – Positive-Sum, not Zero-Sum*, por sua vez, busca mitigar a ideia, comumente difundida, de que a proteção de dados sempre deve competir com os interesses das empresas. A ideia central desse princípio é de que não seja mais necessário que o titular dos dados tenha que escolher entre segurança e proteção em detrimento do ganho de funcionalidade do sistema. Ou seja, as plataformas digitais não devem limitar suas funcionalidades ao sujeito que opte por não permitir o tratamento de seus dados.[75]

O meio digital tem sido considerado um ambiente adequado para que adolescentes consigam exercer toda a gama de direito civis, políticos, culturais, econômicos e sociais - estabelecidos no ordenamento jurídico brasileiro e na Convenção Internacional sobre os Direitos das Crianças.[76] Dessa forma, caso o adolescente escolha por não compartilhar

---

[72] CAVOUKIAN, Ann. *Operationalizing Privacy by Design:* a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 31.
[73] HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020, p. 218.
[74] FERNANDES, Elora. Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANDP. In: LATERÇA, Priscilla; Fernades, Eloara; TEFFÉ, Chiara de; BRANCO, Sérgio. *Privacidade e proteção de dados de crianças e adolescentes*. Rio de Janeiro: Obliq, 2021. p. 203.
[75] CAVOUKIAN, Ann. *Operationalizing Privacy by Design:* a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 34.
[76] COMITÊ DOS DIREITOS DA CRIANÇAS DA ONU. Comentário Geral n. 25 sobre Direitos da Criança em relação ao ambiente digital. Nova York: ONU, 2021. p. 1.

seus dados, as empresas não devem impedi-lo de utilizar as plataformas digitais. Excluí-los dos serviços online, ou não permitir a sua participação de acordo com sua condição peculiar de desenvolvimento, impossibilitam o exercício de diversos direitos, como a proteção dos dados pessoais.[77]

3.1.5 *End-to-End Security – Full Lifecycle Protection*

O quinto princípio é o *End-to-End Security – Full Lifecycle Protection*. Para a autora, a empresa que adota a *Privacy by Design* deve incorporar aos seus produtos e serviços a proteção do dado pessoal, do ponto de vista técnico, em todas as fases do ciclo de vida do dado. Ou seja, a garantia da segurança do dado deve ocorrer quando este está em repouso, em trânsito, durante sua utilização e após sua destruição.[78]

A autora utiliza como exemplo, para a operacionalização deste princípio, a ferramenta da encriptação nos ambientes em que há alta disponibilidade de dados, como o ambiente hospitalar. Tal mecanismo busca codificar os dados, de forma que apenas pessoas autorizadas tenham acesso aos códigos gerados. Assim, garante-se o livre fluxo dos dados entre os prestadores de serviços autorizados e, ao mesmo tempo, os dados permanecem inacessíveis a qualquer outra pessoa não autorizada, preservando a segurança do dado.[79] Esse é apenas um exemplo dentre as possíveis formas de aplicação do princípio. Nesse sentido, a sua operacionalização garante que os dados dos adolescentes não circulem, em nenhum momento, de forma indevida na sociedade.

3.1.6 *Visibility and Transparency – Keep it Open*

O sexto princípio é o da *Visibility and Transparency – Keep it Open*. A sua implementação pelas empresas emerge da necessidade do constante diálogo entre as organizações e os titulares dos dados, de modo a criar um ambiente de confiança entre os sujeitos. As políticas e os procedimentos das empresas devem ser levados ao conhecimento dos usuários de forma clara, simples e de fácil compreensão, para que haja uma tomada de decisão informada.[80] Isso significa detalhar como o tratamento dos

---

[77] HOF, Simone Van Der; LIEVENS Eva. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. *Communications Law*, London, v. 23, n. 1, p. 1-25, oct, 2017. p. 3

[78] CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles - implementation and mapping of fair information practices. *Information and privacy commissioner of Ontario*, Canadá, v. 5. 2009. p. 4.

[79] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 41.

[80] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 45.

dados ocorre, os mecanismos que serão utilizados quando presentes falhas na proteção dos dados, dentre outros aspectos.

Ann Cavoukian, assim como o posicionamento defendido neste trabalho, reconhece que a abordagem prevalente de aviso e escolha em relação à proteção dos dados pessoais, por meio das políticas de privacidade, é insuficiente e não empodera o indivíduo. Para a autora, raramente os titulares dos dados leem os longos termos de uso, baseados no "tudo ou nada".[81]

Os adolescentes, enquanto titulares de direitos, também devem ter assegurada a possibilidade de compreender como seus dados estão sendo utilizados, por quem e em quais situações. Para além disso, a operacionalização deste princípio deve oportunizar que os adolescentes: i) entendam como o ambiente virtual funciona, em termos de tecnologia, economia e negócios; ii) revejam a sua decisão e alterem quando achar necessário; iii) manifestem sua vontade, de forma específica, a respeito da utilização de dados sensíveis; iv) reconheçam os perigos de se autorizar o uso dos dados sensíveis; e v) recebam as indicações dos riscos associados a cada decisão tomada pelo sujeito. No entanto, faz-se necessária uma abordagem flexível, a qual reconheça as diferenças entre os adolescentes, em seus diversos graus de desenvolvimento.[82] Isso porque, aquilo que funciona para um adolescente de treze anos, por exemplo, pode não ser suficiente para outro da mesma idade.

3.1.7 *Respect for User – Keep it User-Centric*

Por fim, tem-se o princípio do *Respect for User Privacy – Keep it User-Centric*. Para sua operacionalização, exige-se que os interesses e as necessidades dos titulares dos dados estejam no cerne do desenvolvimento dos serviços e produtos das empresas - acima, inclusive, dos interesses econômicos. As empresas devem criar mecanismos para que os usuários adquiram conhecimento sobre as operações e o funcionamento de qualquer tecnologia ou sistema com os quais estejam interagindo, de preferência em tempo

[81] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 45.
[82] BITTENCOURT, Izabella Alves Jorge. Além do consentimento parental: o design como ferramenta da garantia de direitos de privacidade e proteção de dados de crianças no mundo online. *In*: PEREIRA, Fábio Queiroz; LARA, Marina Alves (orgs.). *Os direitos da personalidade na sociedade em rede*. Belo Horizonte: Dialética, 2023. p. 211.

real.[83][84] O principal objetivo é capacitar os sujeitos para desempenharem um papel ativo no gerenciamento de seus dados pessoais.

Desse modo, toda a arquitetura do sistema ou produto deve ser centrada no usuário. Assim, ao lidar com adolescentes, as empresas devem criar ferramentas direcionadas para atender às demandas deste público. Assim, busca-se capacitá-los frente aos riscos e benefícios da Internet. Inclusive, o Comentário Geral n. 25 sobre os Direitos das Crianças em Relação ao Ambiente Digital, da ONU, é contundente ao informar que tanto as políticas públicas, quanto os produtos e serviços digitais devem ser pensados para garantir o envolvimento dos adolescentes no ambiente virtual, bem como assegurar seu acesso seguro.[85]

3.1.8 O que pode ser extraído da aplicação dos princípios da *Privacy by Design?*

A partir da compreensão dos princípios, reitera-se a constatação já feita de que não existe um conceito fechado de como deve ocorrer a implementação da *Privacy by Design*. A aplicação e operacionalização desses princípios, desde a concepção de determinado produto ou serviço, de forma sólida e sistemática, ajudam a promover um ambiente no qual os riscos à proteção de dados dos indivíduos são minimizados ou impedidos de ocorrer. Além de estimular: i) a definição clara dos objetivos com a proteção dos dados; ii) metodologias sistemáticas e verificáveis; iii) soluções práticas e resultados demonstráveis; iv) visão, criatividade e inovação.[86]

Além disso, observa-se que a implementação da *Privacy by Design* mostra-se fundamental em relação a três aspectos. Primeiro, as empresas conseguem obter um consentimento mais autêntico quando implementam os princípios discutidos em sua estrutura de funcionamento. Segundo, para a concretização da maioria deles, exige-se alta participação dos indivíduos, o que coaduna com a ideia de o sujeito ter o direito de controlar seus dados. Terceiro, as empresas, enquanto responsáveis pela aplicação dos princípios, passam a ter mais responsabilidades quanto ao tratamento dos dados

[83] CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles - implementation and mapping of fair information practices. *Information and privacy commissioner of Ontario*, Canadá, v. 5. 2009. p. 7.
[84] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 50.
[85] COMITÊ DOS DIREITOS DA CRIANÇAS DA ONU. *Comentário Geral n. 25 sobre Direitos da Criança em relação ao ambiente digital*. Nova York: ONU, 2021. Disponível em: https://encurtador.com.br/fyzET. p. 4.
[86] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 9.

pessoais. Isso porque, o consentimento, da forma como é obtido, deposita todo o ônus no titular dos dados: se manifesta sua vontade, qualquer consequência posterior deverá ser suportada.

No Brasil, a Lei Geral de Proteção de Dados, sob influência do GDPR, já adotou a ideia da metodologia da *Privacy by Design,* ao determinar que as medidas de segurança dos dados sejam observadas desde a fase de concepção do produto ou serviço até a sua execução. Em seu art. 46, o legislador dispôs:

> 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*.

Embora o artigo 46, LGPD, não seja voltado à proteção dos dados pessoais dos adolescentes, entende-se que essa regulamentação pode impulsionar sua proteção quando bem implementadas e voltadas a este fim. A adoção de tal instituto pode representar uma abordagem abrangente da proteção de dados pessoais de adolescentes, já que não possui como objetivo principal apenas a proteção, mas também a participação e desenvolvimento desses indivíduos.[87]

Considerações finais

Hoje, adolescentes estão constantemente inseridos no ambiente digital, seja para realizar trabalhos escolares, estabelecerem relações com seus pares ou utilizarem redes sociais. A dissociação entre esses sujeitos e a internet torna-se tarefa praticamente impossível. No entanto, como foi possível identificar neste trabalho, o meio virtual não foi pensado

[87] HOF, Simone Van Der; LIEVENS, Eva. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. *Communications Law*, London, v. 23, n. 1, p. 1-26, oct, 2017. p. 3.

e desenhado para atender às necessidades desta parcela da população, já que a experiência virtual de adolescentes e adultos se mostra muito semelhante.

A partir dessa premissa e da identificação da insuficiência da proteção dos dados pessoais dos adolescentes, este trabalho buscou demonstrar que a adoção da metodologia da *Privacy by Design* pelas empresas, públicas e privadas, apresenta-se como um expediente adequado para a sua proteção no ambiente digital.

Como discutido, os serviços tecnológicos estão cada vez mais sofisticados e, consequentemente, a atividade de tratamento de dados pessoais passa a impactar diretamente a vida das pessoas. Contudo, o controle sobre os próprios dados, já difícil para adultos, torna-se ainda mais complexo quando exercido por adolescentes. No entanto, é importante ter em mente que os dados pessoais destes também são colhidos e utilizados por empresas de tecnologia.

Embora a Lei Geral de Proteção de Dados apresente avanços significativos, torna-se necessário reconhecer que, em relação à proteção de dados dos adolescentes, o diploma legal ainda apresenta incongruências. O artigo 14, § 1º adota o modelo de consentimento parental para o tratamento de dados de crianças, mas não menciona o adolescente no dispositivo. Interpreta-se, assim, que o legislador teria reconhecido que esses indivíduos podem manifestar, pessoalmente, o seu consentimento - reforçando tal mecanismo como meio para garantir aos indivíduos o controle de seus dados.

No entanto, na maioria das vezes em que os indivíduos se deparam com a necessidade de autorizar a utilização de seus dados, para usufruírem de determinado produto ou serviço, o consentimento é obtido pelas empresas por meio das políticas de privacidade. Esse mecanismo tem se mostrado ineficaz nas manifestações de vontade dos adolescentes no ambiente virtual, haja vista que ainda estão em fase de desenvolvimento. De tal modo, essa ferramenta não consegue garantir-lhes o exercício do direito de participação efetiva, bem como o exercício de sua autonomia de acordo com suas capacidades.

Mais do que protegê-los, é preciso que a eles seja oportunizada a efetividade do seu direito à proteção de dados. Assim, adolescentes necessitam de ambientes virtuais adequados ao seu desenvolvimento, com o objetivo de criarem sua própria identidade. Por isso, a *Privacy by Design* apresenta-se como um expediente adequado. Ann

Cavoukian não elabora um conceito definido do que seja a metodologia, mas elenca sete princípios norteadores que devem ser seguidos pelas empresas.

Conclui-se que as empresas, públicas ou privadas, ao aplicarem os princípios da *Privavy by Design,* fazem com que os usuários se envolvam mais no controle de seus dados pessoais. Além disso, uma vez aplicados tais princípios, de forma sólida e sistemática, o consentimento obtido se torna um meio de proteção mais autêntico, visto que passa a atender aos critérios exigidos pela LGPD – afastando-se da estrutura de "tudo ou nada". Ademais, as empresas também passam a ter maiores responsabilidades em relação ao tratamento de dados. Será papel dessas organizações, para uma boa operacionalização de todos os princípios, buscar equipes multidisciplinares, as quais consigam entender o público de determinado serviço ou produto. Dessa forma, importa que a proteção dos dados pessoais seja desenvolvida à luz das individualidades de seus usuários.

Referências bibliográficas

5RIGHTS FOUNDATION. The risks: Content, Contact, Conduct and Contract. *Risky-by-Design*, [s.l.], 2020. Disponível em: https://www.riskyby.design/risks. Acesso em: 20 jun. 2023.

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

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In*:* BIONI, Bruno Ricardo et al (coord.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020.

BITTENCOURT, Izabella Alves Jorge. Além do consentimento parental: o design como ferramenta da garantia de direitos de privacidade e proteção de dados de crianças no mundo online. In: PEREIRA, Fábio Queiroz; LARA, Marina Alves (orgs.). *Os direitos da personalidade na sociedade em rede*. Belo Horizonte: Dialética, 2023.

BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *Cadernos Adenauer***,** Rio de Janeiro, v. 3, n. 1, p. 113-135, 2019.

CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012.

CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles - implementation and mapping of fair information practices. *Information and privacy commissioner of Ontario*, Canadá, v. 5, 2009.

COMITÊ DOS DIREITOS DA CRIANÇAS DA ONU. *Comentário Geral n. 25 sobre Direitos da Criança em relação ao ambiente digital*. Nova York: ONU, 2021. Disponível em: https://encurtador.com.br/fyzET.

DATA protection laws of the world. Disponível em: https://encurtador.com.br/dkJU3.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2020.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno Ricardo et al. (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020.

EBELIN, Fernando Büscher von Teschenhausen. *Direitos da criança na sociedade da informação*. São Paulo: Revista dos Tribunais, 2020.

FERNANDES, Elora. Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANDP. In*:* LATERÇA, Priscilla; Fernades, Eloara; TEFFÉ, Chiara de; BRANCO, Sérgio. *Privacidade e proteção de dados de crianças e adolescentes*. Instituto de Tecnologia e Sociedade do Rio de Janeiro: Obliq, 2021.

FRAJHOF, Isabella Zalcberg; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. In*:* MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

GLOBAL survey finds 85% of mobile apps fail to provide basic privacy information. *WiredGov*, Manchester, 14 sep. 2014. Disponível em: https://bit.ly/3koO8en.

GREENLEAF, Graham; COTTIER, Bertil. 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business Internacional Report*, [s.l.], v. 163, [s.n], p. 1-5, maio, 2020. Disponível em: https://encurtador.com.br/gloxS.

HARTUNG, Pedro; HENRIQUES, Isabella; PITA, Marina. A proteção de dados pessoais de crianças e adolescentes. In*:* BIONI, Bruno Ricardo et al (orgs.). *Tratado de Proteção de Dados Pessoais*. São Paulo: Forense, 2020.

HOF, Simone Van der. I agree... Or do I? A rigthts-bases analysis of the law on children' consente in the digital world. *Wisconsis International Law Journal*, [s.l.], v. 34, n. 2, p. 410-445, 2016.

HOF, Simone Van Der; LIEVENS, Eva. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. *Communications Law,* London, v. 23, n. 1, p. 1-26, oct, 2017.

INTERNET ACTIVITIES BOARD. *Request for comments 1087*: ethics and the internet. [s.l]: Internet activities board, jan. 1898. Disponível em: https://bit.ly/3AiJzq3. Acesso em: 21 abr. 2023.

LIVINGSTONE, Sônia; MARIYA, Stoilova. The 4Cs: Classifying Online Risk to Children. CO:RE – Children Online. *Social Science Open Access Repository*, [s.v], [s.n], p. 1-14, 2021. Disponível em: https://encurtador.com.br/gySTW.

MACEDO, Davi Manzini; PETERSEN, Circe Salcides; KOLLER, Silvia Helena. Desenvolvimento cognitivo, socioemocional e físico na adolescência e as terapias cognitivas contemporâneas. In: NEUFELD, Carmem Beatriz. *Terapia Cognitivo-Comportamental para adolescentes*: uma perspectiva transdiagnóstica e desenvolvimental. Porto Alegre: Artmed, 2017.

MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. *Revista Eletrônica Direito e Política*, Itajaí, v. 15, n. 3, p. 955-984, 2020. Disponível em: https://encurtador.com.br/cdMR5.

MCDONALD, Aleecie M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. *Journal of Law and Policy for the Informations Society*, United Kingdom, v. 4, p. 1-22, 2008. Disponível em: https://encurtador.com.br/BDFN8.

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

MENEZES, Joyceane Bezerra de; MORAES, Maria Celina Bodin de. Autoridade parental e privacidade do filho menor: o desafio de cuidar para emancipar. *Revista Novos Estudos Jurídicos*, Itajaí, v. 20, n. 2, p. 501-532 jul. 2015. Disponível em: https://encurtador.com.br/msLT7.

MORASSUTTI, Bruno Schimitt. *Regulação de tecnologia e arquitetura de sistema:* um estudo sobre o privacy by design e a transparência aplicada a algoritmos computacionais. 2019. 182 p. Dissertação (Mestrado) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2019.

NÚCLEO de informação e coordenação do ponto BR. *Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil:* TIC Kids Online Brasil 2019. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

PROFESSOR CARLOS AUGUSTO. *Terms and Conditions May Apply*, 2013. 1 vídeo (1h16m). Disponível em: https://encurtador.com.br/BNOUX. Acesso em: 24 jun. 2023.

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

ROMERO, Luiz. Não li e concordo. *SuperInteressante*, São Paulo, 27 mar. 2018. Disponível em: https://encurtador.com.br/afuWX. Acesso em: 24 jun. 2023.

RUBINSTEIN, Ira S. Regulating privacy by design. *Berkley Technology Law Journal*, California, v. 26, n. 3, p. 1409-1456, 2011.

SCHARTUM, Dag Wiese. Making privacy by design operative. *International Journal of Law and Informations Technology*, [s.l], v. 24, n. 2, p. 151-175, fev. 2016.

TARGET: entenda como a loja monitora o comportamento do consumidor. *Traycorp,* São Paulo, mar. 2020. Disponível em: https://bit.ly/3v6JB09.

TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. In: MULLHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélago, 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil - RBDCivil,* Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. Disponível em: https://encurtador.com.br/qzIJ5.

TIC Kids Online Brasil 2021: 78% das crianças e adolescentes conectados usam redes sociais. *Cetic.br*, São Paulo, 16 ago. 2022. Disponível em: https://bit.ly/3ksqdKQ.