



A PROTEÇÃO DE DADOS PESSOAIS DAS CRIANÇAS E ADOLESCENTES NO ÂMBITO DA EDUCAÇÃO ONLINE

Ingrid Dias da Fonseca¹

Maria Beatriz Torquato Rego²

RESUMO

A presente pesquisa tem como cerne a análise da violação a dados pessoais de crianças e adolescentes dentro do contexto da educação online. Para tanto, utiliza-se o método hipotético-dedutivo, testando a hipótese de que o ensino à distância e a hiperconexão nas redes aumentam as chances de possíveis violações. Desse modo, com a projeção de cenários, além das possíveis repercussões no futuro, concluiu-se que o mau aproveitamento desses dados pode gerar danos, como por exemplo no âmbito profissional, e para obstar tais efeitos é imprescindível a adoção de determinadas medidas de proteção, tanto pelas instituições de ensino como pelos responsáveis.

Palavras-chave: Educação online. Proteção de dados pessoais. Crianças e adolescentes.

1 INTRODUÇÃO

¹ Advogada, pós-graduanda em Direito Processual Civil pelo Instituto Damásio de Direito (Faculdade IBMEC São Paulo) e membro da Comissão de Direito Digital e Estudos Aplicados da OAB/RN.

² Advogada, pós-graduanda em Direito Constitucional pela Academia Brasileira de Direito Constitucional (ABDConst) e membro da Comissão de Direito Digital e Estudos Aplicados da OAB/RN.

Recentemente, com o surgimento da pandemia do Covid-19 e a adoção de medidas de combate à doença, algumas mudanças ocorreram, e uma delas foi a utilização do ensino online. A educação à distância foi uma novidade, em especial para as crianças e adolescentes, até então acostumados com aulas e interação presencial. Diante desse novo ambiente - o virtual -, há a intensificação de uma preocupação: a proteção dos dados pessoais dessa faixa etária.

Dessa forma, a problemática é desenvolvida a partir da necessidade de se entender como a educação online pode influenciar na proteção de dados pessoais desse grupo alvo.

A presente pesquisa tem como objetivo geral investigar de que forma as crianças e adolescentes podem ter seus dados pessoais violados dentro do contexto da educação online, e consequente potencialização do acesso à informação; bem como projetar os possíveis efeitos dessas violações.

Os objetivos específicos têm o propósito de abordar o cenário da pandemia mundial da Covid-19 e os avanços tecnológicos, aliados à potencialização da educação online e a necessidade de adequação à Lei Geral de Proteção de Dados Pessoais; demonstrar e reconhecer a vulnerabilidade de crianças e adolescentes, bem como projetar cenários da educação online/acesso à informação em que podem ocorrer violações; como também apresentar consequências e desenvolver soluções.

Para tanto, o estudo analisou primariamente a conjuntura e regulamentação da educação online no contexto da pandemia, em especial a maior exposição na internet dos menores de idade, e o tratamento de seus dados pessoais.

Em seguida, abordou-se o tema da proteção de dados pessoais das crianças e adolescentes nas legislações nacionais e estrangeiras. No Brasil, o cerne foi a Lei Geral de Proteção de Dados Pessoais. Enquanto, no âmbito da regulamentação internacional, teve como referência tanto a *General Data Protection Regulation*³ (União Europeia), como o *Children's Online Privacy Protection Act*⁴ (Estados Unidos). Após esse estudo, demonstrou-se também a vulnerabilidade do grupo em questão.

Ato contínuo, foram apresentados cenários da educação online em que a possibilidade de violação aos dados pessoais mostra-se evidente, além das consequências que um potencial vazamento pode acarretar para o público infantojuvenil.

³ Em tradução livre do inglês para o português: Regulamento Geral de Proteção de dados pessoais.

⁴ Em tradução livre do inglês para o português: Lei de Proteção da Privacidade Online Infantil.

Por fim, soluções e sugestões para viabilizar a proteção da privacidade e combater o mau uso dos dados pessoais foram apontadas com o intuito de reduzir as chances de violação aos dados.

Trata-se de uma pesquisa científica de cunho descritivo, em que visa expor e interpretar os fatos relacionados à educação online e acesso à informação das crianças e adolescentes. Já o método adotado é o hipotético-dedutivo, uma vez que testa a hipótese de que o ensino à distância e a hiperconexão nas redes aumentam as chances de possíveis violações a dados pessoais. Enquanto as técnicas de pesquisa utilizadas envolvem o estudo da lei, jurisprudência, artigos científicos, notícias e doutrina.

Assim sendo, o tema deste artigo científico tem relevância pois proporciona o entendimento de aspectos inerentes ao uso das tecnologias e dos dados pessoais de um grupo vulnerável que está, cada dia mais, conectado sem a supervisão ou auxílio de responsáveis.

2 COVID-19, EDUCAÇÃO ONLINE E PROTEÇÃO DE DADOS PESSOAIS

Na contemporaneidade, o tratamento de dados pessoais tem ocupado um papel de notoriedade em nível mundial e nacional. A relevância da referida temática foi intensificada com o surgimento da pandemia da Covid-19. Desde então, a tecnologia tem sido utilizada como uma aliada indispensável no combate à doença.

Todavia, essa conjuntura tem ensejando questionamentos acerca da proteção à privacidade dos dados pessoais e do potencial mau uso ou até mesmo violação dos dados coletados. Uma das situações em que esse cenário preocupa é na educação online de crianças e adolescentes.

Isso acontece porque diante da impossibilidade de contato físico e de aglomerações, foram tomadas diversas medidas de prevenção ao coronavírus. Uma delas foi a suspensão das aulas presenciais em todo o país. Em 17 de março de 2020, o Ministério da Educação (MEC), publicou a primeira portaria tratando da substituição das aulas presenciais por aulas em meios digitais enquanto durar a situação de pandemia do Novo Coronavírus – COVID-19. O período de autorização era de até 30 (trinta) dias, porém, prorrogáveis. Ato contínuo, foram publicadas outras portarias, quais sejam, a n.º 345/2020 e a n.º 473/2020, prorrogando o primeiro prazo estabelecido.

A portaria mais recente acerca do assunto supramencionado é a nº 544/2020, que estende a autorização, em caráter excepcional, das atividades letivas online até 31 de dezembro de 2020.

Desse modo, é evidente que o ensino online se tornou protagonista na educação em 2020. A escola e os alunos tiveram que fazer essa transição para o mundo digital de forma abrupta e inovadora. A implementação da educação à distância para crianças e adolescentes foi um desafio por se tratar de uma modalidade de ensino totalmente nova para essa faixa etária e em um período atípico.

Os professores tiveram que se reinventar e usar a tecnologia como solução para a manutenção das aulas. Para tanto, plataformas como *Zoom*, *YouTube* e *Google Meeting* têm sido utilizadas com essa finalidade. A necessidade de adaptação às novas ferramentas foi tamanha que surgiram cursos voltados para essa temática no intuito de auxiliar os professores nessa empreitada, a exemplo do promovido em conjunto pelo Facebook e a ONG Nova Escola⁵. Iniciativas como essa buscam minimizar a dificuldade de transição para o mundo virtual.

Essa migração das atividades escolares integralmente para o espaço digital também foi uma mudança intensa para os alunos, já que fez com que as crianças e adolescentes ficassem ainda mais conectadas ao celular ou computador, haja vista que a rotina de aulas passou a ser online⁶. Dentro dessa conjuntura, há um aspecto que preocupa: a maior exposição na internet dos menores de 18 anos, em especial o tratamento dos dados pessoais dessa faixa etária.

Nessa perspectiva, é importante destacar que os dados possuem tanta importância para o atual cenário de inovações na Indústria 4.0, que especialistas já os consideram o novo petróleo do mundo⁷. Diariamente eles são capturados, interpretados e utilizados para os mais diversos fins. Dentro desta leitura massiva, também se encontram dos dados pessoais, cujo compartilhamento compreende uma preocupante banalização, pois a sociedade não foi educada para protegê-los, nem para evitar que sejam os produtos principais em uma relação de consumo.

Diante da indispensabilidade e urgência na proteção de dados pessoais, surge no Brasil a Lei Geral de Proteção de Dados Pessoais, com o objetivo de proteger os direitos fundamentais

⁵ VALENTE, Jonas. Plataformas e instituições firmam parcerias para ensino a distância. **Agência Brasil**, 01 abr. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/educacao/noticia/2020-03/plataformas-e-instituicoes-firmam-parcerias-para-ensino-distancia>. Acesso em 25. ago. 2020.

⁶ GOMES, Bianca. Estudo em casa traz questões para pais e escolas. **Estadão**, São Paulo, 05 abr.2020. Disponível em: <https://www.estadao.com.br/infograficos/saude,seu-filho-esta-online,1087061>. Acesso em 25. ago. 2020.

⁷ Tradução livre para o significado original: “*Data is the new oil*”, frase criada por Clive Humby, matemático londrino especialista em ciência de dados.

de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º).

2.1 Tratamento de dados pessoais das crianças e adolescentes

As crianças e adolescentes do século XXI se encontram em um contexto de alta velocidade nas mudanças sociais e ascensão do mundo digital. Elas são formadas pela Geração Z (nascidos entre 1998 e 2009), caracterizada por usuários acostumados com a internet e confortáveis com os desenvolvimentos tecnológicos, como também pela Geração Alpha (nascidos a partir de 2010), que, conectados desde o berço, representam a “primeira geração digital”⁸.

Crianças e adolescentes são usuários leais, a maioria dependentes da internet e suas ferramentas, de maneira que é impossível separá-los, pois eles já nasceram conectados. Este grupo está habituado à prática diária do compartilhamento de dados pessoais como chave de acesso para plataformas virtuais (aplicativos, redes sociais, jogos, portais do aluno), bem como para a manutenção de dispositivos.

O crescimento exponencial do fluxo de dados na economia digital desperta anseios sociais, pois não existem dados insignificantes no atual contexto tecnológico. Todos os indivíduos têm o direito de autodeterminar o compartilhamento de seus dados, e diante do *status* de pessoas em situação peculiar de desenvolvimento, cabe à família, à sociedade e ao Estado assegurar a proteção das informações relacionadas a crianças e adolescentes (art. 227, da Constituição Federal de 1988).

Nesse sentido, a Lei Geral de Proteção de Dados prevê um dispositivo (art. 14) destinado exclusivamente ao tratamento de dados pessoais deste grupo, o qual deve ser realizado de acordo com o princípio do melhor interesse. Este metaprincípio estabelece a prioridade absoluta quando o assunto diz respeito a crianças e adolescentes, compreendendo o “exame de razoabilidade quanto à aplicação de uma ou outra norma jurídica, ou quanto à não aplicação de normas positivas, sempre com o objetivo de garantia do melhor interesse da pessoa em desenvolvimento” (ROSSATO; LÉPORE; CUNHA, 2017, p. 68).

⁸ BORRULL, Alba Solé. O que é a geração alfa, a 1ª a ser 100% digital. **BBC News Brasil**, 29 maio 2019. Disponível em: <https://www.bbc.com/portuguese/geral-48438661#:~:text=Foi%20a%20vez%20ent%C3%A3o%20da,de%20comunica%C3%A7%C3%A3o%20e%20tecnologias%20digitais.&text=Ela%20ser%C3%A1%20a%20primeira%20gera%C3%A7%C3%A3o,bem%20distantes%20de%20sua%20realidade>. Acesso em 03 set. 2020.

O § 1º, do art. 14, dispõe que 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. Todos os esforços devem ser empreendidos para atestar que o consentimento foi atendido (COTS; OLIVEIRA, 2020, p. 121), sendo dever dos pais ou responsáveis legais realizar este ato com autoridade, responsabilidade e seriedade.

O consentimento é hipótese de tratamento de dados pessoais (art. 11, inciso I, da Lei Geral de Proteção de Dados) e deve ser fornecido de modo livre (sem má-fé ou coerção), informado (com elementos destinados a total compreensão) e inequívoco (informações precisas). Não existe consentimento tácito, pois o titular precisa demonstrar a sua concessão em uma ação afirmativa. Além disso, para cumprir o princípio da finalidade (art. 6º, I, da Lei Geral de Proteção de Dados) é necessário especificar qual o propósito daquele tratamento, bem como se haverá o compartilhamento com terceiros interessados.

Dessa forma, as crianças são amparadas pela supervisão de seus responsáveis, que, teoricamente, possuem uma maior capacidade de discernimento e experiência para orientar no uso da internet. Isso diminui a incidência do “menor abandonado digital”, sujeitos a abordagens de estranhos e a todo tipo de situação, já que a internet é a maior rua do planeta, a rua digital⁹.

Contudo, a lei não previu o consentimento dos pais ou responsáveis legais para o tratamento de dados dos adolescentes e essa circunstância acaba indo de encontro ao Código Civil, ao Estatuto da Criança e do Adolescente, e conseqüentemente à Constituição Federal.

O Código Civil (arts. 3º e 4º, inciso I), prevê que são absolutamente incapazes os menores de 16 (dezesseis) anos, o responsável substitui o menor na tomada de decisões; e relativamente incapazes os maiores de 16 (dezesseis) e menores de 18 (dezoito) anos, o responsável apenas verifica a regularidade e a validade da decisão tomada pelo menor. Enquanto o Estatuto da Criança e do Adolescente (art. 2º) considera criança a pessoa até 12 (doze) anos de idade incompletos e adolescente aquela entre 12 (doze) e 18 (dezoito) anos de idade.

Percebe-se que o Código Civil tomou precaução em limitar os atos da vida civil dos menores, assim como o Estatuto da Criança e do Adolescente especificou que tanto à criança, como ao adolescente é garantido o melhor interesse. Inclusive, a Constituição Federal de 1988

⁹ PINHEIRO, Patrícia Peck. *A LGPD aplicada ao cenário da educação*. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/educacao-lgpd#:~:text=Logo%2C%20crian%C3%A7a%20n%C3%A3o%20pode%20ficar,o%20artigo%2018%20do%20ECA. Acesso em 10 ago. 2020.>

foi explícita ao citar ambos e assegurar a proteção integral (art. 227, da Constituição Federal de 1988).

A Lei Geral de Proteção de Dados, então, descuidou dos adolescentes ao dar autonomia para dispor sobre seus dados pessoais sem a supervisão de um responsável. Tal situação pode ser considerada como imprudente, visto que eles se encontram na fase mais vulnerável do desenvolvimento humano.

Por isso, o consentimento dos pais ou responsáveis legais deve ser estendido aos adolescentes como forma de orientar o acesso à informação. Sendo esta regulamentação de incumbência da Autoridade Nacional de Proteção de Dados (ANPD), já que a lei foi omissa.

Importante destacar que há a prescindibilidade do consentimento quando a coleta de dados pessoais de crianças é necessária para a sua proteção ou para contatar os pais ou o responsável legal, neste caso as informações não podem ser armazenadas e só devem ser utilizadas uma única vez (art. 14, § 3º, da Lei Geral de Proteção de Dados). Mas em nenhuma ocasião os dados poderão ser repassados a terceiros sem o devido consentimento.

A hipótese do consentimento é apenas uma das bases legais para o tratamento de dados pessoais, existem outras previstas no art. 11, da Lei Geral de Proteção de Dados, que apesar do silêncio da lei, se mantêm vigentes para o tratamento dos dados pessoais das crianças e adolescentes. Com exceção do legítimo interesse do controlador e da proteção ao crédito, como defende Cots e Oliveira (2020, p. 122).

Dando continuidade, o § 2º, do art. 14, da Lei Geral de Proteção de Dados, assegura que os controladores (pessoa natural ou jurídica a quem compete as decisões referentes ao tratamento de dados pessoais) deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos previstos na lei. Outrossim, o § 4º, reconhece que não devem ser fornecidas informações pessoais além das estritamente necessárias à atividade.

Estes dispositivos possuem amparo nos princípios previstos no art. 6º, da Lei Geral de Proteção de Dados (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas), que são premissas gerais sobre o tratamento de dados pessoais.

A lei também garante que as informações sobre o tratamento de dados devem ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com o uso de audiovisuais quando adequado (art. 14, § 4º, da Lei Geral de Proteção de Dados). O controlador deve realizar todos

os esforços razoáveis para verificar que o consentimento foi dado pelo responsável da criança (art. 14, § 5º, da Lei Geral de Proteção de Dados).

Para isto, dois conceitos inovadores que afirmam a ética e a transparência são o de *Privacy by Design*¹⁰, que coloca a proteção de dados pessoais como o centro de qualquer projeto na empresa, compreendendo todas as etapas do processo de desenvolvimento; e o de *Privacy by Default*¹¹, que atua no produto ou serviço já lançados ao público em uma configuração de privacidade no modo mais restrito possível por padrão, no qual o usuário só libera o acesso à coleta de mais informações caso julgue necessário¹².

Essa metodologia estimula a cultura da proteção de dados. Podendo ser aplicada a crianças e adolescentes a partir da adoção de um processo diferenciado voltado aos que se encontram em situação de vulnerabilidade e necessitam, tanto de mecanismos mais precisos e dinâmicos para o consentimento, como de um tratamento digno.

Enfim, o tratamento de dados pessoais do menor é assunto delicado e prioritário. É dever da família, da sociedade e do Estado empreender todos os esforços para proteger aqueles que ainda não conseguem, por si só, autodeterminar suas informações. O mundo e, conseqüentemente, o direito se adaptarão a essa nova realidade digital, com responsabilidade e iniciativas conscientes.

2.2 Comparativo entre legislações internacionais

Em um comparativo com legislações internacionais, percebe-se que não só o Brasil, mas o mundo está em busca de regulamentar e fortalecer o tratamento de dados pessoais. Não há mais espaço para políticas irresponsáveis e práticas abusivas, a nova realidade terá que se adequar à cultura do tratamento responsável. Além disso, é notória a adoção de procedimentos mais rígidos e específicos quando se trata da proteção de crianças e adolescentes.

A pioneira e principal referência legislativa é a *General Data Protection Regulation*¹³, criada pela União Europeia, diante da necessidade de os cidadãos entenderem o que acontecia

¹⁰ Em tradução livre do inglês para o português: Privacidade desde a concepção.

¹¹ Em tradução livre do inglês para o português: Privacidade por defeito.

¹² DANTAS, Henrique. **AdvogaTech**, 2020. Dispõe sobre aspectos estruturais da proteção de dados pessoais. O que é *Privacy by Design* e *Privacy by Default*. Disponível em: <https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv>. Acesso em 03 set. 2020.

¹³ EUROPEAN UNION (EU). **EU General Data Protection Regulation 2016/679 (EU-GDPR)**. Disponível em: <https://www.privacy-regulation.eu/en/index.htm>. Acesso em 22. abr. 2020.

com seus dados pessoais. Essa regulamentação foi responsável por inspirar a Lei Geral de Proteção de Dados e incentivar várias outras nações a seguirem seu exemplo.

A norma prevê que é legal o tratamento dos dados pessoais de uma criança quando ela possuir pelo menos 16 (dezesseis) anos. No caso de ter idade inferior, o tratamento só será legal se o consentimento for dado ou autorizado pelo detentor da responsabilidade parental (art. 8º). Porém, autoriza os Estados-Membros a fixarem uma idade menor para esses fins, não sendo possível ultrapassar o limite de 13 (treze) anos.

O fato de a Lei Geral de Proteção de Dados ter adotado apenas o termo “criança” em seu art. 14, sugere uma hipótese de justificativa a partir da sua inspiração na *General Data Protection Regulation*, pois esta regulamentação também utiliza o termo em questão, entretanto fixa a idade de 16 (dezesseis) anos, ato desconsiderado pelo legislador brasileiro. Circunstância essa, que acabou ocasionando divergência em relação aos demais dispositivos legais, entre eles o Estatuto da Criança e do Adolescente.

A *General Data Protection Regulation* destinou um artigo especificamente para destacar a necessidade do consentimento dos responsáveis pela criança, isto confirma o reconhecimento da incapacidade de autodeterminação de seus dados. A falta de discernimento e experiência para agir provocam esta ponderação mesmo em ordenamentos jurídicos diferentes.

Um exemplo de sua aplicação ocorreu no estado de Hesse, Alemanha, no qual foi proibido o uso, pelas crianças, das ferramentas: *MS Office 365*, *iWork* da *Apple* e *Google Docs*, para a realização de trabalhos nas escolas. Isso ocorreu devido ao não atendimento das regras previstas quanto à coleta de dados dos menores, que acontecia sem o devido consentimento, essa decisão foi tomada pela Comissão Local para Proteção de Dados e Liberdade da Informação (HBDI)¹⁴.

Outro destaque é a *Children’s Online Privacy Protection Act*¹⁵, criada em 1998 pela *Federal Trade Commission* – FTC, órgão independente de proteção ao direito dos consumidores, pertencente aos Estados Unidos. Este regulamento dispõe orientações para a proteção de dados pessoais de crianças, indivíduo menor de 13 (treze) anos, na internet. Foi

¹⁴ PINHEIRO, Patrícia Peck. *A LGPD aplicada ao cenário da educação*. Disponível em:

[¹⁵ FEDEERAL TRADE COMMISSION. *Children’s Online Privacy Protection Rule \(“COPPA”\)*. Disponível em: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>. Acesso em 06 set. 2020.](https://www.serpro.gov.br/lgpd/noticias/2020/educacao-lgpd#:~:text=Logo%2C%20crian%C3%A7a%20n%C3%A3o%20pode%20ficar,o%20artigo%2018%20do%20E.CA. Acesso em 10 ago. 2020.</p>
</div>
<div data-bbox=)

criada para impedir que *sites* e empresas arrecadem essas informações e utilizem em benefício próprio.

A *Children's Online Privacy Protection Act* também demonstra métodos para se obter a verificação do consentimento parental, diferentemente da *General Data Protection Regulation* e Lei Geral de Proteção de Dados que se limitam a definir hipóteses/princípios e apresentar formas de tratamento para prevenir que as irregularidades venham a ocorrer.

O §312.5, b, da *Children's Online Privacy Protection Act*, aponta esses métodos, quais sejam: (i) o fornecimento de um formulário de consentimento a ser assinado pelos pais ou responsáveis e ser devolvido ao operador por *e-mail*, fax ou digitalização eletrônica; (ii) o requerimento de uma transação monetária, que notifique o titular do cartão de crédito/débito (ou outro sistema de pagamento online) sobre cada transação; (iii) ter um número de telefone para o qual o responsável possa ligar, gratuitamente, e falar com pessoas treinadas; (iv) ter acesso, por videoconferência, a pessoas treinadas, e possivelmente fornecer o consentimento; (v) verificar a identidade dos pais ou responsáveis comparando com formulários do governo, devendo esses dados serem excluídos dos registros do operador logo após a verificação ser concluída; ou (vi) utilizar um *e-mail* com etapas adicionais para garantir que quem está consentindo é o pai ou responsável, dentre as etapas adicionais estão incluídos: carta, ligação ou outro *e-mail*.

Essas medidas, “apesar de não frustrarem todas as possibilidades de um consentimento falso, dado pela própria criança, apontam um caminho que permite ao operador criar e aprimorar soluções que superem esta barreira” (YANDRA; SILVA; SANTOS, 2020, p. 238).

Um exemplo bem definido de aplicação da *Children's Online Privacy Protection Act* é no *YouTube*¹⁶. Primeiro é necessário entender que essa plataforma ganha dinheiro com publicidades personalizadas e direcionadas de acordo com os gostos/interesses dos usuários, pois a partir do momento que se conectam, eles deixam rastros digitais que são lidos por *Cookies* (rastreadores da internet). Isso porque, toda e qualquer interação que se faz com dispositivos tecnológicos, existe hoje uma outra tecnologia para que aquela interação seja interpretada e se tenham *insights*¹⁷. A leitura é feita por algoritmos que direcionam os conteúdos de acordo com interesses, é uma experiência customizada.

¹⁶ O FIM dos canais de Cultura Pop no Youtube, 2020. 1 vídeo (32 min.). Publicado pelo canal Andrei Bedene. Disponível em: <https://www.youtube.com/watch?v=-J-Emcd576U&t=189s>. Acesso em 04 set. 2020.

¹⁷ *Insight* significa compreensão súbita de alguma coisa ou determinada situação. Na *internet*, os algoritmos (processos matemáticos de interpretação) realizam esse ato de percepção e apresentam conteúdos coerentes aos usuários.

O *YouTube* vende esses perfis estruturados para anunciantes que irão direcionar sua publicidade ao público alvo. O *YouTube Kids*, destinado às crianças, não possui publicidade, justamente para protegê-las de conteúdos inapropriados, contudo, é notório que também possuem acesso à plataforma que não lhes é destinada, e conseqüentemente há o recolhimento de seus dados pessoais.

Diante disso, em conformidade com a *Children's Privacy Protection Act*, a FTC atua de modo a impedir o recolhimento de dados de crianças sem o consentimento dos pais ou responsáveis. Essa atuação funciona com base no conteúdo oferecido pelos canais do *YouTube* e o potencial alcance do público infantil. Assim, um vídeo será direcionado para criança (chamados de “feito para criança”) se: as crianças são o público principal ou se não são o público principal, mas o vídeo ainda é direcionado a elas, ou seja, chamam a sua atenção.

Os proprietários dos canais devem, então, classificar os vídeos como para criança ou não, pois quando há a escolha da opção “sim, é para criança”, o *YouTube* desativa a coleta de dados. Isso ocorre em razão da possibilidade de não só a plataforma, mas os próprios canais (por meio de cadastros), se aproveitarem dos dados infantis.

Toda essa cautela é dispendida devido ao fato de o *YouTube* ser uma rede de preferência entre as crianças, tanto para o lazer, como para os estudos. Logo, também se torna fonte de abuso e discriminação.

Portanto, observa-se que além das regulamentações, os órgãos estatais estão mais rígidos na fiscalização, uma ação conjunta para reduzir as práticas abusivas à indivíduos que compõem um grupo vulnerável.

3 VULNERABILIDADE DE CRIANÇAS E ADOLESCENTES

O conceito de vulnerável está relacionado àquele que pode ser atacado e ferido física ou moralmente (GEIGER, 2004, p. 821). Enquanto vulnerabilidade caracteriza indivíduos fragilizados, jurídica ou politicamente, na promoção, proteção ou garantia de seus direitos (AYRES; JÚNIOR; CALAZANS; FILHO, 2009, p. 121).

Isto posto, verifica-se que crianças e adolescentes se inserem nestas concepções, uma vez que possuem a condição peculiar de pessoa em desenvolvimento. Este grupo necessita de proteção integral para a tutela de direitos, bem como de sua integridade física e moral.

Segundo Silva (2017, p. 230) “a inexperiência, o incompleto desenvolvimento das faculdades intelectuais, a facilidade de se deixar influenciar por outrem, a falta de autodeterminação e auto orientação impõem ao menor a completa abolição da capacidade de ação”.

Logo, a vulnerabilidade em questão se manifesta na ausência de autonomia vinculada à presença do risco. A incapacidade de governar a si próprio, acaba fragilizando o indivíduo frente a uma situação de perigo ou circunstância decisiva para a proteção de seus direitos.

A carência de autossuficiência advém do *status* de indivíduos em construção. Na infância, a criança passa pela socialização primária (período em que molda seus traços de personalidade), já na adolescência, além da continuidade na formação da personalidade, há o impulso de querer deixar suas marcas no ambiente que convive (YANDRA; SILVA; SANTOS, 2020, p. 240).

A presença do risco, no que diz respeito à proteção de dados, procede da falta de conhecimento sobre as consequências que o compartilhamento irresponsável é capaz de gerar. Outrossim, as informações imprecisas fornecidas pelas plataformas acerca do tratamento de dados, arrecadação excessiva, políticas de privacidade redigidas de forma complexa de se entender e técnicas de incentivo para escolhas ruins, são exemplos de percalços que compõem o risco do fluxo de dados pessoais na *internet*.

Por tais razões há a insistência da legislação brasileira em proteger crianças e adolescentes. Este tratamento diferenciado reflete o reconhecimento social de sua vulnerabilidade. Além disso, a maior cautela é a confirmação dos ideais presentes no Estatuto da Criança e do Adolescente, que os qualificou como sujeitos de direitos.

Nesse contexto, a classificação como sujeito de direitos demonstra a importância de enxergar e tratar os pensamentos, palavras, declarações e opiniões das crianças e adolescentes com a devida seriedade e respeito, atentando sempre para o grau de desenvolvimento, de maneira que “a proteção integral orienta e prescreve direitos às pessoas em desenvolvimento, impondo deveres à sociedade, inclusive na implantação de políticas públicas, de modo a contemplar essa situação e proporcionar a construção de um panorama jurídico especial”.¹⁸

O Estatuto da Criança e do Adolescente é considerado um marco jurídico na proteção integral, com absoluta prioridade, deste grupo vulnerável e, em 2020, comemora seus 30 (trinta)

¹⁸ ANJOS, Eduardo Pereira dos. *Quando a proteção integral é invocada para agravar a situação da criança*. Disponível em: https://www.conjur.com.br/2020-out-06/tribuna-defensoria-quando-protECAo-integral-invocada-agravar-situacao-crianca#_ftn5 Acesso em 22 dez. 2020.

anos. Esta data tem notável importância, pois representa a luta da sociedade em prol do melhor interesse e dignidade daqueles que são o passado, o presente e o futuro da nação.

3.1 Educação online e o acesso à informação

Apesar da internet ser um ambiente hostil e instável, principalmente para o público infanto-juvenil, também é fonte valiosa de notícias e conhecimento. Ademais, com a evolução da educação *online* e a pandemia, este público passou a ficar ainda mais tempo conectado, haja vista a impositiva troca das aulas presenciais pelas virtuais.

Em que pese a hiperconexão das crianças e adolescentes na *internet*, a tecnologia possibilitou que este grupo continuasse a exercer seu direito fundamental à educação, previsto no art. 6º da Constituição Federal de 1988.

O referido direito de natureza social é disposto também no capítulo III, seção 1, artigos 205 a 214 da Constituição Federal de 1988. Nesse sentido, destaque-se a importância dada à educação como um direito de todos e do papel da família, Estado e sociedade para concretizá-lo.

No entanto, com o advento da pandemia e do fato de que a navegação na rede se tornou necessária para a continuidade do calendário acadêmico e do ano letivo. “A falta de infraestrutura de computador, Internet e acesso remoto de 17% das crianças e adolescentes”¹⁹ comprometeu significativamente a efetivação do direito à educação.

Além disso, diante de um modo de ensino totalmente novo para crianças e adolescentes, surgiram alguns receios, sendo um deles a possível violação de dados pessoais a que estariam sujeitos os menores de idade.

Já foram vistas nos tópicos anteriores a importância dos dados na sociedade e da privacidade para os seus titulares, de maneira que um potencial vazamento poderia acarretar sérios danos aos envolvidos. Para tornar essa situação mais tangível, é importante projetar cenários do novo modelo educacional em que a violação de dados poderia ocorrer.

Nesse sentido, destaque-se que as aulas têm ocorrido por meio de plataformas online, e nessas ferramentas há a circulação e consequente coleta de dados envolvendo imagens, falas

¹⁹ VASCO, Késya Luciana do Nascimento Silva Vasco. *Direito à educação de crianças e adolescentes em tempos de pandemia*. Disponível em: <https://migalhas.uol.com.br/depeso/331717/direito-a-educacao-de-criancas-e-adolescentes-em-tempos-de-pandemia> Acesso em 22 dez. 2020.

e manifestações de preferências e convicções dos estudantes²⁰. É evidente que tais dados são relevantes e significativos para os titulares, pois envolvem questões íntimas e que em condições normais iriam se restringir às paredes das salas de aula.

Todavia, no mundo digital as chances de esses rastros ficarem registrados aumentam significativamente, e é nesse enquadramento que surgem inquietações. Imagine-se, hipoteticamente, a seguinte situação: uma criança de dez anos durante a aula de língua portuguesa, em uma discussão com colegas e professor(es) acerca da história do Brasil, profere uma opinião que envolve etnia, religião e até mesmo um ponto de vista político.

Tal situação, em tempos de aulas presenciais, muito provavelmente seria apenas mais uma entre inúmeras opiniões dos alunos e em breve seria esquecida ou ficaria registrada apenas na memória deles.

No entanto, no mundo virtual, elas devem ser vistas sob uma nova vertente: a dos dados pessoais sensíveis (art. 5º, inciso II, Lei Geral de Proteção de Dados). Estes dados possuem uma maior proteção da legislação, pois são informações com potencial discriminatório, sendo mais invasivos à privacidade do indivíduo. O seu tratamento depende de consentimento destacado e específico, com uma finalidade definida, ou em outras hipóteses elencadas no art. 11 da Lei Geral de Proteção de Dados.

Desse modo, percebe-se a importância do tratamento de dados como esses, que estão sujeitos à violação, principalmente, neste momento revolucionário da educação online. Ainda utilizando a situação hipotética dos parágrafos anteriores, pode-se questionar como esse vazamento poderia ocorrer, e mais uma vez, a título exemplificativo, projete-se os seguintes contextos: a) a escola X onde estuda a criança de dez anos supramencionada, grava as aulas que acontecem na plataforma Y e deixam à disposição para que os alunos possam revê-la a qualquer tempo; b) a referida escola não deixa as aulas gravadas, mas vários funcionários têm acesso a plataforma e ao banco de dados que a envolve; c) o acesso às aulas é restrito apenas aos professores e alunos.

Vislumbra-se que o que há em comum em todas as conjunturas mencionadas acima é a evidente possibilidade de potencial vazamento de dados dos estudantes. Ainda que em graus de risco diferentes, em todos os cenários isso se mostra factível.

²⁰ MARRAFON, Marco Aurélio; FERNANDES, Elora Raad. *A necessária proteção de dados das crianças e adolescentes na educação online*. Disponível em: <https://www.conjur.com.br/2020-jul-06/constituicao-poder-necessaria-protexcao-dados-criancas-adolescentes-educacao-online>. Acesso em 30 ago. 2020.

Assim sendo, cabe mencionar o mau uso dos dados pessoais pode trazer consequências não só para os titulares, como será demonstrado mais à frente, como também para responsáveis pelo dano causado, conforme dispõe a seção III do capítulo VI da Lei Geral de Proteção de Dados (arts. 42 a 45). Ademais, os agentes de tratamento também estão sujeitos a sanções administrativas dispostas na Seção I do Capítulo VIII da Lei Geral de Proteção de Dados, dentre as quais pode-se elencar como exemplo a advertência e as multas.

4 O POTENCIAL MAU USO DOS DADOS PESSOAIS

Como visto no tópico acima, a educação online por meio de plataformas digitais é uma circunstância que potencializa as chances de uma possível violação ou até mesmo vazamento de dados. Dentro desse cenário, é essencial ressaltar as prováveis consequências para as crianças e adolescentes.

Novamente, para tratar de forma didática do assunto, exemplos se mostram imprescindíveis. Idealize-se que na situação hipotética abordada no item anterior, a criança de dez anos estava tendo aulas online e fez comentários sobre o cabelo de uma colega que podem ser considerados racistas, bem como comentou sobre o partido político A criticou a religião B. Em uma situação como essa, comentários possivelmente efêmeros de uma criança, podem vir a influenciá-la por toda a sua vida.

O fenômeno da datificação da infância nesses tempos de ensino remoto pode levar a severas consequências futuras, como a recusa de uma vaga trabalho²¹. Ora, se a empresa não coaduna com os valores demonstrados pela criança e futura adulta, o fato de aquilo estar na rede pode influenciar, de forma direta, a negativa pro emprego.

Ademais, outro aspecto interessante a ser levado em consideração é o fato de que para ter acesso a muitas das plataformas de ensino digitais, é necessário fornecer dados pessoais, de maneira que as ferramentas podem se aproveitar para traçar um perfil comportamental dos usuários e no futuro usar disso para propagandas direcionadas. Como bem esclarece Bioni (2020, p.18) “o usuário da rede é, portanto, a todo momento, monitorado, acumulando-se uma

²¹ MARRAFON, Marco Aurélio; FERNANDES, Elora Raad. *A necessária proteção de dados das crianças e adolescentes na educação online*. Disponível em: <https://www.conjur.com.br/2020-jul-06/constituicao-poder-necessaria-protacao-dados-criancas-adolescentes-educacao-online>. Acesso em 30 ago. 2020.

série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária”.

Assim sendo, é notório que a violação dos dados pessoais de crianças e adolescentes pode causar consequências nos anos subsequentes, de maneira que se torna questionável como viabilizar a proteção dos referidos dados, o que poderia ser feito no que concerne a essa temática.

Nesse enquadramento e sem a pretensão de esgotar a temática, algumas alternativas merecem destaque. A primeira seria a escola fazer um mapeamento dos dados que possui e onde eles estão localizados. Depois de fazer essa organização, é importante restringir ao máximo o acesso aos referidos dados, de modo que se coadune com o dispõe os princípios da Lei Geral de Proteção de Dados, em especial o do consentimento, já que a autorização para o tratamento dos dados dos estudantes deve ser solicitada pela escola aos responsáveis legais dos menores. Além disso, também é primordial que a escola promova cursos e/ou palestras de capacitação para os funcionários para que eles possam entender a importância dos dados e do cumprimento da Lei Geral da Proteção de Dados²².

Outro aspecto que deve ser levado em consideração é a própria política de privacidade das plataformas online. Um exemplo interessante de plataforma de acesso à informação e muito utilizada por crianças é o *YouTube Kids*, que conforme o próprio site aduz “foi criado para proporcionar às crianças um ambiente mais controlado que torna a exploração mais simples e divertida, além de facilitar a orientação dos pais e cuidadores à medida que descobrem novos e incríveis interesses ao longo do caminho”²³.

Na tela inicial do *site* há a menção expressa da necessidade de os pais configurarem a ferramenta e ter acesso a recursos de controle para monitorar os conteúdos acessados pelos menores. Além disso, é exigido que se digite a data de nascimento para verificar a idade dos usuários. Há também um quadro de aviso aos responsáveis com informações de privacidade importantes, dentre elas: como são usadas as informações que são coletadas e a proibição de que os menores compartilhem informações pessoais com terceiros ou que as disponibilize publicamente²⁴.

²² FERREIRA, Felipe. *Lei Geral de Proteção de dados para escolas*. Disponível em:

<http://www.proesc.com/blog/lei-geral-de-protecao-de-dados-para-escolas/> Acesso em 15 ago. 2020

²³ GOOGLE. **Youtube Kids**. Dispõe informações sobre o aplicativo da plataforma. Disponível em:

[https://youtube.com/kids/?gclid=CjwKCAjwkdL6BRAREiwA-](https://youtube.com/kids/?gclid=CjwKCAjwkdL6BRAREiwA-kiczIp3DdK_FWt_xP0RgkBn3YGLFplQyvT_6PnDWk6LNXYHrtbx8HaaZhoCb4sQAvD_BwE&gclsrc=aw.ds)

[kiczIp3DdK_FWt_xP0RgkBn3YGLFplQyvT_6PnDWk6LNXYHrtbx8HaaZhoCb4sQAvD_BwE&gclsrc=aw.ds](https://youtube.com/kids/?gclid=CjwKCAjwkdL6BRAREiwA-kiczIp3DdK_FWt_xP0RgkBn3YGLFplQyvT_6PnDWk6LNXYHrtbx8HaaZhoCb4sQAvD_BwE&gclsrc=aw.ds) Acesso em 01 set. 2020.

²⁴ GOOGLE. **Youtube Kids**, 2020. Aviso aos pais: informações de privacidade importantes sobre o YouTube Kids. Disponível em: <https://www.youtubekids.com/>. Acesso em 02 set. 2020.

Informações de privacidade como essa do *YouTube Kids* são um exemplo de transparência e zelo com o cuidado com a privacidade dos menores. Por outro lado, do mesmo modo que as plataformas digitais e os responsáveis têm importância dentro desse ambiente, também é imprescindível desde cedo promover a conscientização das crianças e adolescentes acerca da valia dos dados.

Sendo assim, uma das formas de oportunizar essa compreensão é através de histórias (PEREIRA; SANTOS; SILVA, 2018, p. Internet) e jogos (IBLISS, p. Internet) como o da *IBLISS Digital Security*. De forma lúdica e didática é mostrado aos menores os perigos do mundo virtual e a necessidade do constante monitoramento dos responsáveis para ajudá-los. Iniciativas como essas fomentam o conhecimento sobre o mundo digital e se mostram cada vez mais necessárias como ferramentas no combate à desinformação e principalmente como uma forma de contribuir para a proteção dos dados pessoais de crianças e adolescentes.

5 CONSIDERAÇÕES FINAIS

Como foi visto, com a pandemia e a necessidade do distanciamento social, a educação online se tornou a solução para a manutenção do ensino. A mudança ocorreu de uma forma abrupta e afetou principalmente as crianças e adolescentes, grupo que até então costumava ter aulas integralmente presenciais. Foi nesse contexto de transição para o mundo virtual que se intensificou a preocupação com os dados pessoais dos menores de idade.

Nesse sentido, destacou-se a importância dos dados pessoais, a legislação que rege o tema no que concerne às crianças e adolescentes, bem como a vulnerabilidade em que estão inseridos esses seres em desenvolvimento. Ademais, foi feita uma análise específica da educação online e da hiperconexão nas redes como potencializadoras de possíveis violações à dados pessoais.

Dentro desse contexto, verifica-se que mesmo com a necessária educação online em virtude da pandemia, é essencial ter cautela com o tratamento dos dados pessoais, a fim de buscar impedir o mau aproveitamento deles no futuro. Desse modo, compreendeu-se que a potencial violação de dados pode interferir em uma futura seleção de emprego ou até mesmo perseguir a carreira profissional do indivíduo.

Sem pretender esgotar o tema e como uma forma de inibir tais condutas, identificou-se algumas soluções que englobam a escola, as plataformas digitais e os menores de idade junto a seus responsáveis.

No que tange a escola, mostra-se indispensável fazer um mapeamento dos dados, como também respeitar os princípios da Lei Geral de Proteção de Dados e a capacitação dos funcionários acerca do tema. Já as plataformas digitais podem usar como exemplo a política de privacidade sucinta e transparente do *Youtube Kids*, além de se inspirar nos métodos de verificação do consentimento parental estabelecidos pela *Children's Online Privacy Protection Act*.

Enquanto aos pais ou responsáveis legais cabe a missão de constante fiscalização, auxílio e orientação. Uma das formas de estimular o conhecimento, o aprendizado e chamar atenção ao mundo virtual é através de histórias e jogos, visto que possuem a capacidade de transformar um assunto complexo e necessário em mais simples e didático.

Portanto, conclui-se que as crianças e adolescentes são indivíduos vulneráveis e em desenvolvimento, eles são prioridade na tutela contra os perigos existentes na internet. É imprescindível se adaptar a essa nova realidade para lhes garantir a proteção integral.

REFERÊNCIAS

- AYRES, José Ricardo de Carvalho Mesquita; JÚNIOR, Ivan França; CALAZANS; Gabriela Junqueira; FILHO, Haraldo César Saletti. O conceito de vulnerabilidade e as práticas de saúde: novas perspectivas e desafios. *In*: CZERESNIA, Dina; FREITAS, Carlos Machado de. **Promoção da saúde: conceitos, reflexões e tendências**. Rio de Janeiro: Editora Fiocruz, 2009.
- BIONI, Bruno Ricardo. **Proteção dos dados pessoais: a função e os limites do consentimento**. 2. ed. rev., atual. e reform. Rio de Janeiro: Forense, 2020.
- COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed., rev., atual. e ampl. São Paulo: Thomson Reuters, 2019.
- GEIGER, Paulo. **Minidicionário contemporâneo na língua portuguesa Caldas Aulete**. Rio de Janeiro: Nova Fronteira, 2004.

IBLISS DIGITAL SECURITY. **O mundo virtual é tão perigoso quanto o real**. Disponível em: <https://www.ibliss.digital/wp-content/uploads/jogo-da-seguranca-ibliss-joao-e-maria-na-era-cyber.pdf>. Acesso em: 03 set. 2020.

PEREIRA, Eva; SANTOS, Diego dos; SILVA, Francisca. **João e Maria na era Cyber**. IBLISS Digital Security, 2018. Disponível em: <https://www.ibliss.digital/wp-content/uploads/ebook-educacional-de-seguranca-ibliss-joao-e-maria-na-era-cyber.pdf>. Acesso em: 01 set. 2020.

ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo; CUNHA, Rogério Sanches. **Estatuto da Criança e do adolescente**: comentado artigo por artigo. 9 ed. São Paulo: Saraiva, 2017.

SILVA, Carlos Mário Pereira da. **Instituições de Direito Civil**. ed. 30. Rio de Janeiro: Forense, 2017. vol. 1.

YANDRA, Bárbara Fernanda Ferreira; SILVA; Amanda Cristina Alves; SANTOS, Jéssica Guedes. Lei Geral de Proteção de Dados e a tutela dos dados pessoais de crianças e adolescentes: a efetividade do consentimento dos pais ou responsáveis legais. **Internet & Sociedade**. n. 1, v. 1, 2020.

THE PERSONAL DATA PROTECTION OF CHILDREN AND TEENAGERS IN THE SCOPE OF ONLINE EDUCATION

ABSTRACT

The present research has as core the analysis the violation of children and teenagers personal data within context of online education. Therefore, the hypothetical-deductive method is used, testing the hypothesis that distance learning and hyperconnection in networks increases the chances of possible personal data breaches. Scenarios are designed where violations can happen, beyond the possible

repercussions in the future. Lastly, points out measures that can be adopted for data protection.

Keywords: Online education. Personal data protection. Children and teenagers.