POLICY PAPER

EDUCAÇÃO, PRIVACIDADE E TRANSPARÊNCIA: UMA ENCRUZILHADA DE DIREITOS

Resumo:

A privacidade, aliada ao acesso à informação, deve ser alçada ao centro da agenda de defesa do direito à educação. Isso porque, em um contexto de baixa transparência e de escassa regulação nos países da América Latina e Caribe, o tratamento inadequado dos dados pessoais da comunidade educativa pode aprofundar ainda mais as desigualdades existentes, além de provocar novas violações de direitos fundamentais. Este *policy paper* se propõe a apresentar aos integrantes da Rede da Campanha Latino-americana pelo Direito à Educação (CLADE) um panorama sobre os principais conceitos e desafios relacionados à privacidade e à proteção de dados pessoais no contexto educativo. Com o documento, pretende-se iniciar um debate sobre o tema, elencando os pontos de atenção para o campo e delineando uma proposta de agenda e de caminhos possíveis para incidência.

Introdução

Existe hoje um complexo mercado de dados pessoais em funcionamento no mundo, do qual todos nós somos ativos partícipes — estejamos conscientes do nosso papel, ou não. Se, há duas décadas, *Compact Discs* (CDs) gravados com nossos dados cadastrais — números de identidade, endereços e telefones — até povoavam os recônditos de mercados informais de São Paulo, Bogotá ou Cidade do México, a situação atual é a um só tempo maior, mais grave e mais invisível. Os dados se tornaram as **"pegadas" digitais de cada um**, gerados a cada instante e lugar em cada aparelho, dispositivo fixo ou móvel, nos sites que navegamos, imagens e sons que captam de nós, além do que fornecemos de maneira consentida ou inadvertida. Trata-se de um **fluxo constante de dados**, armazenados e compartilhados por meio de intrincadas infraestruturas digitais entre diferentes atores institucionais e corporativos, formal e informalmente, com funções distintas nessa cadeia de valor.

O campo da educação, especialmente pública, é percebido pelos atores desse mercado como amplo terreno a ser explorado e expandido. Em primeiro lugar, porque o próprio Estado reúne, tradicionalmente, grande quantidade de dados a respeito das cidadãs e dos cidadãos para operacionalizar as políticas e os serviços públicos. Em segundo, porque esse movimento de busca por exploração econômica (ou "comoditização") de dados pessoais encontra e potencializa outro: a privatização da educação. Os dados coletados ou a atenção dispensada pelos usuários a eventual publicidade passam a ser mais valiosos que o próprio *software* — esses produtos, antes comercializados, chegam a ser "doados" ou fornecidos "gratuitamente".

Como se argumentará ao longo deste documento, esses mecanismos de usurpação e desvio de finalidade de dados pessoais da comunidade educativa têm potencial de aprofundar desigualdades e tornar ainda mais vulneráveis grupos historicamente expostos a processos de exclusão e discriminação. E um vírus, não de computador, pode ter acelerado enormemente esse processo: a situação de calamidade pública instalada ao longo de 2020 com a pandemia de Covid-19 impôs a

adoção mais rápida e ampla já vista de tecnologias para ensino a distância e comunicação entre estudantes e docentes. Muitas vezes, sem a devida transparência da doação ou contratação pública das tecnologias em questão.

Toda essa situação colocou o campo da defesa do direito à educação diante de uma verdadeira "encruzilhada de direitos": transparência versus privacidade. Ao mesmo tempo em que é preciso reafirmar e conter retrocessos no direito à privacidade, também é preciso pleitear o resgate da noção de **dados públicos como um bem comum**. A realização dessa ideia depende de uma governança pública, em que o Estado se coloque como garantidor desses direitos.

Desde que não exponham indivíduos, os dados devem ser tratados com a máxima transparência — incluindo a do código-fonte das tecnologias adotadas para as atividades educacionais. O direito de acesso à informação e o direito à privacidade não são direitos conflitantes, mas complementares. Juntos, contribuem para a plena garantia do direito à educação.

Este documento é um convite para iniciar um debate. Está estruturado em quatro partes: (I) a primeira seção define os principais **conceitos** de privacidade e transparência do ponto de vista dos direitos humanos e posiciona a noção de **dados pessoais no contexto educacional**; (II) a segunda parte traz o pano de fundo político e econômico do processo de coleta e compartilhamento de dados pessoais, sobretudo a noção de **capitalismo de vigilância** e a **privatização da educação**; a seção seguinte (III) detalha práticas existentes e os riscos desse processo especificamente para o campo educacional. A quarta parte (IV) propõe uma agenda inicial para o campo, com recomendações de temáticas de incidência sobre privacidade e proteção de dados na educação. Espera-se que, como ponto de partida, o material contribua para gerar reflexão e identificar futuras ações.

I. Conceitos e definições essenciais

Cada um de nós tem o direito de **estar a sós** com seus próprios pensamentos e emoções. Esse princípio se mantém, mas os contornos da noção de **privacidade** têm se transformado desde o artigo dos juristas Samuel Warren e Louis Brandeis, escrito em 1890 e considerado um marco dessa definição (WACKS, 2010). Atualmente, ganha peso a ideia de que a privacidade compreende também o direito de o indivíduo **controlar aquilo que é coletado sobre si** — a proteção de dados. Nunca faltaram interessados em minimizar a importância da privacidade e decretar que ela "morreu".

O sentido do debate sobre a privacidade vive de maneira inequívoca no campo dos direitos e liberdades fundamentais. A afirmação de que "ninguém será sujeito a interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência" está expressa no Artigo 12 da **Declaração Universal dos Direitos Humanos** (1948), assim como o direito à proteção contra esse tipo de ataque. Texto semelhante está enunciado no Artigo 17 do **Pacto Internacional sobre os Direitos Civis e Políticos** (1966), adotado pela Assembleia Geral da Organização das Nações Unidas (ONU) para desenvolver a Declaração de maneira pormenorizada. O termo "correspondência", que os textos buscam proteger, abrange toda forma de comunicação telefônica, telegráfica ou telemática, como a internet. E não apenas do

poder público, mas também — e, cada vez mais — de atores privados (COMPARATO, 2010).

Ainda no campo dos direitos humanos, privacidade e proteção de dados pessoais são considerados fundamentais para a **governança democrática da internet**. O Fórum de Governança da Internet (IGF, na sigla em inglês), plataforma global vinculada ao sistema ONU, reúne pesquisadores, representantes de governos, de empresas e da sociedade civil para a discussão de políticas públicas relativas ao tema. Em suas diversas declarações e documentos de trabalho, o IGF "atualiza" os direitos humanos para o contexto da sociedade conectada em rede. Entre os princípios estabelecidos, está o direito de toda pessoa de não ser submetida a vigilância, de navegar por infraestruturas íntegras, a necessidade de estados regularem a proteção de dados em normativos nacionais etc.[1].

Os ***dados pessoais***, foco de proteção dos direitos já mencionados, são definidos de maneira abrangente, na legislação europeia e em outros marcos normativos mundiais, como

> *informação relativa a uma **pessoa viva**, **identificada** ou **identificável**. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa*[2].

Mesmo que a informação obtida não contenha forma direta de identificação (por exemplo, o nome, ou um número de identidade), ou mesmo que tenha sido tratada para eliminar esse tipo de característica, o fato de ter outros elementos que tornem o indivíduo *identificável* já tornam aquele dado *pessoal*. Por outro lado, bases de dados que possam ser efetivamente *anonimizadas*, ou seja, que não permitam processos de "engenharia reversa" (chamados de "reidentificação") para apontar a identidade de pessoas específicas, podem ser tornadas públicas em políticas responsáveis de transparência e dados abertos. O quadro abaixo traz exemplos do que poderiam ser considerados dados pessoais no contexto de políticas educacionais.

QUAIS DADOS SÃO RELACIONADOS A PESSOAS NAS INSTITUIÇÕES EDUCATIVAS?

A definição de dados pessoais depende do contexto em que estão inseridos. De forma geral, são dados relacionados a uma pessoa e que, isolados ou em conjunto, permitem identificá-la. Este quadro lista tipos de dados que podem ser coletados pelas tecnologias implementadas, adotadas ou contratadas por instituições educativas. Alguns podem ser anonimizados e, com tratamento adequado, tornarem-se bases de dados abertos ou agregados para pesquisa, por exemplo. Mas, se expostos ou desviados da finalidade original, representam sérios riscos aos indivíduos.

Categorias	Tipos de dados coletados e armazenados	Exemplos de tecnologias que os captam

[1] A "Carta de Direitos Humanos e Princípios da Internet" pode ser consultada em: https://internetrightsandprinciples.org/charter/. Último acesso em 09/11/2020.

[2] Referências sobre as definições e a legislação correspondente disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt#referncias. Último acesso em 29/10/2020.

Biometria	Registros como imagens do rosto, impressões digitais e gravação da voz.	Ferramenta que atesta presença de educandos por reconhecimento facial; catracas de acesso à unidade educacional com impressão digital.
Cadastro	Nome do(a) educando(a) e responsáveis, endereço, telefone, matrícula etc.	Sistema de matrícula online; sistema de gestão de pessoas.
Identidade digital	Endereço de IP (protocolo de internet único da conexão); cookies ("testemunhos" de conexão); ID de publicidade do celular; endereço MAC de um dispositivo eletrônico.	Registros feitos por plataformas de cursos EaD; Identificadores de notebooks e tablets distribuídos a cada estudante ou professor.
Cotidiano escolar	Dados operacionais sobre as atividades educativas, tais como frequência escolar, alocação em turma, transferências e outras ocorrências.	Aplicativo ou sistema de diário de classe; aplicativo para agenda ou comunicação com responsáveis.
Avaliação	Dados sobre desempenho de estudantes e docentes, tais como resultados de avaliação, notas, boletins escolares, fluxo escolar etc.	Aplicativo para correção automatizada de avaliações; painel analítico de avaliação de desempenho.
Comportamento	Histórico de navegação pela internet, aplicativos instalados, histórico de deslocamento (geolocalização).	Perfil de usuário no Google; sensores de smartphones.
Personalidade e atitudes	Dados coletados ou inferidos com aparatos digitais, tais como emoções, concentração, dispersão, relacionamentos.	Câmeras em sala de aula ou ambiente escolar; navegação no "feed" das redes sociais (Facebook, Instagram).
Identidade pessoal e preferências	Dados coletados ou inferidos com aparatos digitais, tais como convicção religiosa, origem étnica ou racial, identidade de gênero, orientação sexual, opinião política, saúde.	Registro de interesses manifestados em rede social (Facebook) ou buscas.

Fonte: Elaboração própria.

Entre todos esses dados pessoais que devem ser protegidos, duas dimensões merecem atenção especial: os chamados dados sensíveis e os dados cujos titulares são crianças e adolescentes. Para esses dados, a legislação reserva condições de tratamento específicas e camadas de proteção extra.

Dados pessoais sensíveis[3] são aqueles que revelem:

- a origem racial ou étnica ou convicções políticas, religiosas ou filosóficas;
- filiação sindical;
- dados genéticos e biométricos;
- dados relacionados à saúde;
- dados relativos à identidade de gênero, vida sexual ou orientação sexual.

[3] De acordo com o normativo europeu, disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_pt. Último acesso em 29/10/2020.

O tratamento de **dados de crianças e adolescentes** deve ser analisado sob a ótica do marco normativo de proteção de seus direitos, como a Convenção sobre os Direitos da Criança, adotada pela Assembleia Geral da ONU em 1989. O princípio do **melhor interesse**, previsto na Convenção e reafirmado pelas constituições nacionais e Estatutos da Criança e do Adolescente, deve nortear as decisões sobre como tratar esses dados. Ele prevalece sobre eventuais conflitos — caso o uso do dado de uma criança contrarie o seu melhor interesse, deve ser coibido, mesmo que haja consentimento dos responsáveis. O limite de idade segue o regramento local.

Ao contrário do que se possa imaginar, o marco normativo de proteção de dados não versa apenas sobre violações como situações de vazamento, invasão de sistema ou compartilhamento indevido de dados. O debate legal sobre privacidade vem se pautando com frequência nas noções de **tratamento de dados** e **consentimento**.

O *tratamento de dados* é um conjunto amplo de operações efetuadas sobre dados pessoais, por meios manuais ou automatizados. Basicamente, é **tudo o que se possa fazer com informação**: coleta, registro, organização, estruturação, conservação, adaptação, alteração, recuperação, consulta, utilização, divulgação, cruzamentos, limitação, apagamento ou destruição de dados pessoais[4].

As instituições educativas são consideradas **responsáveis pelo tratamento,** sempre que determinem a finalidade e os meios de uma dessas operações com dados pessoais da comunidade educacional. Inclusive se optarem pela contratação de terceiros. Ou seja, não são somente os governos e secretarias/departamentos públicos de educação os responsáveis que devem ser cobrados por políticas de proteção de dados pessoais. Cada unidade que operacionaliza a política pública de educação e que lida com tecnologias, administrativas ou pedagógicas (vide exemplos na tabela acima), também o é. A comunidade educativa deve saber exatamente o que se faz com seus dados. Daí a necessidade de o tratamento ser, sempre, acompanhado de políticas de transparência e prestação de contas (*accountability*).

O papel do **consentimento** também vem ganhando proeminência no debate. Ele costuma ser definido como a "manifestação de vontade, livre, específica, informada e explícita, por meio da qual a pessoa titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[5]. É nas **políticas de privacidade** — os contratos em "letrinhas miúdas" de aplicativos e serviços online — que esse consentimento costuma ser coletado.

Finalmente, chama-se **violação de dados pessoais** uma brecha da segurança que provoque, de modo *ilícito* ou até *acidental*, destruição, perda, alteração, divulgação ou acesso não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento[6].

PARA LEMBRAR: CONCEITOS E IDEIAS-CHAVE

[4] Definição e referências na legislação europeia disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_pt. Último acesso em 29/10/2020.

[5] Definição presente no Artigo 4º, Inciso XI, da GDPR europeia; o conceito é replicado em diversos outros normativos nacionais.

[6] Definição presente no Artigo 4, Inciso XII, da GDPR europeia.

Dados pessoais	Dados que permitam identificar direta ou indiretamente um indivíduo de forma inequívoca
Dados sensíveis	Revelam convicções, aspectos de saúde ou origem étnica e racial, por ex.; recebem camada extra de proteção.
Dados de crianças e adolescentes	Devem ser tratados sob a ótica do melhor interesse dos vulneráveis; recebem mecanismos extra de proteção, incluindo consentimento de responsáveis.
Tratamento de dados	Basicamente toda operação que se possa fazer com dados, desde a coleta ao compartilhamento, passando pela armazenagem.
Consentimento	Manifestação de concordância informada e explícita do usuário a respeito de um tratamento específico de seus dados.
Responsáveis pelo tratamento	Instituições ou pessoas que definem a finalidade e a forma de tratar os dados pessoais em questão. Pode ser uma unidade educacional, um diretor de escola ou uma secretaria de governo.
Violação de dados pessoais	Situação ilícita ou acidental em que os dados pessoais recebem qualquer tratamento não autorizado, por má-fé ou inépcia.

Fonte: elaboração própria.

II. Pano de fundo

Os dados obtidos e monetizados por meio de vigilância tecnológica tornaram-se tão centrais para o funcionamento dessa "nova economia" baseada na internet que inspiraram uma nova roupagem para o capitalismo: o **capitalismo de vigilância** (ZUBOFF, 2015). Esse sistema tem como um de seus principais insumos os fluxos de atenção individual, e os dados coletados são matéria-prima para analisar e prever gostos, interesses e desejos (SILVEIRA, 2017).

Nos últimos anos, de forma bastante acelerada, esse mercado vem se tornando mais complexo, gerando estudos sobre a "microeconomia da interceptação de dados pessoais" (SILVEIRA, 2017, 832:834). Existem, por exemplo, agentes especializados em fazer a "corretagem" ou negociação desses dados (*data brokers*), substitutos mais lucrativos e legalizados dos vendedores ambulantes que vendiam CDs com dados vazados. A tabela abaixo resume esse mercado em quatro camadas de funcionamento.

O FUNCIONAMENTO DO MERCADO DE DADOS EM CAMADAS

1. Coleta e armazenamento	Plataformas de relacionamento online, sites, mecanismos de pesquisa e de rastreamento de navegação, formulários online, sensores espalhados nas cidades, antenas de celulares etc.

2. Processamento e mineração	Tratamento e agregação dos dados coletados e armazenados, reunindo-os com outros disponibilizados publicamente ou fornecidos por diferentes fontes. Visa aprimorar e enriquecer um perfil pessoal mais detalhado, por meio de algoritmos e tentativas de uso de softwares de inteligência artificial.
3. Análise e formação de amostras	Usadas por departamentos de marketing de empresas e pelas plataformas que organizam a venda dos públicos segmentados e das chamadas audiências semelhantes ("lookalikes")
4. Modulação	Oferta de produtos e serviços a partir das estratégias de venda traçadas após as análises. Inclui os dispositivos de filtro, formação de bolhas ou *clusters* de consumidores. Também está incluída a atividade de venda final dos produtos considerados adequados a públicos específicos.

Fonte: elaborado a partir das definições e tipologia proposta por Sérgio Amadeu da Silveira (2017, 892:921)

A ideia de que "a privacidade morreu" é evocada por atores da indústria de tecnologia para justificar a coleta indiscriminada de dados pessoais. Esse discurso, cada vez mais comum, se tornou um dos maiores empecilhos para reivindicar o direito à proteção de dados no debate público. Para o público em geral, a barganha pode soar justa: qual o problema em fornecer informações pessoais em troca de serviços gratuitos como jogos e aplicativos de comunicação que me são úteis? *Afinal* — também se diz com frequência — "*não tenho nada a esconder*".

O problema é que as pesso**as não costumam saber a extensão dos dados que estão sendo coletados** sobre elas. Mais ainda, **desconhecem os usos** que podem ser feitos deles, e as consequências imediatas e futuras dessa concessão.

Esses dados são muitas vezes usados para *data profiling* — processos automatizados para construir perfis individuais detalhados visando "prever" e induzir comportamentos. Isso ocorre por meio da coleta e análise de "pegadas digitais" durante a navegação pela internet e uso de aplicativos.

O perfil digital é construído por meio do mercado apresentado no quadro acima. Ele classifica as pessoas individualmente em dezenas de milhares de categorias, de acordo com atributos e pontuações ("scores") de educação, emprego, visões políticas, interesses de saúde, religião e origem étnica, usos de mídia, consumo, renda, estabilidade econômica e personalidade. Também incluem análises de seus comportamentos online, inclusive tipos de sites e conteúdos visitados, interesses, incluindo tópicos sensíveis. Uma das empresas com a maior base de dados sobre consumidores do mundo, a Acxiom já dizia ter, em 2013, até 3 mil atributos sobre 700 milhões de pessoas. A Oracle, gigante de tecnologia, diz fornecer mais de 30 mil elementos sobre 2 bilhões de perfis (CHRISTL; KOPP; RIECHERT, 2017).

A esta altura, já fica evidente que esse mercado e suas técnicas de "perfilamento" não servem somente a fins publicitários. O mundo do trabalho e do emprego, o setor imobiliário, as companhias de seguro e de crédito, até mesmo as dinâmicas da democracia e do debate eleitoral, do sistema de justiça e do estado de bem-estar social — todos esses campos começam a ser afetados pelo uso de tecnologias, dos algoritmos e das decisões automatizadas que se alimentam desses dados. E é por isso que, quando direcionadas a grupos tradicionalmente marginalizados, essas tecnologias podem acentuar a desigualdade, criando um verdadeiro "feedback loop de injustiça" (GANGADHARAN, 2017). Exemplos desses efeitos serão tratados na seção seguinte.

Na educação, este processo se encontra e se potencializa com outro em curso nas últimas décadas: as diferentes formas de **privatização das políticas educacionais**, bem como a imbricada relação entre o setor público e o privado nas redes de ensino latino-americanas. Em um mapeamento da literatura que abarcou o período de 1990 a 2014, tratando das formas recentes da privatização da educação básica no Brasil e outros países, Adrião (2018) apontou a "compra ou adoção de tecnologias educacionais e demais insumos escolares desenvolvidos pelo setor privado" como um tipo específico de privatização dos processos pedagógicos/currículo.

Por "tecnologias educacionais"[7] entende-se a oferta de "livros, conteúdos digitais, acessos a plataformas e sistemas de informação para redes públicas e escolas privadas" (p.15). Na esteira desse processo, surge uma nova face desses mercados: as *edtechs*. A sigla, do inglês *Education and Technology*, denomina de forma abrangente as empresas de produtos para o setor educacional — tanto de hardware (equipamentos), quanto de software (aplicativos, programas e sistemas). A moda de juntar o sufixo "tech" ao prefixo da "indústria" (*agro*, *gov*, *ad*, *fin*, *legal*, *health*) em geral pretende ressaltar o aspecto de inovação das tecnologias do segmento, sejam startups (empresas nascentes) ou não.

No Chile, por exemplo, estimam-se 100 edtechs num mercado avaliado em 50 milhões de dólares, volume semelhante ao investimento do Ministério da Educação chileno em livros didáticos. Um "marketplace" governamental facilita a compra pública das tecnologias pelas escolas (OMIDYAR, 2019b). No Brasil, o mapeamento mais recente do CIEB (2020) indica que há no país cerca de 449 edtechs ativas, sendo que 70,6% delas oferecem tecnologias para o ensino básico (infantil, fundamental e médio). No mapeamento do ano anterior (CIEB, 2018), 47% das 364 então existentes declaravam atuar nesse segmento.

Para prosperar, esse mercado depende da **infraestrutura** de telecomunicações, eletricidade e internet. Por isso, costuma vir acompanhado de forte *lobby* para a expansão de programas público-privados desse tipo, para uso das tecnologias dentro e fora das escolas. Um exemplo de como o programa de universalização da infraestrutura permitiu o surgimento do mercado de edtechs é o programa de conectividade Enlaces, do Chile (OMIDYAR, 2019b).

[7] Não se pretende discutir, neste texto, as potencialidades e desafios do uso das tecnologias educacionais para os processos de ensino e aprendizagem. Certamente há boas propostas e intenções entre as aplicações em debate. O enfoque deste artigo são os processos de coleta e tratamento de dados pessoais que acompanham os usos das tecnologias, bem como a necessidade de se pensar formas transparentes e responsáveis para a comunidade educativa optar ou não pela adoção das ferramentas.

"Habilitar infraestrutura" é uma das categorias necessárias no modelo da Omidyar Network[8] (2019a, p.11) para "escalar o impacto" de edtechs, com quatro recomendações para o cenário ideal:

- indivíduos usam aparelhos pessoais e serviços móveis em casa e em suas comunidades;
- há acesso universal à internet para toda a população por meio de tecnologia sem fio, cabeada ou outros meios;
- há infraestruturas de rede específicas para as escolas para uma conectividade confiável a custos acessíveis e
- iniciativas de govtech conectam escolas a plataformas administrativas (por exemplo, de compras online ou de gestão escolar) cuja infraestrutura possa ser aproveitada pelas edtechs.

A armadilha aqui não está na ideia de **ampliar o acesso à conexão de internet**; este **também é um direito fundamental** que deve ser garantido. O risco é tornar a infraestrutura ainda mais opaca e sujeita às práticas de violação de privacidade. As medidas de privatização das infraestruturas de dados, não só no campo da educação, são um aspecto central na discussão. Sua governança pública ou privada define aspectos *informacionais* (Quem acessa o quê? O que deve ficar aberto ou sigiloso?) e *institucionais* (De quem é a propriedade dos dados? Podem ser explorados economicamente ou são um bem público?)[9].

Mais uma vez, é importante posicionar esse debate no campo mais amplo das discussões sobre a **governança da internet**. A infraestrutura, ou seja, a escolha de tecnologias por meio das quais esses dados devem trafegar, é decisiva para obter um ambiente mais ou menos democrático. Quanto mais abertas e transparentes as tecnologias, mais universal e não-discriminatório pode ser o acesso.

A falta de materiais adequados nas escolas e o quadro de subfinanciamento da educação enfrentado pelos países da região tornam as escolas mais suscetíveis à adoção pouco criteriosa de ferramentas tecnológicas "gratuitas" que coletam dados da comunidade escolar. Diante disso, fica muito difícil também a defesa do desenvolvimento de softwares próprios ou soluções customizadas, pois elas trazem possíveis custos que serão vistos como mais altos do que o de ferramentas "doadas".

Por fim, se essa já era uma tendência em curso, a pandemia de Covid-19 abriu oportunidades[10] para os que visam acelerar o processo. A seção seguinte traz alguns exemplos de como, a depender de como são implementadas, as tecnologias da educação podem colocar em risco a privacidade da comunidade educativa.

---

[8] A fundação Omidyar Network expandiu recentemente sua iniciativa de educação e criou, no início de 2020, um braço chamado "Imaginable Futures" para atuar exclusivamente no setor. Desde 2009, diz já ter investido 200 milhões de dólares em 100 organizações *for-profit* e *nonprofit* no campo, como a Khan Academy. Um de seus focos será a América Latina, ao lado da África. Sobre o tema, ver: "Omidyar Network Spins Off Education Portfolio Into Independent Investment Firm", do site Edsurge.com, disponível em: https://www.edsurge.com/news/2020-01-23-omidyar-network-spins-off-education-portfolio-into-independent-investment-firm. Último acesso em 29/10/2020.

[9] Sobre a privatização de infraestruturas digitais e a noção de privacidade que decorre da distinção público-privado, ver Hoeyer (2020).

[10] Ver, por exemplo, "Why COVID-19 is an EdTech opportunity for Latin America", artigo no site do Fórum Econômico Mundial publicado em 15 set. 2020. Disponível em: https://www.weforum.org/agenda/2020/09/what-covid-19-means-for-edtech-latin-america

III. Casos na educação

Ainda não há um mapeamento abrangente e sistemático publicado sobre as práticas de coleta de dados e de vigilância sobre o campo da educação, especialmente na América Latina e Caribe. A literatura já tem levantado preocupações sobre o espaço que a indústria edtech tem ganhado nas escolas, indo além da violação de privacidade e interferindo em processos de ensino e aprendizagem. O papel crescente de fornecedores e a falta de regulação sobre esse fluxo de dados "dentro e fora das salas de aula é visto como ameaça à autonomia, liberdade de pensamento, equidade e oportunidade" (CARMEL, 2016, p. 10).

A preocupação com a privacidade dos estudantes e a concentração de dados nas mãos de atores privados em infraestruturas opacas é um tema levantado com frequência cada vez maior (LINDH & NOLIN, 2016; PARRA et al., 2018; STULPIN, 2015; WILLIAMSON, 2015; HARTONG & FÖRSCHLER, 2019). Em geral, pesquisadores e grupos que fazem o controle social dessas iniciativas têm se dedicado a estudar os casos de implementação nas escolas e universidades dos pacotes e ferramentas de "Big Techs", ou gigantes da tecnologia — Google, Apple, Facebook, Amazon e Microsoft. O grupo também é conhecido pelo acrônimo GAFAM ou "Big Five", por representarem as cinco maiores empresas da indústria nos Estados Unidos e no mundo.

Mas, como visto anteriormente, as engrenagens do mercado de dados pessoais não são movimentadas apenas pelas gigantes. Empresas menores do ramo das edtechs também podem ter seu modelo de negócios calcado na coleta e no repasse de dados pessoais a terceiros, ou no direcionamento de anúncios e conteúdo personalizado aos usuários. Esse objetivo nem sempre é explicitamente declarado. Essas ferramentas podem ser adquiridas diretamente pelas escolas ou adotadas pelos departamentos de educação. Muitas vezes, a adoção é oferecida de forma gratuita para uso nas redes públicas, por meio de termos de parceria entre as redes e instituições como fundações ou institutos privados. Justamente por ainda não estarem no radar dos estudos sobre a vigilância na educação, é preciso atenção redobrada.

Como fenômeno mais recente, entram nesse mercado como investidoras as "venture philanthropy" (ADRIÃO & DOMICIANO, 2018). São atores privados que não ocultam seu interesse em lucrar diretamente com a atuação em áreas sociais e que, por essa razão, se diferenciam dos tradicionais 'braços sociais' dos grupos empresariais" (ADRIÃO, 2018, p.15). Acumulam capital investindo na produção e no desenvolvimento das edtechs, articulando-se a segmentos da economia financeirizada, como fundos de investimento e bancos.

Em resumo, esse breve panorama do campo das tecnologias educacionais permite distinguir os seguintes atores privados atuando e colaborando entre si:

- **Big Techs**, na condição de gigantes corporações de tecnologia, oferecem gratuitamente pacotes de aplicativos e infraestrutura às escolas e também vendem em larga escala equipamentos para redes de educação pelo mundo (ex.: Google, Microsoft, Apple).
- **Edtechs** desenvolvem produtos e serviços para o campo educacional, seja de software ou hardware, com variados modelos de negócio, coletando e processando dados ao longo de todo o processo.

- **Corporações do campo educacional** já atuam no setor público e privado com o desenvolvimento de sistemas de ensino, material didático etc. Passam interagir com o ramo edtech ao produzir tecnologias de ensino e aprendizagem, além de equipamentos, que podem ser introduzidos na educação pública a partir de processos que fazem parte do que se entende por privatização da educação. Os dados coletados em massa também podem ser usados para desenho e planejamento estratégico de suas próprias operações.
- **Fundações e institutos de natureza privada** fazem parcerias com governos para doação de produtos de edtechs, desenvolvem pesquisas e projetos-piloto para facilitar a contratualização de edtechs nas redes públicas e financiam o segmento;
- **investidores de *venture capital*ou *venture philantropy*** financiam startups para dar escala aos seus negócios — o que lhes permite, por exemplo, oferecer inicialmente o produto de forma gratuita para redes de ensino inteiras, até obter retornos financeiros de seus produtos.

Os casos abaixo ilustram como essas interações acontecem na prática e quais são os riscos que eles levantam para a privacidade e a proteção dos dados da comunidade educativa.

Pacotes "classroom"

Microsoft, Apple e Google criaram pacotes com o mesmo nome, "Classroom", oferecidos gratuitamente a escolas ao redor do mundo. Por meio deles, professores podem criar e aplicar avaliações e testes, estudantes podem fazer trabalhos colaborativos online, responsáveis pelos estudantes podem obter informações e todos podem se comunicar, inclusive por meio de videoconferências, além de outras funcionalidades. Além dos programas, que costumam sincronizar conteúdos na nuvem para serem acessados de outros dispositivos, como celular, as empresas também comercializam suas marcas de notebooks e tablets.

A Google afirma ter, hoje, 90 milhões de usuários pelo mundo em seu programa "For Education". Outros 30 milhões de pessoas usam o Chromebook[11], um laptop simplificado e mais barato que depende de conexão constante à internet. Com uma estratégia mais agressiva de oferta gratuita, é a marca que captou mais usuários entre as três gigantes[12]. A empresa oferece cursos e programas de certificação no uso de suas ferramentas para docentes, e também sugere currículos e planos de aula. Entre os conteúdos disponíveis, um curso de "cidadania digital" ambienta crianças à navegação segura pela internet — todo baseado nas ferramentas da própria empresa. Uma das preocupações relatadas por professores, em escolas que adotaram o pacote, é a de que essa ênfase habitue as crianças a confiar nessas ferramentas de uma só empresa "por padrão"[13].

---

[11] A empresa não detalha em quais países. Números gerais para Google Suite e Chromebook na página inicial: https://edu.google.com/partners/. Último acesso em 30/10/2020.

[12] Ver "Teachers across America are obsessed with Google products — here's how Apple and Microsoft plan to win them back", disponível em: https://www.businessinsider.com/google-apple-microsoft-competing-dominate-education-technology-market-2018-11. Último acesso em 30/10/2020.

[13] Ver "Teachers love Google's education products but are suspicious. Why is a megacorporation giving them a perfect tool for free?", disponível em:

A Electronic Frontier Foundation (EFF) realizou um *survey* e uma série de entrevistas sobre privacidade de estudantes envolvendo mais de mil estudantes, professores, familiares, bibliotecários e outros integrantes da comunidade educativa nos Estados Unidos (ALIM et al., 2017). Casos envolvendo os pacotes das "Big Five", em especial da Google, foram menções frequentes — embora a pesquisa tenha identificado o uso de 152 *apps* distintos, muitos deles de empresas pequenas e médias. A tabela abaixo resume os problemas mais comuns.

PROBLEMAS MAIS COMUNS RELACIONADOS À PRIVACIDADE

Falta informação para a comunidade educativa	Responsáveis recebem pouca ou nenhuma informação sobre novos equipamentos ou contas de e-mail ou plataformas que educandos recebem nas escolas.
Não há consentimento	Professores, funcionários e estudantes têm novas contas (por exemplo, de e-mail ou serviços na nuvem) criadas em seus nomes sem dar consentimento ou ao menos conhecer a respectiva política de privacidade.
Não há alternativa	Na maior parte das vezes, não há "opt-out", ou seja, a tecnologia é adotada oficialmente pela rede de ensino e passa a ser obrigatória para todos.
Práticas inseguras de gestão da informação	Quando acessos são gerados em massa para a comunidade educativa, muitas vezes são usados padrões inseguros de senha (por ex., data de aniversário ou matrícula).

Fonte: elaboração própria, a partir da compilação de casos da EFF (ALIM et al., 2017)

No Brasil, a iniciativa Educação Vigiada[14] identificou que 72% das universidades públicas e secretarias estaduais de educação do país já firmaram parcerias com Google ou Microsoft para controle de seus servidores de e-mails.

Aplicativos de gestão educacional

Usando acordos de cooperação ou termos de doação, redes públicas de ensino municipais e estaduais em pelo menos 15 entes federativos brasileiros adotaram, entre 2017 e 2019, o aplicativo "Mira Educação"[15]. Suas funcionalidades incluíam: 1) substituir o diário de classe por uma versão digital, com notas de alunos, observações sobre comportamento e frequência; 2) envio de mensagens SMS aos responsáveis e 3) correção automatizada de avaliações padronizadas.

Desenvolvido por uma edtech e autodefinido como "negócio de impacto social", o aplicativo coletou, segundo a própria empresa, dados pessoais de mais de 2,3 milhões

https://www.businessinsider.com/google-classroom-free-ed-tech-teacher-reaction-2018-11. Último acesso em 30/10/2020.

[14] Mapeamento completo disponível em: https://educacaovigiada.org.br. Último acesso em 30/10/2020.

[15] A missão e objetivos do Mira Educação foram registrados em seu website, não mais publicado na internet. O texto pode ser obtido no Internet Archive, que disponibiliza "screenshots" da página em diversos momentos desde sua criação. A última versão, de 15/03/2019, está em: https://web.archive.org/web/20190110014638/https://miraeducacao.com.br/quem-somos. Último acesso em 29/10/2020.

de estudantes e familiares, além de mais de 140 mil docentes. Sobre seu alcance e implementação, só se conhecem os números declarados pela própria empresa em seu site ou notas de imprensa das secretarias de educação parceiras.

A empresa desenvolvedora se apresentava como uma startup, mas tinha entre seus sócios um ex-vice-presidente da corporação Kroton Educacional, hoje chamada Cogna. Trata-se de um grupo brasileiro que se tornou a maior corporação privada de serviços de educação do mundo. Além dele, sócios-investidores teriam injetado 10 milhões de dólares a partir do exterior, tendo optado por permanecer ocultos[16].

O compartilhamento de dados nessas parcerias acontecia de várias formas, como a conexão direta com os sistemas de gestão, envio de planilhas e outros. Apenas no caso dos professores, que deveriam instalar o aplicativo em seus aparelhos pessoais, havia uma política de privacidade[17] — exigência da Apple Store e do Google Play, os maiores *marketplaces* de aplicativos. No documento, a empresa informava que os dados poderiam ser compartilhados com parceiros e que o usuário autorizava o uso desses dados por outras fontes de informação para a construção de um perfil.

Em 31 de março de 2019, a empresa repentinamente comunicou às secretarias o encerramento de suas atividades e, em 1º de abril, deixou de funcionar, sem nenhum tipo de suporte, manutenção ou oferecimento de alternativa às redes[18]. Além da falta de transparência sobre a gestão da informação — antes, durante e depois da parceria — o caso chama a atenção pela precariedade dos instrumentos de contratualização (termos de doação) e pela situação de "aprisionamento tecnológico" (*vendor lock-in*) que acontece quando os governos não se tornam detentores dos bancos de dados e dos códigos das soluções que contratam.

Aulas a distância

Com a pandemia de Covid-19 e a flexibilização das regras de compras públicas, redes de ensino pelo mundo se apressaram em adotar soluções tecnológicas que pudessem substituir as aulas presenciais. Os questionamentos às políticas de privacidade das grandes plataformas já são conhecidos e foram tratados anteriormente, mas recorrer a soluções desconhecidas e igualmente opacas pode trazer à tona uma nova classe de riscos.

No Brasil, quatro estados foram alvo de questionamento da imprensa[19] ao utilizar ferramentas de uma pequena empresa até então desconhecida para dar aulas a mais de sete milhões de alunos da rede pública. Para assistir às aulas, os estudantes devem fazer cadastro e, assim como professores, concordar com a política de

---

[16] Ver "Dos aprendizados, a evolução: a trajetória da Mira Educação", disponível em: www.aupa.com.br/cases_mira-educacao/. Último acesso em 30/10/2020.

[17] O documento estava disponível para download na Apple Store pelo link https://s3-sa-east-1.amazonaws.com/web-mira/politica-de-privacidade.pdf , mas foi removido após a descontinuidade do aplicativo anunciada em 01/04/19. O download do documento foi realizado pela autora em 05/02/2019.

[18] Ver "Empresa fecha e aplicativo da SED sobre frequência de alunos deixa de funcionar", disponível em: https://www.campograndenews.com.br/brasil/cidades/empresa-fecha-e-aplicativo-da-sed-sobre-frequencia-de-alunos-deixa-de-funcionar. Último acesso em 30/10/2020.

[19] Ver "Escola com partido: aulas online obrigam milhões de alunos a usar app de empresa obscura que criou TV Bolsonaro", disponível em: https://theintercept.com/2020/06/15/app-empresa-tv-bolsonaro-aulas-online-pandemia/. Último acesso em 30/10/2020.

privacidade. A regra diz que o usuário autoriza o acesso a dados como o álbum de fotos do celular, de conexão de rede WiFi e trocas de mensagens em grupos de bate-papo — que podem ficar guardados por até seis meses. O aplicativo ainda pode oferecer outros conteúdos e exibir publicidade aos usuários.

De acordo com a apuração do The Intercept Brasil, a empresa IP.TV tinha em seu currículo, até a pandemia, um único produto bem sucedido. Trata-se de "Mano", um aplicativo de streaming de vídeos criado em 2018 para que a campanha de Jair Bolsonaro a presidente pudesse transmitir todos os vídeos que quisesse aos seus seguidores, incluindo os apagados pelas redes sociais por conter notícias falsas. Dessa forma, faz-se, às vésperas de eleições, uma conexão direta de um banco de dados de mais de 7 milhões de usuários (os dispositivos de famílias em situação de vulnerabilidade raramente são usados apenas pela criança) a um fornecedor que tem, entre seus clientes, um grupo político conhecido por escândalos de disseminação de *fake news*.

Jogos "educativos" e publicidade

Na dura rotina que se estabeleceu para as famílias sob quarentena, é muito provável que a exposição de crianças e adolescentes ao uso de tablets e smartphones tenha aumentado. Os jogos online — e especialmente os autodenominados "educativos" — são objeto especial de atenção de pesquisadores do tema da proteção de dados. Na maior parte das vezes são oferecidos gratuitamente, em troca de exibição de publicidade e compartilhamento de dados.

Embora o mercado da publicidade voltada ao público infantil nos meios de comunicação tradicionais tenha sido regulado nas últimas décadas nos países da região, ainda há pouco controle do que ocorre em uma miríade de sites como o YouTube e aplicativos voltados às crianças. Uma análise das políticas de privacidade dos "apps" mais populares para o público infantil no Brasil (BRITO CRUZ; SOUZA ABREU; LUCIANO, 2018) revelou que a maioria afirma coletar "dados de uso", que revelam padrões comportamentais e interesses, além de compartilhá-los com terceiros.

A extensão do que se coleta sobre as crianças nessas plataformas pode espantar. Um raro estudo sobre o tema foi conduzido por uma empresa do setor de jogos. Segundo os resultados, uma criança que começou a utilizar a internet aos três anos terá tido até os 13 anos de idade 72 milhões de pontos de dados coletados sobre si apenas por empresas especializadas em anúncios (adtechs). Isso, afirma, é provavelmente subestimado, uma vez que exclui rastreadores de redes sociais[20].

DADOS PESSOAIS NA EDUCAÇÃO: UM RESUMO DOS RISCOS

Caso os dados pessoais não recebam tratamento adequado, há diversos riscos de mau uso e ameaças à privacidade da comunidade educativa. Este quadro resume, para referência rápida, os principais desses problemas que foram abordados neste documento. .

Riscos no setor público	Riscos no setor privado

[20] Ver "How much data do adtech companies collect on kids before they turn 13?", disponível em: https://www.superawesome.com/blog/how-much-data-do-adtech-companies-collect-on-kids-before-they-turn-13/ . Último acesso em 30/10/2020.

Vazamento de dados Viés em algoritmos de políticas públicas Vigilância e perseguição política (em contextos autoritários) Apropriação indevida para fins eleitorais	Vazamento de dados Venda de dados a terceiros Data profiling (construção de perfis) Anúncios direcionados Modulação de comportamentos Viés em algoritmos de serviços privados (emprego, crédito, consumo etc)
Quando o público e o privado se "encontram"	
Compartilhamento não-transparente de dados para finalidade diversa daquelas para as quais foram coletados Doação de aplicativos e sistemas privados para uso gratuito com coleta de dados dos usuários	

Fonte: Elaboração própria.

IV. Uma proposta de agenda para o campo

Neste breve panorama, buscou-se mostrar por que e como a educação é terreno fértil para o mercado de dados pessoais. Essa face da nova economia digital, que alguns estudiosos chamam de "capitalismo de vigilância", coleta, analisa, usa e explora economicamente dados da comunidade educativa.

Declarada "morta" pela indústria da tecnologia, a privacidade respira e está mais viva que nunca no campo dos direitos digitais. A proteção de dados pessoais vem ganhando novo fôlego com uma nova onda de aprovação de leis específicas na última década. Também no campo dos direitos humanos, as organizações que atuam com a defesa da educação pública não podem ficar indiferentes ao embate.

Como o objetivo deste documento é iniciar um debate, esta seção não apresenta conclusões, mas caminhos que podem ser explorados em futuras investigações. Também abre um primeiro conjunto de propostas de incidência nesta agenda. Nesta encruzilhada de direitos, a reflexão proposta é como trazer a proteção de dados pessoais e a ampliação da transparência para o centro da roda da defesa da educação na América Latina.

Pesquisa

- **Mapeamento.** Um levantamento mais abrangente e sistemático pode capturar outras formas de atuação das edtechs no campo da educação pública na América Latina e Caribe e seus modelos de negócio, identificando os riscos para a privacidade da comunidade educativa — não só entre as Big Techs — e nuances regionais específicas.
- **Implicações para o direito à educação.** As práticas de apropriação de dados pessoais da comunidade educativa por parte de atores privados — muitas vezes contratados com recursos públicos, trazem consequências para o próprio conceito de direito à educação e de suas garantias. Os "conteúdos" e ferramentas introduzidos, o conhecimento construído e o próprio sentido da educação podem ser afetados pela lógica dessa nova "economia dos dados".

- **“Comoditização” dos dados**. É promissor estabelecer um diálogo entre a literatura sobre a privatização da educação e o campo de estudos críticos de dados (ILIADIS & RUSSO, 2016). Os dados, que podem ser um bem comum ou um direito individual a ser protegido, a depender da situação, passam a ser novo foco de privatização e exploração econômica (além dos objetos já conhecidos e estudados no campo da privatização da educação).
- **Inteligência artificial**. O uso crescente de algoritmos de aprendizagem de máquina para criação, implementação e focalização de políticas públicas educacionais merece atenção especial. Os dados pessoais são insumos necessários para alimentar os modelos matemáticos dos algoritmos. Quando implementados de forma pouco transparente e em escala, geram distorções e aprofundam desigualdades (O’NEIL, 2016). No Reino Unido, a implementação desastrosa de um algoritmo enviesado de avaliação de estudantes levou a protestos no país inteiro mesmo em meio à pandemia[21].

Advocacy

- **Transparência de contratos e doações**. Recorrer a pedidos de acesso à informação para obter instrumentos firmados com edtechs e suas políticas de privacidade é uma forma de começar a compreender e mapear os riscos que eles envolvem. Mesmo que se constate a ausência dessa informação ou de respostas, a falta de transparência é um assunto importante a ser pautado no debate público.
- **Governança de dados**. A transparência do tratamento de dados também é um tema que merece acompanhamento: quem são os responsáveis pelo tratamento? Existem documentos com avaliação de riscos? Quais são as políticas de segurança que os departamentos de educação estão seguindo? São algumas das categorias de questões que podem ser demandadas ao poder público.
- **Tecnologias abertas**. A pauta do software livre e dos códigos abertos é essencial para a privacidade e a proteção de dados pessoais, pois amplia a participação cidadã sobre a infraestrutura digital dos governos. Os softwares devem ser desenvolvidos desde o início com o princípio “privacy by design”, ou “privacidade por padrão”. Experiências de código-aberto (*open source*) na educação podem ser ampliadas e replicadas na região — não apenas os aplicativos usados na ponta pela comunidade educativa, mas também os sistemas de gestão educacional.

Litigância estratégica

- **Denúncias formais**. A maior parte dos países da América Latina possui em sua constituição nacional a previsão do direito à proteção de dados pessoais. Vários deles já possuem leis específicas para sua regulamentação, em estágios distintos de implementação: Chile (1999), Argentina (2000), México (2010), Peru (2011), Colômbia (2012), Brasil (2018), Barbados (2019) e Panamá (2019). As organizações que já atuam com litígio estratégico em direitos humanos podem se apropriar desse

[21] Ver “A-level results: Government accused of 'baking in' inequality with 'boost' for private schools“, disponível em: https://news.sky.com/story/35-of-a-level-results-downgraded-by-one-grade-figures-reveal-12048251. Último acesso em 30/10/2020.

marco normativo nascente para articular o tema às pautas do direito à educação — por exemplo, a gratuidade.

- **Casos coletivos**. Assim como nas experiências de litígio em direito à educação, é possível pensar do ponto de vista estruturante das políticas públicas de proteção de dados pessoais, cobrando no poder judiciário a implementação de ações preventivas e de planejamento do poder público na matéria. Por exemplo, questionar a inexistência de avaliações de risco sobre dados pessoais.

Formação e articulação

- **Novos vocabulários**. É preciso construir capacidades nas organizações do campo educativo para analisar e compreender os termos de serviço e as políticas de privacidade que se apresentam embutidas nos aplicativos, sistemas e equipamentos que não param de surgir. Esse novo vocabulário também ajuda a fazer as questões certas para atuar em pesquisa e advocacy. Por isso, uma agenda de formação para os direitos digitais que contemple os desafios específicos do campo da educação se faz necessária.
- **Somar forças**. As organizações do campo dos direitos digitais têm, em diversos países, atuado intensamente em pesquisa, advocacy e litigância na temática de proteção de dados pessoais e acesso à informação, mas não necessariamente conhecem as ameaças práticas que recaem sobre as políticas educacionais. Essa aliança estratégica pode gerar oportunidades de ação para ambos os campos.

Referências bibliográficas

ADRIÃO, T. Dimensões e formas da privatização da educação no Brasil: Caracterização a partir de mapeamento de produções nacionais e internacionais. **Currículo sem Fronteiras**, v. 18, n. 1, p. 8–28, 2018.

ADRIÃO, T.; DOMICIANO, C. A. A Educação Pública e as Corporações: avanços e contradições em uma década de ampliação de investimento no Brasil. **FINEDUCA - Revista de Financiamento da Educação**, v. 8, 2018.

ALIM, F. *et al*. **Spying on students: School-issued devices and student privacy.** 2017.

SILVEIRA, S.A. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados**. São Paulo: Edições Sesc SP, 2017. 7300 Kbp.

BRITO CRUZ, F.; SOUZA ABREU, J. de.; LUCIANO, M. Não fale com estranhos: Recursos interativos e tratamento de dados pessoais em apps infantis. *In*: **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2017**. São Paulo: Comitê Gestor da Internet no Brasil, 2018. p. 49–64.

CARMEL, Y. H. Regulating "big data education" in Europe: Lessons learned from the US. **Internet Policy Review**, v. 5, n. 1, 2016.

CIEB. **Mapeamento Edtech: Investigação sobre as tecnologias educacionais no Brasil 2018**. Centro de Inovação para a Educação Brasileira, 2018.

___. **Mapeamento Edtech: Investigação sobre as tecnologias educacionais no Brasil 2019**. Centro de Inovação para a Educação Brasileira, 2020.

CHRISTL, W.; KOPP, K.; RIECHERT, P. U. **Corporate surveillance in everyday life**. Cracked Labs, 2017.

COMPARATO, F. K. **A Afirmação Histórica dos Direitos Humanos**. 7. ed.ed. São Paulo: Saraiva, 2010.

GANGADHARAN, S. P. The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. **New Media and Society**, 2017.

HARTONG, S.; FÖRSCHLER, A. Opening the black box of data-based school monitoring: Data infrastructures, flows and practices in state education agencies. **Big Data and Society**, 2019.

HOEYER, K. Data promiscuity: how the public–private distinction shaped digital data infrastructures and notions of privacy. **Humanities and Social Sciences Communications**, v. 7, n. 37, 2020.

ILIADIS, A.; RUSSO, F. Critical data studies: An introduction. **Big Data and Society**, 2016.

LINDH, M.; NOLIN, J. Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. **European Educational Research Journal**, v. 15, n. 6, p. 644–663, 2016.

OMIDYAR. **Scaling Access & Impact: Realizing the Power of EdTech. Executive Summary.** Omidyar Network. 2019a.

_____. **Scaling Access & Impact: Realizing the Power of EdTech. Chile Country Report**. Omidyar Network. 2019b.

O'NEIL, C. **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. New York: Crown Books, 2016.

PARRA, H. *et al*. Infraestruturas, economia e política informacional: o caso do Google Suite for Education. **Mediações - Revista de Ciências Sociais**, v. 23, n. 1, p. 63–99, 2018.

WACKS, R. **Privacy: A Very Short Introduction**. Oxford: Oxford University Press, 2010.

WILLIAMSON, B. Governing software: networks, databases and algorithmic power in the digital governance of public education. **Learning, Media and Technology**, v. 40, n. 1, p. 83–105, 2015.

ZUBOFF, S. Big other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, n. 1, p. 75–89, 2015.