

The background of the entire page is a complex, abstract geometric pattern. It consists of numerous black dots of varying sizes connected by thin black lines. These connections form a variety of polygons, primarily triangles and quadrilaterals, creating a web-like or network structure that spans the entire page. The pattern is more dense in some areas and more sparse in others, giving it a dynamic and interconnected appearance.

REDE

DE PESQUISA
EM GOVERNANÇA
DA INTERNET

Anais do Encontro Virtual
da Rede de Pesquisa em
Governança da Internet
Outubro de 2021

IV ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2021

FICHA TÉCNICA

**ANAIS DA REDE DE PESQUISA EM
GOVERNANÇA DA INTERNET-VOL. 4,
ISSN 2675-1690**

Editores

Gustavo Ramos Rodrigues
Hemanuel Jhosé Alves Veras
Kimberly de Aguiar Anastácio
Nathan Paschoalini Ribeiro Batista

Autores

Alexandre Arns Gonzales
André Ramiro
Carolina Fiorini Ramos Giovanini
Hemanuel Jhosé Alves Veras
João Paulo Aguiar
Luis Gustavo de Souza Azevedo
Marcos César M. Pereira
Maria Vitoria Pereira de Jesus
Mark William Datysgeld
Nathalia Sautchuk Patrício
Nathan Paschoalini Ribeiro Batista
Pedro Amaral
Sergio Marcos Carvalho de Ávila Negri

Revisores

Alexandre Arns Gonzales
Carolina Israel
Hemanuel Jhosé Alves Veras
Luis Gustavo de Souza Azevedo
Maria Vitoria Pereira de Jesus
Nathan Paschoalini Ribeiro Batista

COMITÊ ORGANIZADOR

**Núcleo de Coordenação da Rede de
Pesquisa em Governança da Internet**

Carolina Batista Israel
Diego Jair Vicentin
Fernanda R. Rosa
Gustavo Ramos Rodrigues
Hemanuel Jhosé Alves Veras

Kimberly de Aguiar Anastácio
Maria Vitoria Pereira de Jesus
Nathan Paschoalini Ribeiro Batista

Comitê Científico

Ana Paula Camelo
Daniela Araújo
Diego Jair Vicentin
Edison Spina
Fernanda Rosa
Flávio Rech Wagner
Gills Vilar-Lopes
Jean Santos
Leonardo Ribeiro da Cruz
Lisandro Granville
Maria Mônica Arroyo
Marta Mourão Kanashiro
Olga Cavalli
Raquel Gatto
Rodolfo Avelino
Rosemary Segurado

Moderadores

Ana Paula Camelo
Ana Claudia Farranha
Flávio Rech Wagner
Leonardo Ribeiro da Cruz
Marisa von Bulow
Maria Alexandra Viegas Cortez da Cunha
Rodolfo Avelino
Rodolfo Avelino
Rosemary Segurado

Debatedores

Hemanuel Jhosé Alves Veras
Luis Gustavo de Souza Azevedo
André Ramiro
Nathalia Sautchuk Patrício
Alexandre Arns Gonzales
Carolina Giovanini
Nathan Paschoalini Ribeiro Batista
Mark William Datysgeld
João Paulo Aguiar
Maria Vitoria Pereira de Jesus



CONCENTRAÇÃO DE PLATAFORMAS E PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES DURANTE O ENSINO REMOTO

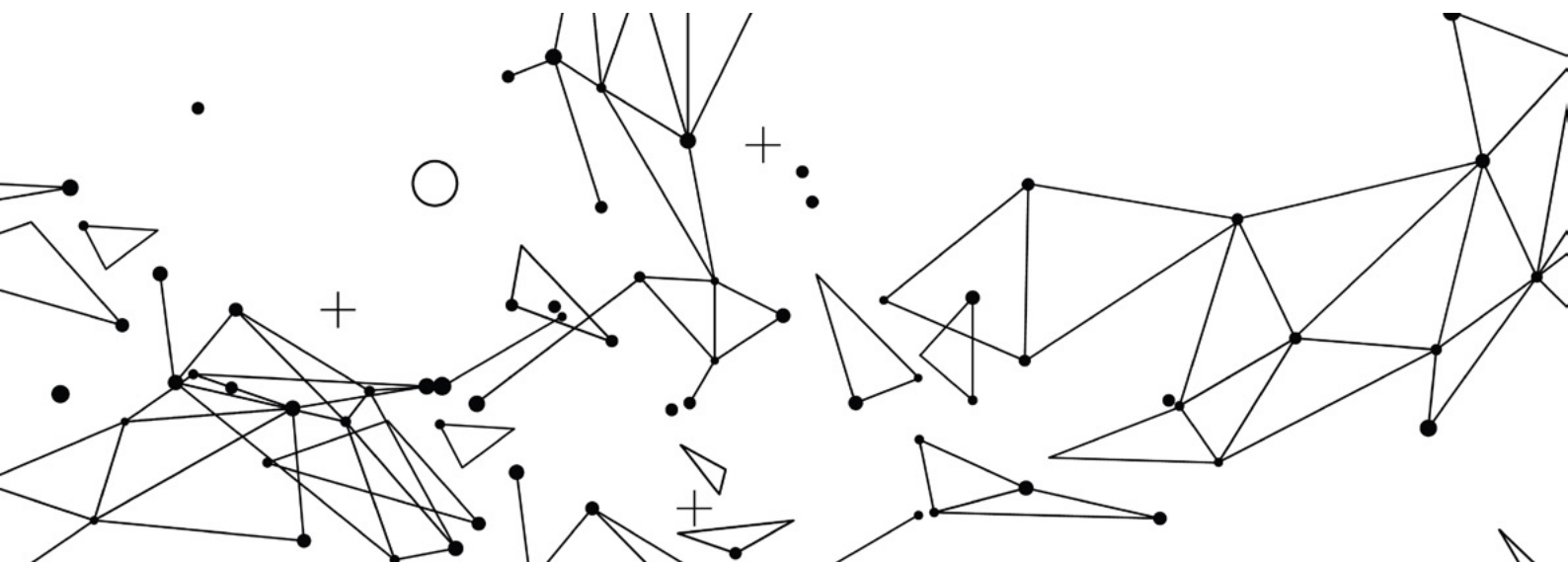
SERGIO MARCOS CARVALHO DE ÁVILA NEGRI

NATHAN PASCHOALINI RIBEIRO BATISTA

CAROLINA FIORINI RAMOS GIOVANINI

SUMÁRIO

INTRODUÇÃO.....	5
CONSIDERAÇÕES TEÓRICO-METODOLÓGICAS.....	6
A CONCENTRAÇÃO DA WEB COMO SOLO FÉRTIL PARA O CAPITALISMO DE VIGILÂNCIA	8
A PANDEMIA DE COVID-19 E O SOLUCIONISMO TECNOLÓGICO NA EDUCAÇÃO.....	12
TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES: VULNERABILIDADE E RISCOS	13
CONCLUSÃO	21
REFERÊNCIAS	22





CONCENTRAÇÃO DE PLATAFORMAS E PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES DURANTE O ENSINO REMOTO

Sergio Marcos Carvalho de Avila Negri¹

Nathan Paschoalini Ribeiro Batista²

Carolina Fiorini Ramos Giovanini³

RESUMO

O presente trabalho busca analisar os impactos à proteção de dados de crianças e adolescentes, resultantes da concentração de plataformas de educação utilizadas durante o ensino remoto. A pesquisa é estruturada a partir das observações e das reflexões obtidas na realização de projeto de extensão acerca da proteção de dados no ensino-aprendizagem de crianças e adolescentes durante a pandemia de coronavírus. Considerando a vulnerabilidade de crianças e adolescentes, o fato desses sujeitos estarem em estágio de desenvolvimento, bem como a concentração de plataformas, parte-se de uma abordagem exploratória, ancorada em evidências empíricas, para compreender quais são os riscos e possíveis consequências decorrentes desse cenário e os parâmetros a serem avaliados quando do tratamento de dados de crianças e adolescentes.

PALAVRAS-CHAVE

Centralização da web; Proteção de Dados; Crianças e adolescentes.

ABSTRACT

This paper aims to analyze the impacts on data protection of children and adolescents, arising from the concentration of educational platforms used during remote learning. The research is structured from the observations and reflections obtained during an extension project on data protection in the teaching-learning process of children and

¹ Professor Adjunto do Departamento de Direito Privado da Faculdade de Direito da UFJF. Membro do corpo docente permanente do programa de pós-graduação Stricto Sensu em Direito e Inovação da UFJF. Doutor e mestre em Direito Civil pela UERJ. Especialista em Direito Civil pela Università degli Studi di Camerino (Itália). Coordenador do Núcleo de Estudos Avançados em Pessoa, Inovação e Direito (NEAPID/UFJF). E-mail: smcnegri@yahoo.com

² Bacharel em Direito e Mestrando em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF). Pesquisador no Núcleo de Estudos Avançados em Pessoa, Inovação e Direito (NEAPID/UFJF). E-mail: nathanprb18@gmail.com

³ Graduada em Direito pela Universidade Federal de Juiz de Fora (UFJF). Pesquisadora no Núcleo de Estudos Avançados em Pessoa, Inovação e Direito (NEAPID/UFJF). E-mail: cfrgiovanini@gmail.com

adolescents during the coronavirus pandemic. Considering the vulnerability of children and adolescents, the fact that these subjects are in a stage of development, as well as the concentration of platforms, an exploratory approach is taken, anchored in empirical evidence, to understand what are the risks and possible consequences arising from this scenario and the parameters to be evaluated when processing data from children and adolescents.

KEY WORDS

Web centralization; Data Protection; Children and adolescents.

INTRODUÇÃO

Com a pandemia de Covid-19, ingressamos em uma crise sanitária de escala global. Diversos hábitos e atividades cotidianas foram transpostos para o ambiente virtual em decorrência das medidas e protocolos sanitários que objetivavam conter a propagação do vírus. No ambiente escolar, esse cenário também foi verificado na medida em que instituições de ensino passaram a utilizar plataformas digitais para retomarem as atividades escolares à distância.

O discurso coletivo que se espalhou nos primeiros meses de pandemia, pautado na narrativa de que o vírus “não escolhe entre pessoas” e que “estamos todos no mesmo barco” esconde o fato de que determinados indivíduos encontram-se em situação de vulnerabilidade e sofrem com os impactos da crise de forma potencializada.

Esse contexto pode ser ilustrado a partir de reportagens e notícias que narram a vida de estudantes durante o ensino remoto. No município de Alencar, no oeste do Pará, um aluno sobe em árvores para buscar melhor sinal de Internet e conseguir acompanhar as aulas⁴. Em São Paulo, uma aluna assiste às aulas somente nas terças-feiras porque este é o dia de folga da mãe, a única pessoa da casa que possui um dispositivo *smartphone*⁵.

Por um lado, a veiculação destes relatos ativa o imaginário meritocrático e cria a ilusão de que as dificuldades vividas por crianças e adolescentes no ensino remoto podem ser superadas, por outro, há uma clara demonstração de que a desigualdade - por vezes, politicamente induzida - impacta o desenvolvimento e a formação de estudantes.

⁴ FANTÁSTICO. Jovem sobe no alto de árvore para melhorar sinal de internet e assistir aulas no Pará. Disponível em: <<https://g1.globo.com/fantastico/noticia/2021/03/21/jovem-sobe-no-alto-de-arvore-para-melhorar-sinal-de-internet-e-assistir-aulas-no-para.shtml>>. Acesso em 11/09/2021

⁵ SOUZA, Felipe. Ensino remoto na pandemia: os alunos ainda sem internet ou celular após um ano de aulas à distância. G1. Disponível em: <<https://g1.globo.com/educacao/noticia/2021/05/03/ensino-remoto-na-pandemia-os-alunos-ainda-sem-internet-ou-celular-apos-um-ano-de-aulas-a-distancia.shtml>>. Acesso em 11/09/2021

A transposição do ambiente escolar para o ambiente virtual também é marcada pela adoção de plataformas digitais, que possibilitam reuniões, envio de arquivos, comunicação em tempo real, mensagens instantâneas, etc. Tal adoção indiscriminada remonta o histórico da educação pública brasileira - que sofre um constante processo de desinvestimento - culminando na incapacidade das instituições públicas de ensino, especialmente as instituições de educação básica, de proporem iniciativas de digitalização que atendam, de fato, ao interesse público.

O avanço dessas plataformas digitais para o ambiente educacional, propiciado pelo sucateamento da educação pública, revela algumas preocupações acerca da privacidade e proteção de dados dos usuários, sobretudo de usuários crianças e adolescentes.

Considerando o contexto apresentado e levando em consideração que um ano se passou desde o início da pandemia de coronavírus, e a consequente necessidade de isolamento social, o presente trabalho busca analisar como a concentração de plataformas no ensino remoto impacta na proteção de dados de crianças e adolescentes, considerando a vulnerabilidade desses sujeitos que ainda estão em desenvolvimento.

CONSIDERAÇÕES TEÓRICO-METODOLÓGICAS

Esta pesquisa é estruturada a partir das reflexões decorrentes do projeto de extensão “A proteção de dados no ensino-aprendizagem de crianças e adolescentes”, desenvolvido pelo Núcleo de Estudos Avançados em Pessoa, Inovação e Direito (NEAPID/UFJF), e que tem por objetivo a atuação junto às escolas de ensino básico da rede pública de Juiz de Fora, de modo a auxiliar na construção de uma cultura de proteção de dados, considerando o contexto de intensa digitalização e virtualização das experiências de ensino-aprendizagem que já estão em curso, mas cuja implementação foi acelerada em decorrência da pandemia de COVID-19.

Vale destacar que, em se tratando da rede pública de ensino do Município de Juiz de Fora e Estado de Minas Gerais, não houve a adoção de plataformas digitais como o *Google for Education*, ainda que ferramentas como o *WhatsApp* fossem utilizadas para o prosseguimento das atividades escolares. A política educacional definida pelo estado de Minas Gerais, durante a pandemia de COVID-19, foi direcionada ao estabelecimento do Regime Especial de Atividades Não Presenciais (REANP), por meio da Resolução SEE nº 4310/2020. Segundo tal resolução, as Escolas Estaduais

deverão ofertar aos alunos e às alunas um Plano de Ensino Tutorado (PET), os quais seriam distribuídos por meio de Tecnologias da Informação e Comunicação (TICs) e, em casos, específicos seria garantida a impressão dos referidos PETs, assegurando a sua distribuição aos estudantes. Além disso, foi estabelecida a transmissão de aulas gravadas pela emissora Rede Minas, por meio de um programa intitulado de “Se Liga na Educação”, e desenvolvido o aplicativo “Conexão Escola”, que funcionaria como mais uma forma de acesso aos Planos de Ensino Tutorado e às aulas disponibilizadas através da Rede Minas.

Contudo, apesar da não adoção de plataformas como a exemplificada anteriormente, em um exercício de abstração, preocupações acerca da proteção de dados de crianças e adolescentes surgiram, especialmente quando se leva em conta a intensificação da utilização de plataformas proprietárias no ambiente escolar.

Feitas tais considerações, faz-se necessário discorrer acerca da escolha teórica que orientará as reflexões a seguir. A partir da significativa literatura acerca da Economia Política da Internet, da vigilância e dos riscos envolvidos no tratamento de dados de crianças e adolescentes durante o ensino remoto, busca-se demonstrar como a concentração de plataformas digitais impacta o ambiente escolar e, consequentemente, o ensino-aprendizagem. Para o desenvolvimento do trabalho, alguns conceitos são de fundamental importância, como Capitalismo de Vigilância, concentração da web, vulnerabilidade e risco.

Dessa forma, considerando o contexto de ensino remoto imposto pela pandemia de COVID-19, bem como o movimento concomitante de digitalização e adoção de plataformas digitais distribuídas por *Big Techs* como Google e Microsoft, questiona-se: considerando as dinâmicas socioeconômicas próprias de países do sul global, como o Brasil, quais são os riscos para a privacidade e proteção de dados de crianças e adolescentes diante da adoção massiva de plataformas digitais voltadas ao ambiente escolar?

Para que seja possível delinear uma resposta ao questionamento elaborado, a presente pesquisa valer-se-á de uma abordagem exploratória, com intuito de estabelecer uma investigação geral do problema de pesquisa, permitindo uma aproximação com o objeto de estudo, de modo que seja possível o desenvolvimento e aprofundamento posterior do tema em análise, de forma mais precisa (GIL, 2008).

Aliada à abordagem exploratória, este trabalho baseia-se em uma análise qualitativa tanto dos dados produzidos ao longo do estudo “Educação Viglada” quanto dos dados disponibilizados pela terceira edição da pesquisa “Painel TIC Covid-19” (2020), cujo escopo encontra-se na análise dos indicadores relativos ao ensino remoto e ao teletrabalho durante o ano de 2020, além da pesquisa “TIC Educação 2020 - Edição Covid-19”. A escolha pela perspectiva qualitativa fundamenta-se no fato de que, segundo Groulx (2008), a contribuição desta à pesquisa quantitativa reside justamente na possibilidade de conferir uma renovação no olhar dirigido ao problema social a ser investigado, no caso do presente trabalho, tal problema está atrelado aos riscos à proteção de dados de crianças e adolescentes.

A utilização destes dados visa o oferecimento de um aporte empírico acerca da concentração de plataformas no ensino remoto, subsidiando o desenvolvimento do raciocínio sobre a proteção de dados de crianças e adolescentes. Para tanto, apoiar-se-á nas regras de inferência, em especial na elaboração de inferências descritivas, as quais buscam conhecer fatos desconhecidos a partir de fatos já conhecidos pelos pesquisadores (EPSTEIN, KING, 2013).

A CONCENTRAÇÃO DA WEB COMO SOLO FÉRTIL PARA O CAPITALISMO DE VIGILÂNCIA

Historicamente, o desenvolvimento econômico das sociedades tem se ancorado em distintos elementos que assumem papéis estruturantes na constituição da sociabilidade e dos regimes de acumulação, como, por exemplo, foram as fábricas para o período da Revolução Industrial do século XVIII. Contudo, segundo Bioni (2021), após a Segunda Guerra Mundial, houve um deslocamento na forma em que se dava a organização social, de modo que esta passou a estruturar seu desenvolvimento econômico em torno de um novo elemento fundamental: a informação.

Tal reorganização social foi possibilitada não somente pelo crescente desenvolvimento tecnológico que permite um aumento até então inimaginável na capacidade de processamento e, conseqüente, intensificação na produção de dados durante o nosso itinerário no mundo virtual, mas também pela capacidade que as grandes corporações de tecnologias têm de extrair valor dessas informações (BIONI; ZANATTA, 2020). Segundo Rodotà (2008), uma das facetas de tal extração de valor das informações reside na possibilidade de se criar perfis de consumo individual ou familiar, análises de pre-

ferências, etc., os quais são especialmente lucrativos para outros sujeitos, para quem tais “novas informações” podem ser vendidas.

A partir dessa compreensão, houve o avanço de modelos de negócio que se baseiam na expropriação de informações decorrentes do processo de datificação das mais diversas experiências humanas, dando início àquilo que se denomina de Capitalismo de Vigilância. Segundo Mayer-Schönberger e Cukier (2013), datificação é o processo de transformação de determinado fenômeno em um formato quantificável, o qual se torna passível de ser analisado, diferindo, portanto, do processo de digitalização. Este, por sua vez, pode ser considerado como o processo de transformação de informações analógicas em linguagem computacional. Van Dijck (2014), ao discorrer sobre tal conceito, acrescenta que a datificação permite o rastreamento em tempo real, bem como a análise preditiva a partir dos dados coletados.

O Capitalismo de Vigilância, segundo Zuboff (2021), é uma inovação no regime de acumulação e que possui raízes nas bases político-econômicas e ideológicas do neoliberalismo. Trata-se, portanto, de uma lógica de produção que reivindica “de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais” (ZUBOFF, 2021, p. 18).

Tal matéria prima é coletada sob a justificativa do aprimoramento de serviços oferecidos gratuitamente, no entanto, aqueles dados coletados e não utilizados para esses fins são considerados excedentes comportamentais (*behavioral surplus*), servindo, por conseguinte, de elemento fundamental para o desenvolvimento de produtos de predição, os quais são negociados em mercados futuros comportamentais (ZUBOFF, 2021). Segundo Amadeu (2021), há uma tentativa, nesses mercados, de antecipação dos comportamentos, gostos e interesses dos consumidores, de modo a atingi-los no momento em que há a necessidade de consumo.

Zuboff (2021) salienta que o Capitalismo de Vigilância não é a tecnologia em si, mas uma lógica que imbui o desenvolvimento tecnológico, de modo a orientar suas ações. Nesse sentido, apesar dessa dinâmica de acumulação de capital necessitar do ambiente digital, Capitalismo de Vigilância e o “digital” não se confundem.

A compreensão do Capitalismo de Vigilância enquanto uma lógica de desenvolvimento e não a tecnologia em si é indispensável para se questionar tais modelos de negócio, pois que subverte a expectativa dos capitalistas de vigilância quanto à inevita-

bilidade de suas práticas econômicas, quando elas são, na realidade, meticulosamente articuladas para fins comerciais (ZUBOFF, 2021).

Nessa forma de acumulação de capital, a vigilância assume papel fundamental. Segundo Lyon (2018), a Internet se tornou um espaço de vigilância que dificulta a distinção entre atividades de monitoramento e rastreo executadas por agências de segurança, e iniciativas de vigilância cotidiana. Desse modo, os dados e, consequentemente, a datificação constituem engrenagem essencial da constituição da Internet, uma vez que eles são parte desta rede em todos os seus níveis (LYON, 2018).

A expansão da Internet cumpre, portanto, um papel fundamental para o florescer desta lógica de acumulação, tendo em vista que as tecnologias da Informação e Comunicação (TICs) possuem uma tendência a entrar em conflito com a plena construção da esfera privada, compreendida a partir da noção de autodeterminação informativa (RODOTÀ, 2008), que não se confunde com a mera manifestação de consentimento, mas que se vale de instrumentos de controle e accountability para que seja garantida a autodeterminação informativa do indivíduos.

Com a abertura comercial da Internet, entre o final dos anos 1980 e início dos anos 1990, houve uma popularização do acesso a essa rede pública mundial de computadores (DEMENTSHUK; HENRIQUES, 2019). Contudo, tal abertura significou uma mudança fundamental na organização da Internet, pois houve um deslocamento

de uma lógica estatal-militar-acadêmica, segundo o modelo clássico norte-americano de inovação puxada pelo complexo industrial-militar, a partir de demandas do Departamento de Estado, para outra acadêmico-mercantil, a partir da privatização geral de meados da década de 90.

Não se trata meramente da passagem de uma lógica estatal para outra privada, mas, por um lado, de uma economia pública, centrada no investimento estatal, para outra de mercado, de acordo com diferentes modalidades de mercantilização e, por outro, de uma lógica política militar, de defesa, para outra, de privatização, regulação e globalização econômica, de apoio à reestruturação capitalista e à manutenção da hegemonia norte-americana nas relações internacionais no campo econômico (BOLAÑO et al 2007, p.60-61).

Nesse sentido, Bolaño e Vieira (2014) argumentam que a economia da Internet passa a se desenvolver da forma que conhecemos, se tornando alvo do capital especulativo a partir do momento em que o contexto de ação conjunta entre Estado, academia e setor privado se tornou atrativo para os investidores de capital de risco, resultando em enormes investimentos em pequenas empresas de tecnologia, culminando na

criação da “bolha especulativa das empresas de tecnologia” (BOLAÑO, VIEIRA, 2014, p. 74). Desse modo, Sposito (2008) aponta que a estrutura da Internet, ao final da última década do século XX, já estava privatizada, passando a configurar uma arquitetura que permitia a conexão de todas as outras redes informáticas.

Como consequência desses eventos, houve o rompimento da bolha especulativa no início dos anos 2000, provocando uma grande crise no setor produtivo de tecnologias baseadas em serviços para a Internet, que se traduziu em um

extenso processo de demissões em massa e de fusões que constituirão o atual oligopólio da rede. As empresas que conseguiram sobreviver à crise são exatamente as gigantes que conhecemos hoje, as quais passaram a utilizar a Internet como plataforma e não mais como ferramenta. (BOLAÑO, VIEIRA, 2014, p. 74).

A consequente “inovação” nas modalidades de mercantilização operadas por esses oligopólios tecnológicos, permitiu a descoberta do dado pessoal e não pessoal como matéria prima fundamental para a organização de seus modelos de negócio, em especial o Google – considerado por Zuboff (2021) como a corporação pioneira nessa forma de acumulação denominada de Capitalismo de Vigilância.

Bolaño et al (2007) argumentam que essa estrutura de comunicação tida, inicialmente, como revolucionária, se apresenta, atualmente, como uma complexa e assimétrica relação entre diferentes atores, na qual a capacidade de acesso à informação relevante está atrelada aos elementos que “no passado garantiam o acesso à esfera pública liberal: poder econômico (propriedade), político e conhecimento, nessa ordem de importância” (BOLAÑO et al, 2007, p. 58). De modo que, segundo os autores, tais mudanças na estrutura da Internet apontam para uma constituição de mundo em que o poder encontra-se cada vez mais concentrado - hodiernamente nas figuras das *big techs*.

Nesse contexto, e considerando a mudança de paradigma trazida pela constante datificação, processo que alçou os dados à categoria de elemento essencial para a manutenção de determinados modelos de negócio, as big techs desenvolvem diversos mecanismos, denominados de “jardins murados” com intuito de forçar os usuários a se manterem em suas plataformas - estas são caracterizadas como infraestruturas digitais, capazes de viabilizar a interação entre usuários, apresentando-se como intermediárias que reúnem uma diversidade de usuários, como consumidores, anunciantes e produtores (SRNICEK, 2017) - de forma a massificar a coleta de informações desses usuários (DEMENTSHUK; HENRIQUES, 2019).

Uma das facetas dos “jardins murados” é justamente a diversificação no oferecimento de serviços por uma mesma empresa de tecnologia, pode-se citar como exemplo, novamente, a Google, que além de oferecer seu já hegemônico sistema de buscas online, oferece também, dentre outros serviços, uma série de ferramentas voltadas e otimizadas para o ambiente educacional, comercializada sob o nome de *Google Workspace for Education*⁶. Tal diversificação atende à necessidade de se ampliar os tipos de dados coletados, de modo a aprimorar os produtos de predição.

A PANDEMIA DE COVID-19 E O SOLUCIONISMO TECNOLÓGICO NA EDUCAÇÃO

A ocorrência da pandemia de COVID-19 e a necessidade de se estabelecer um método de ensino remoto, considerando a urgência em se manter o distanciamento social, revelaram “o despreparo das instituições públicas em dispor de infraestruturas adequadas para a interação a distância e abriu espaço para um aumento na adoção de soluções oferecidas por grandes empresas do capitalismo global” (CRUZ, VENTURINI, 2020, p. 1061).

Segundo Cruz e Venturini (2020), ainda que o interesse dessas empresas no espaço educacional como uma oportunidade de negócio não tenha se originado com a pandemia, em razão da crise sanitária, foram celebrados acordos às pressas, como um esforço de se manter, a qualquer custo, um calendário escolar, sem que se conhecesse, de fato, quais são os riscos inerentes à utilização de tais plataformas educacionais.

Morozov (2018) argumenta que rupturas tecnológicas - como o desenvolvimento, por parte de grandes empresas de tecnologias, de plataformas digitais voltadas para o ambiente educacional - possuem raízes em todos os campos, exceto no campo da tecnologia, de modo que esta se torna apenas um meio para se concretizar interesses econômicos. Segundo o autor, tais rupturas são viabilizadas por crises políticas e econômicas, que incidem diretamente na forma como nos relacionamos e vivemos.

Dessa forma, o contexto de urgência em se digitalizar as atividades escolares associada à medidas neoliberais de desinvestimento em educação, seja ela superior ou básica, se torna ambiente fértil para o solucionismo tecnológico (CRUZ, VENTURINI, 2020) que, segundo Morozov (2020), se tornou uma prática que busca, a partir da implantação de tecnologias, solucionar problemas que são ocasionados pelo próprio estado neoliberal. No caso aqui em estudo, o solucionismo tecnológico se dá na medida em que, para se

⁶ <https://www.blog.google/outreach-initiatives/education/google-workspace-for-education/>

resolver a situação de desmonte da educação pública, adota-se plataformas de ensino, cujas propriedades são de grandes corporações de tecnologia, como Google e Microsoft.

Nesse sentido, ao adotar medidas pura e simplesmente tecnológicas, Morozov (2020) argumenta que os solucionistas buscam evitar a política e defendem medidas que mantêm o pleno funcionamento do capitalismo global, que tem se apresentado, hodiernamente, na forma do Capitalismo de Vigilância. Conforme argumentam Cruz e Venturini (2020), o atual cenário demonstra um crescimento vertiginoso do mercado de plataformas educacionais concentrado em duas grandes corporações, as quais possuem tanto uma infraestrutura técnica quanto de recursos humanos que nenhuma instituição pública de ensino possui.

TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES: VULNERABILIDADE E RISCOS

A pesquisa TIC Educação 2020 - Edição Covid-19 demonstrou que, durante a pandemia de Covid-19, 87% das escolas adotaram ao menos uma atividade com o uso de tecnologias. A pesquisa evidenciou, entre outros aspectos, a falta de dispositivos (como computadores e celulares) e de acesso à Internet nos domicílios dos alunos. Além disso, os desafios no atendimento a alunos em condição de vulnerabilidade social foram demonstrados, por exemplo, nos casos de alunos sem acesso à alimentação no domicílio.

Na mesma direção, a terceira edição da pesquisa “Painel TIC Covid-19” (2020) demonstrou que o celular foi o principal dispositivo utilizado para acompanhar as aulas e atividades remotas, especialmente nas classes DE, por outro lado, o uso predominante de computador (notebook, computador de mesa e tablet) foi maior nas classes AB (66%), revelando um cenário de desigualdade que foi potencializado no decorrer da pandemia.

A pesquisa também demonstrou que a maior parte dos estudantes acessou os conteúdos relacionados ao ambiente escolar por meio de recursos digitais, principalmente via *website*, rede social ou plataforma de videoconferência, enquanto a utilização de aplicativos das escolas, universidades ou Secretarias de Educação ocorreu em menor medida.

Os dados sobre o ensino remoto auxiliam a demonstrar o cenário de desigualdade que permeia a educação brasileira. A centralização da web e concentração do ensino remoto em poucas e determinadas plataformas também faz parte deste contexto e revela uma preocupação com os dados pessoais das crianças e adolescentes que utilizam as interfaces para acompanharem as aulas e realizarem atividades, especialmente

diante das dinâmicas socioeconômicas próprias de países do sul global, como o Brasil.

Em relação ao tratamento de dados pessoais, cabe destacar que a Lei Geral de Proteção de Dados (Lei nº 13.709/2018, “LGPD”) regulamenta o uso de dados no setor privado e no setor público, em meio físico ou digital, estabelecendo diretrizes para o tratamento de dados pessoais, obrigações para agentes de tratamento e direitos de titulares de dados.

No que diz respeito ao tratamento de dados de crianças e adolescentes, a LGPD traz um dispositivo específico, porém, insuficiente e de difícil interpretação. O artigo 14 da LGPD determina que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. Os parágrafos do referido dispositivo acrescentam algumas previsões, estabelecendo, por exemplo, que o tratamento de dados de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Teixeira e Rettore (2021) apontam que os direitos das crianças e dos adolescentes estão amparados em um importante tripé: (i) a doutrina da proteção integral, pela qual verifica-se um dever social; (ii) a prioridade absoluta; e (iii) o princípio do melhor interesse, que deve ser analisado à luz das condições fáticas vividas pela criança e pelo adolescente, uma vez que se trata de um princípio de conteúdo dinâmico e flexível, a ser estabelecido conforme o caso concreto.

Ao considerar que o melhor interesse deve ser analisado à luz das condições objetivas e subjetivas das crianças e adolescentes - inclusive com relação à exposição deste sujeitos a um ambiente plataformizado, em que há a concentração do espaço virtual na figura de um grupo seleto de empresas de tecnologias - revela-se um caráter contextual da aplicação do princípio do melhor interesse, sem a qual pode-se chegar em um processo denominado, por Stefano Rodotà, de “expropriação da subjetividade” que, ao separar a titularidade dos direitos do exercício destes, em nome da tutela de um sujeito abstrato, retiram-se direitos inerentes aos seres humanos (NEGRI, 2016), como o livre desenvolvimento da personalidade, nos casos de crianças e adolescentes.

Cabe destacar que a proteção da criança e do adolescente em um contexto de tratamento de dados pessoais deve ser amparada em outras normas, como o Estatuto da Criança e do Adolescente (Lei nº 8069/80), o Código de Defesa do Consumidor (Lei nº 8079/90) e a própria Constituição Federal de 1988, que estabelece em seu art. 227 o dever da família, da sociedade e do Estado de assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimen-

tação, 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.

A preocupação com o tratamento de dados de crianças e adolescentes surge, em um primeiro momento, na coleta de dados para cadastro e criação de conta de usuário. Posteriormente, o comportamento apresentado durante o uso da plataforma pode ser convertido em dados e, conseqüentemente, gerar correlações que podem não corresponder à realidade. Nesse sentido, Parra, Cruz, Amiel e Machado (2018) apontam que a concentração da web faz com que seja possível construir uma realidade unidimensional ao apresentar realidades selecionadas para o usuário, a partir da criação de perfis de interesse e com o objetivo de modular o comportamento do indivíduo.

A perfilização (*profiling*) de alunos, como pessoas individualizadas ou como grupo, a partir de dados comportamentais extraídos da utilização de plataformas de ensino remoto, traz à tona questionamentos sobre quais seriam as possíveis consequências da perfilização de crianças e adolescentes durante o ensino remoto. Conforme aponta Doneda (2020), a perfilização permite a obtenção de uma “metainformação”, que traduz hábitos e preferências do indivíduo ou do grupo a partir de métodos estatísticos e de técnicas de inteligência artificial.

Doneda (2020) esclarece que, uma vez que o perfil eletrônico é a única parte da personalidade de uma pessoa exposta a outrem, a consequência é a potencial diminuição de sua liberdade. Nesse sentido, verifica-se que a busca por predições comportamentais, classificações em padrão e correlações em geral pode trazer ainda mais riscos ao titular quando este é uma criança ou adolescente (FERNANDES, KORKMAZ e NEGRI, 2019).

As preocupações decorrentes do tratamento de dados de crianças e adolescentes no contexto de concentração de plataformas no âmbito da educação somam-se aos riscos gerados pelo monitoramento sistemático das atividades acadêmicas, pelo tratamento de dados em grande escala (envolvendo alto número de estudantes e diversos tipos de dados) e pelas possibilidades de perfilização e classificação (*scoring*).

Parra, Cruz, Amiel e Machado (2018) apontam que a concentração de poder em um grupo pequeno de empresas altamente capitalizadas gera uma preocupação sobre o que pode ser feito com esse grande volume de dados extraídos, em especial no que se refere ao monitoramento, vigilância e controle.

Acerca da extração de dados comportamentais, Zuboff (2021) alerta que o imperativo da extração da experiência humana passa a ser conjugado com o imperativo da predição, uma vez que o objetivo do capitalismo de vigilância é “gerar um comportamento que conduza, de forma confiável, definitiva e certa, aos resultados comerciais desejados”, de modo a reduzir a diferença entre predição e observação a fim de se aproximar da certeza.

Por vezes, a arquitetura das plataformas é permeada por opacidade, permitindo que a coleta velada de dados gerem a perfilização de crianças e adolescentes, direcionamento de publicidade e conteúdo em geral. O tratamento de dados pessoais tem o potencial de influenciar escolhas individuais e, como crianças e adolescentes são pessoas vulneráveis em desenvolvimento, esse risco deve ser analisado com atenção.

Henriques, Pita e Hartung (2021) entendem que crianças e adolescentes compõem o grupo mais vulnerável de pessoas cujos dados pessoais circulam, pois vivem período de desenvolvimento físico, cognitivo, psicológico e social. Acerca da vulnerabilidade, Konder e Konder (2021) apontam que este conceito busca demonstrar como determinados grupos, em razão de características específicas, estão mais suscetíveis a certos riscos, relacionados à ameaça de lesão a aspectos existenciais da pessoa humana.

A vulnerabilidade pode ser ilustrada a partir do fato de que, mesmo que as novas tecnologias de informação e comunicação estejam amplamente difundidas entre crianças e adolescentes e - durante a pandemia de Covid-19 - firmaram-se como principal forma de interação entre estudantes e professores, as crianças e os adolescentes, por vezes, não compreendem a complexidade do contexto e das consequências inerentes a utilização dessas ferramentas.

A partir dessa compreensão, Henriques, Pita e Hartung (2021) apontam que o tratamento de dados de crianças e adolescentes pode gerar ameaças à integridade da pessoa, hiperexposição, discriminação, modulação e manipulação de comportamento, microsegmentação da prática abusiva e ilegal da publicidade infantil. Além dos impactos perceptíveis no presente, a hiperexposição pode comprometer o futuro da criança ou do adolescente devido à formação de um “rastros digital”.

Nesse sentido, cabe destacar que Citron e Solove (2020) apontam que o dano à privacidade pode não ser totalmente reconhecível por estar na forma de um risco futuro de lesões, que podem ser variadas. Além disso, os autores destacam que danos

à privacidade geralmente envolvem danos à sociedade e não somente aos indivíduos. Evidentemente, a proteção de dados não tutela somente a privacidade, mas simboliza um parâmetro para as condições de exercício de outros direitos humanos, como o livre desenvolvimento da identidade pessoal, e o dano à privacidade pode ser potencializado no caso de atividade de tratamento envolvendo crianças e adolescentes.

O *Article 29 Data Protection Working Party* em suas *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679* estabelece que crianças são titulares vulneráveis e, por tal razão, o tratamento de dados pessoais será considerado como de risco. Uma das possibilidades de avaliação do risco é analisar a probabilidade - possibilidade de que o fator ou evento apontado venha a ocorrer - e o impacto - gravidade das consequências que seriam verificadas diante da ocorrência de um fator ou evento. Evidentemente, o foco da análise deve ser o risco de dano para direitos e liberdades do titular de dados.

No contexto de utilização de plataformas digitais no ambiente escolar, especialmente quando atividades de profiling, scoring e monitoramento sistemático são realizadas, é necessário avaliar, à luz dos princípios da LGPD, riscos às liberdades civis e aos direitos fundamentais de crianças e adolescentes, conforme elencado abaixo:

Princípio (fundamento legal)	Risco identificado
Princípios da finalidade e adequação (art. 6º, I e II, da LGPD)	Potencial irregularidade e incompatibilidade do uso dos dados coletados no contexto educacional para finalidades secundárias, isto é, para objetivos distintos daqueles que justificaram a coleta de dados de crianças e adolescentes (por exemplo, uso de dados coletados para viabilizar acesso aos materiais educacionais em finalidades secundárias voltadas para desenvolvimento de novos produtos nas plataformas privadas).
Princípio da necessidade (art. 6º, III, da LGPD)	Potencial de coleta excessiva de dados à luz da finalidade de utilização destas plataformas, qual seja, possibilitar o acesso aos conteúdos utilizados no processo de ensino-aprendizagem, ou seja, possibilidade de coleta e armazenamento de dados considerados desproporcionais e excessivos.
Princípios do livre acesso e da transparência (art. 6º, IV e VI, da LGPD)	Ausência de informações fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais de crianças e adolescentes. Além disso, é recomendável que as informações sejam fornecidas de modo assertivo, evitando o excesso informacional (<i>overload information</i>).

Princípio da segurança (art. 6º, VII, da LGPD)	Considerando-se o tratamento de dados de crianças e adolescentes (titulares vulneráveis) é realizado em larga escala e caracteriza-se como atividade uma das atividades centrais do modelo de negócios de plataformas, faz-se necessário avaliar as medidas de segurança adotadas, de modo a garantir que acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão não ocorram.
Princípio da não discriminação (art. 6º, IX, da LGPD)	Potenciais discriminatórios, privações relacionadas a direitos fundamentais e limitações de acesso a direitos e/ou oportunidades devem ser analisadas à luz do princípio da não discriminação, uma vez que a lei proíbe o tratamento para fins discriminatórios ilícitos ou abusivos.

O relatório de impacto à proteção de dados pessoais pode auxiliar na identificação e minimização dos riscos envolvendo o tratamento de dados de crianças e adolescentes. O art. 5º, XVII, da LGPD, estabelece que o relatório é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais de titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Kloza (2014) destaca que a gestão de risco e a verificação de conformidade legal são os elementos centrais de avaliações de impacto e, a partir de uma metodologia de gestão de risco adequada, todos os riscos possíveis e outros impactos negativos sobre a privacidade podem ser identificados e idealmente mitigados, de modo que eventuais riscos residuais são justificados e registrados.

A tipologia de riscos adotada pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) ao tratar da presença de menores no ambiente digital está baseada em quatro “Cs”: (i) conteúdo: potencial de que crianças e adolescentes tenham contato com conteúdos danosos, como conteúdo violento, discriminatório ou de ódio; (ii) contato: potencial de que estes sujeitos estejam envolvidos em atividades com agentes maliciosos, por exemplo, em situações de aliciamento, exploração e assédio; (iii) conduta: potencial de dano quando crianças e adolescentes interagem com outros membros desse grupo, como bullying, sexting, intimidação etc.; e (iv) contrato (também denominado risco comercial): potencial risco decorrente de relações contratuais abusivas, por exemplo, fraudes, golpes, uso indevido e apropriação indevida da propriedade intelectual.

Ressalta-se que a experiência de risco e dano poderá impactar crianças e adolescentes de modo distinto, conforme fatores verificados em cada situação concreta,

incluindo, mas não se limitando a gênero, idade, circunstâncias familiares, estatuto socioeconômico, localização e experiências e disponibilidade de tecnologia digital (5RIGHTS FOUNDATION).

É importante notar que os recentes movimentos regulatórios observados na União Europeia, no campo da inteligência artificial, estão fundamentados em uma abordagem baseada no risco, que modula o conteúdo das normas de acordo com a intensidade dos riscos criados pelos sistemas de IA⁷. A construção de relatórios de impacto à proteção de dados deve observar classificações de risco adotadas pelo ordenamento jurídico e por autoridades públicas que atuam no tema.

Nesse sentido, a título de exemplificação, observa-se que a proposta de regulamento sobre inteligência artificial, apresentada no âmbito da União Europeia, traz a classificação de (i) risco inaceitável (art. 5º), pelo qual os sistemas de IA devem ser proibidos; (ii) risco elevado (art. 6º), gerando restrições e obrigações, inclusive a implementação de um sistema de gestão de riscos contínuo, que deve estar presente durante todo o ciclo de vida, ou seja, até mesmo antes da colocação destes sistemas no mercado; (iii) risco limitado, do qual decorrem obrigações de transparência; e (iv) risco mínimo, no qual não há intervenção do regulamento.

Esse cenário evidencia a possibilidade de que, futuramente, o ordenamento jurídico brasileiro estabeleça quais práticas serão classificadas como de risco inaceitável para a proteção de dados de crianças e adolescentes e, conseqüentemente, determine quais práticas de negócio serão proibidas.

Outra ferramenta essencial para assegurar a proteção de dados de crianças e adolescentes é o estabelecimento de canais de atendimento direto aos titulares, por meio dos quais é possível realizar solicitações de modo simplificado e facilmente acessível. A LGPD prevê que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, incluindo informações sobre os direitos do titular, com menção explícita aos direitos previstos no art. 18.

No contexto de tratamento de dados de crianças e adolescentes, ressalta-se que, conforme estabelece o art. 14, §6º, da LGPD, as informações sobre o trata-

⁷ Em 21 de abril de 2021, a Comissão Europeia apresentou a Proposta de Regulamento sobre a Inteligência Artificial (*Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union Legislative Act*), com o objetivo de estabelecer um quadro jurídico uniforme para o desenvolvimento, a comercialização e a utilização da inteligência artificial no âmbito da União Europeia.

mento de dados de crianças e adolescentes devem ser fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário. Desse modo, a disponibilização de canais diretos de atendimento - acessíveis e adequados aos usuários de plataformas digitais utilizadas durante o ensino remoto - auxilia na concretização dos direitos previstos pela LGPD.

Desse modo, as ferramentas de accountability, como o relatório de impacto à proteção de dados pessoais, e de transparência ativa e passiva, como os avisos de privacidade e os canais de atendimento, especialmente com relação aos contratos celebrados entre escolas de ensino básico e grandes empresas de tecnologia, assumem um papel fundamental para a concretização do princípio do melhor interesse, tendo em vista que a utilização de tais ferramentas permitiria o controle externo, por parte da sociedade civil, das atividades de tratamento de dados pessoais decorrentes da implementação e utilização de plataformas educacionais.

A perspectiva relacional do melhor interesse da criança e do adolescente, isto é, a análise contextual das situações nas quais crianças e adolescentes estão inseridas deve, portanto, levar em consideração a concentração de plataformas digitais voltadas para a educação e, a partir desse cenário, buscar meios que assegurem a autonomia informativa.

Em uma dimensão informacional, a privacidade passa a ser compreendida como o direito de manter controle sobre as próprias informações, nesse sentido dispôs Rodotà (2008) ao afirmar que o direito à privacidade deixa de estar baseado no eixo “pessoa-informação-segreto”, e passa a estar fundamentado no eixo “pessoa-circulação-controle”. Tal controle pode ser operacionalizado por meio de práticas de transparência que garantam o livre acesso às informações e possibilitem a fiscalização por parte da sociedade.

Desse modo, tem-se que a proteção de dados é fundamental para que o ambiente escolar atue com autonomia ao construir um processo de ensino-aprendizagem crítico e possibilitar o desenvolvimento da pessoa. Além disso, o desenvolvimento de uma cultura de proteção de dados em escolas e universidades faz parte do fortalecimento do ensino democrático e possibilita a conscientização de estudantes e da sociedade como um todo.

CONCLUSÃO

O presente trabalho buscou verificar quais são os riscos para a privacidade e proteção de dados de crianças e adolescentes diante da adoção massiva de plataformas digitais voltadas ao ambiente escolar no contexto de países do sul global, como o Brasil. Em primeiro lugar, a discussão passa pelo movimento de concentração da Web e desenvolvimento do Capitalismo de Vigilância, além de explorar as narrativas do solucionismo tecnológico na educação.

A economia política da Internet permite que se faça uma análise mais apurada das dinâmicas que dizem respeito ao desenvolvimento da Internet ao longo do tempo. A modificação na estrutura econômica da Internet no final dos anos 1990 e início dos anos 2000 foi uma das principais responsáveis pela guinada privatista no interior da Internet, de modo que houve um intenso aumento na criação de empresas cujos serviços estão baseados na rede das redes.

Durante esse mesmo período, o referido deslocamento na estrutura econômica da Internet provocou uma intensa crise financeira no setor de tecnologia que culminou em um processo massivo de fusões, resultando na formação do atual oligopólio de empresas de tecnologia, também conhecido como GAFAM, acrônimo para Google, Amazon, Facebook, Apple e Microsoft. A formação desse oligopólio foi fundamental para a descoberta da informação ou, mais precisamente, a descoberta do dado como matéria prima fundamental dos modelos de negócio dessas empresas, inaugurando o que se chama Capitalismo de Vigilância.

Além disso, a análise do impacto da concentração de plataformas deve levar em consideração a vulnerabilidade dos titulares e a gravidade dos danos projetados no futuro, uma vez que o próprio desenvolvimento do titular poderá ser afetado. O tratamento de dados de crianças e adolescentes em larga escala, monitoramento constante do período de aprendizagem, o potencial discriminatório, a possibilidade de decisões automatizadas e limitação ao acesso de benefícios e oportunidades são fatores de risco que devem ser analisados.

Considerando-se que, atualmente, a proteção de dados não está restrita à proteção da privacidade e da intimidade, mas relaciona-se com Estado Democrático e com o exercício de outros direitos humanos, como liberdade de expressão e liberdade de profissional, é possível verificar a importância da construção de uma cultura de proteção de dados no ambiente escolar.

REFERÊNCIAS

5RIGHTS FOUNDATION. The risks: Content, Contact, Conduct and Contract. Disponível em: <https://www.riskyby.design/the-risks>. Acesso em: 5 nov. 2021.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento, 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo; ZANATTA, Rafael Augusto Ferreira. Direito e economia política dos dados: um guia introdutório. In DOWBOR, Ladislau (Org.). Sociedade Vigida: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instalar uma nova distopia. São Paulo: Autonomia Literária, 2020, p. 67-90

BOLAÑO, César Ricardo; HERSCOVICI, Alain; CASTAÑEDA, Marcos; VASCONCELOS, Daniel. Economia Política da Internet. Universidade Federal de Sergipe. Aracaju: Editora UFS. Vol. I, 2007.

BOLAÑO, César Ricardo S.; VIEIRA, Eloy S. Economia Política da Internet e os sites de redes sociais. **Revista EPTIC**, v. 16, n. 2, mai/ago, 2014. Disponível em: <<https://seer.ufs.br/index.php/eptic/article/view/2168/1947>>. Acesso em: 11 set. 2021

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 9 jul. 2021.

BRASIL. Lei n. 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Lex: Estatuto da Criança e do Adolescente*. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8069.htm. Acesso em: 9 jul. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 9 jul. 2021.

CITRON, Danielle Keats; SOLOVE, Daniel J., Privacy Harms. SSRN, 2021, Disponível em: <<http://dx.doi.org/10.2139/ssrn.3782222>>. Acesso em: 9 jul. 2021.

CRUZ, Leonardo Ribeiro da. Tecnologias educacionais da google e o avanço do capitalismo de vigilância na educação pública brasileira. **Anais eletrônicos [...] II Encontro da Rede de Pesquisa em Governança da Internet**, 4 de Novembro, 2018. Disponível em: <https://drive.google.com/file/d/1YNXsV3uZ8GTtaHdDR-Er71FHqelhci3_/view>. Acesso em 9 jul. 2021.

CRUZ, Leonardo Ribeiro da; VENTURINI, Jamila Rodrigues. Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19. **Revista Brasileira de Informática e Educação**, v. 28, [s.l.], 2020. Disponível em: <<https://www.br-ie.org/pub/index.php/rbie/article/view/v28p1060>>. Acesso em: 08 set. 2021.

DEMENTSHUK, Márcia; HENRIQUES, Percival. Pássaros voam em bandos: a história

da Internet do século XVIII ao século XXI. João Pessoa: Editora ANID, 2019.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EDUCAÇÃO VIGIADA. Mapeamento, 2021. Disponível em: <<https://educacaovigiada.org.br/>>. Acesso em: 9 jul. 2021.

EPSTEIN, Lee; KING, Gary. Pesquisa empírica em direito: as regras de inferência. São Paulo: Direito GV, 2013.

ESTADO DE MINAS GERAIS. Resolução nº 4310, de 2020. **Resolução See Nº 4310/2020**. Belo Horizonte, Disponível em: <https://www2.educacao.mg.gov.br/imagens/documentos/Resolucao%20SEE_N_4310.pdf>. Acesso em: 11 set. 2021.

FERNANDES, Elora Raad; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; NEGRI, Sergio Marcos Carvalho de Ávila. *A proteção integral de crianças e adolescentes: desafios jurídicos de uma sociedade hiperconectada. Ciência, Tecnologia e Inovação: Políticas e Leis*. Florianópolis: Tribo da Ilha, 2019

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008.

GROULX, Lionel-H. Contribuição da pesquisa qualitativa à pesquisa social. In: POUPART, J.; DESLAURIERS, J.-P.; GROULX, L.-H.; LAPERRIÈRE, A.; MAYER, R.; PIRES, Á. (eds.). *A pesquisa qualitativa: enfoques epistemológicos e metodológicos*. Petrópolis: Vozes, 2008.

HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes In: MENDES, Laura Schertel et al (org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 199-225.

KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Disponível em: <<https://researchportal.vub.be/en/publications/privacy-impact-assessments-as-a-means-to-achieve-https://researchportal.vub.be/en/publications/privacy-impact-assessments-as-a-means-to-achieve-the-objectives-of-the-objectives-o>>. Acesso em: 01/11/2021.

KONDER, Carlos Nelson; KONDER, Cíntia Muniz de Souza. Da vulnerabilidade à hipervulnerabilidade: exame crítico de uma trajetória de generalização. **Interesse Público [Recurso Eletrônico]**. Belo Horizonte, v.23, n.127, maio/jun. 2021. Disponível em: <https://dspace.almg.gov.br/handle/11037/41221>. Acesso em: 20 jul. 2021.

MARRAFON, Marco Aurélio; FERNANDES, Elora Raad. A, B, C, Google: Riscos ao Direito Fundamental à Proteção de Dados de Crianças e Adolescentes no G Suite for Education. **Revista de Direito Público**, v.17. Brasília, 2020, p.202-229. Disponível em <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4094/Marrafon%3B%20Fernandes%2C%202020>>. Acesso em: 9 jul. 2021.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big Data: A revolution that will transform how we live, work and think. Londres: John Murray Publishers, 2013.

MOROZOV, Evgeny. Solucionismo, nova aposta das elites globais. Traduzido por: Simone Paz. Outras palavras, 2020. Disponível em: <<https://outraspalavras.net/tecnologiaemdisputa/solucionismo-nova-aposta-das-elites-globais/>>. Acesso em: 11 set. 2021

MOROZOV, Evgeny. Big Tech: A ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

NEGRI, Sergio Marcos Carvalho de Ávila. As razões da pessoa jurídica e a expropriação da subjetividade. Civilistica.com. Rio de Janeiro, a.5, n. 2, 2016. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/265/215>>. Acesso em: 07 nov. 2021

NIC.BR – NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. TIC Kids Online Brasil 2019: pesquisa sobre o uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2020a. Disponível em: <https://cetic.br/media/analises/tic_kids_online_brasil_2019_coletiva_imprensa.pdf>. Acesso em: 9 jul. 2021.

NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Painei TIC Covid-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus, 3. ed. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2020b. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20201104182616/painel_tic_covid19_3edicao_livro%20e%20letr%C3%B4nico.pdf>. Acesso em: 11 set. 2021.

NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. TIC Educação 2020: Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas escolas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2021. Disponível em: <<https://cetic.br/pt/pesquisa/educacao/indicadores/>> . Acesso em: 11 set. 2021.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Children in the digital environment. OECD Digital Economy Papers, [s.l.], 8 jan. 2021. <http://dx.doi.org/10.1787/9b8f222e-en>.

PARRA, Henrique; CRUZ, Leonardo; AMIEL, Tel; MACHADO, Jorge. Infraestruturas, economia e política informacional: o caso do google suite for education. **Mediações - Revista de Ciências Sociais**, [S.L.], v. 23, n. 1, p. 63, 6 jul. 2018. Universidade Estadual de Londrina. <http://dx.doi.org/10.5433/2176-6665.2018v23n1p63>. Disponível em: <http://www.uel.br/revistas/uel/index.php/mediacoes/article/view/32320>. Acesso em: 08 set. 2021.

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. 1 ed. Rio de Janeiro: Renovar, 2008.

SECRETARIA DE ESTADO DE EDUCAÇÃO DE MINAS GERAIS. Estude em casa, em 2021. Disponível em: <<https://estudeemcasa.educacao.mg.gov.br/inicio>>. Acesso em: 11 set. 2021.

SILVEIRA, Sergio Amadeu da. O mercado de dados e o intelecto geral. **Margem Esquerda**, n. 36, 2021.

SPOSITO, Eliseu Savério. Redes e Cidades. São Paulo: Editora Unesp, 2008.

SRNICEK, Nick. Platform Capitalism. Cambridge: Polity Press, 2017.

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

VALENTE, Jonas Chagas Lúcio. Plataformas digitais e concentração na Internet. **Anais eletrônicos [...] III Encontro da Rede de Pesquisa em Governança da Internet**, 1 de Outubro, 2019. Disponível em: <<https://drive.google.com/file/d/1f37nWQXul6RzYDs-RLx7LglDo2m-iuCaw/view?usp=drivesdk>>. Acesso em: 9 jul. 2021.

VAN DIJCK, José. Confiamos nos dados? As implicações da datificação para o monitoramento social. **MATRIZES**, v.11, n.1 jan./abr. São Paulo, 2017. Disponível em: <<https://doi.org/10.11606/issn.1982-8160.v11i1p39-59>>. Acesso em: 9 jul. 2021.

VAN DIJCK, José. Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. **Surveillance & Society**, [s.l], v. 12, n. 2, p. 197-208, maio 2014. Disponível em: <<https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication>>. Acesso em: 17 fev. 2021.

ZANATTA, Rafael Augusto. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 9 jul. 2021.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.