POLICY PAPER

EDUCACIÓN, PRIVACIDAD Y TRANSPARENCIA: UNA ENCRUCIJADA DE DERECHOS

Resumen:

La privacidad, aliada al acceso a la información, debe ser llevada al centro de la agenda de defensa del derecho a la educación. Esto es porque, en un contexto de baja transparencia y de escasa regulación en los países de América Latina y el Caribe, el tratamiento inadecuado de los datos personales de la comunidad educativa puede profundizar aún más las desigualdades existentes, además de provocar nuevas violaciones de derechos fundamentales. Este *policy paper* se propone presentar a los integrantes de la Red de la Campaña Latinoamericana por el Derecho a la Educación (CLADE) un panorama sobre los principales conceptos y desafíos relacionados a la privacidad y a la protección de datos personales en el contexto educativo. Con el documento, se pretende iniciar un debate sobre el tema, enumerando los puntos de atención para el campo y delineando una propuesta de agenda y de caminos posibles para su incidencia.

Introducción

Existe hoy un complejo mercado de datos personales en funcionamiento en el mundo, del cual todos somos partícipes activos — estemos o no conscientes de nuestro papel. Si, hace dos décadas, *Compact Disc* (CDs) grabados con nuestros datos catastrales — números de identidad, direcciones y teléfonos — incluso se extendían por lugares recónditos de mercados informales de San Pablo, Bogotá o de la Ciudad de México, la situación actual es al mismo tiempo más grande, más grave y más invisible. Los datos se transformaron en las **"huellas" digitales de cada uno**, generados a cada instante y lugar en cada aparato, dispositivo fijo o móvil, en los sitios en los que navegamos, imágenes y sonidos que captan de nosotros, además de lo que entregamos de manera consentida o inadvertida. Se trata de un **flujo constante de datos**, almacenados y compartidos por medio de intrincadas infraestructuras digitales entre diferentes actores institucionales y corporativos, formal e informalmente, con funciones distintas en esta cadena de valor.

El campo de la educación, especialmente pública, es entendido por los actores de este mercado como amplio terreno para explorar y expandir. En primer lugar, porque el propio Estado reúne, tradicionalmente, gran cantidad de datos al respecto de ciudadanas y ciudadanos para operacionalizar las políticas y los servicios públicos. En segundo lugar, porque este movimiento de búsqueda por explotación económica (o "comoditización") de datos personales encuentra y potencializa otro: la privatización de la educación. Los datos recolectados o la atención dispensada por los usuarios a eventual publicidad comienzan a ser más valiosos que el propio

software — estos productos, antes comercializados, llegan a ser "donados" o suministrados "gratuitamente".

Como se argumentará a lo largo de este documento, estos mecanismos de usurpación y desvío de finalidad de datos personales de la comunidad educativa tienen potencial de profundizar desigualdades y tornar todavia más vulnerables a los grupos históricamente expuestos a procesos de exclusión y discriminación. Y un virus, no de computadora, puede haber acelerado enormemente este proceso: la situación de calamidad pública instalada a lo largo del 2020 con la pandemia de Covid-19 impuso la adopción más rápida y amplia conocida hasta ahora de tecnologías para la enseñanza a distancia y comunicación entre estudiantes y docentes. Muchas veces, sin la debida transparencia de la donación o contratación pública de las tecnologías en cuestión.

Toda esta situación colocó al campo de la defensa del derecho a la educación delante de una verdadera "encrucijada de derechos": transparencia versus privacidad. Al mismo tiempo en que es necesario reafirmar y contener retrocesos en el derecho a la privacidad, también es necesario abogar por el rescate de la noción de **datos públicos como un bien común**. La realización de esta idea depende de una gobernanza pública, en la que el Estado se coloque como garante de estos derechos.

Siempre que no se expongan individuos, los datos deben ser tratados con la máxima transparencia — incluyendo la del código fuente de las tecnologías adoptadas para las actividades educativas. El derecho de acceso a la información y el derecho a la privacidad no son derechos discordantes, sino complementarios. Juntos, contribuyen a la plena garantía del derecho a la educación.

Este documento es una invitación para iniciar un debate. Está estructurado en cuatro partes: (I) la primera sección define los principales **conceptos** de privacidad y transparencia desde el punto de vista de los derechos humanos y posiciona la noción de **datos personales en el contexto educacional**; (II) la segunda parte presenta el telón de fondo político y económico del proceso de recolección e intercambio de datos personales, sobre todo la noción de **capitalismo de vigilancia** y la **privatización de la educación**; la siguiente sección (III) detalla prácticas existentes y los riesgos de este proceso específicamente para el campo educativo. La cuarta parte (IV) propone una agenda inicial para el campo, con recomendaciones de temáticas de incidencia sobre privacidad y protección de datos en la educación. Se espera que, como punto de partida, el material contribuya para generar reflexión e identificar futuras acciones.

I. Conceptos y definiciones esenciales

Cada uno de nosotros tiene el derecho de **estar a solas** con sus propios pensamientos y emociones. Este principio se mantiene, pero los contornos de la noción de **privacidad** se han transformado desde el artículo de los juristas Samuel Warren y Louis Brandeis, escrito en 1890 y considerado un marco de esta definición (WACKS, 2010). Actualmente, gana peso la idea de que la privacidad comprende también el derecho del individuo a controlar **aquello que es recolectado sobre sí** —

la protección de datos. Nunca faltaron interesados en minimizar la importancia de la privacidad y decretar que esta "murió".

El sentido del debate sobre la privacidad vive de manera inequívoca en el campo de los derechos y libertades fundamentales. La afirmación de que "nadie será sujeto a interferencia en su vida privada, en su familia, en su hogar o en su correspondencia" está expresado en el Artículo 12 de la **Declaración Universal de los Derechos Humanos** (1948), así como el derecho a la protección contra este tipo de ataque. Texto similar está enunciado en el Artículo 17 del **Pacto Internacional sobre los Derechos Civiles y Políticos** (1966), adoptado por la Asamblea General de la Organización de las Naciones Unidas (ONU) para desarrollar la Declaración de manera pormenorizada. El término "correspondencia", que los textos buscan proteger, abarca toda forma de comunicación telefónica, telegráfica o telemática, como internet. Y no solo del poder público, sino también — y, cada vez más — de actores privados (COMPARATO, 2010).

Aún en el campo de los derechos humanos, la privacidad y la protección de datos personales son considerados fundamentales para la **gobernanza democrática de internet**. El Fórum de Gobernanza de Internet (IGF, su sigla en inglés), plataforma global vinculada al sistema ONU, reúne investigadores, representantes de gobiernos, de empresas y de la sociedad civil para la discusión de políticas públicas relativas al tema. En sus diversas declaraciones y documentos de trabajo, el IGF "actualiza" los derechos humanos para el contexto de la sociedad conectada en red. Entre los principios establecidos, está el derecho de toda persona a no ser sometida a vigilancia, de navegar por infraestructuras íntegras, la necesidad de que los estados regulen la protección de datos en normativas nacionales etc.[1].

Los ***datos personales***, foco de protección de los derechos ya mencionados, son definidos de manera amplia, en la legislación europea y en otros marcos normativos mundiales, como

> *información relativa a una **persona viva**, **identificada** o **identificable**. También constituyen datos personales el conjunto de informaciones distintas que pueden llevar a la identificación de una determinada persona*[2].

Aunque la información obtenida no contenga forma directa de identificación (por ejemplo, el nombre, o un número de identidad), o aunque haya sido tratada para eliminar este tipo de característica, el hecho de tener otros elementos que convierten al individuo *identificable* ya vuelven ese dato *personal*. Por otro lado, bases de datos que puedan ser efectivamente *anonimizadas*, o sea, que no permitan procesos de "ingeniería inversa" (llamados de "reidentificación") para señalar la identidad de personas específicas, podrán hacerse públicas en políticas responsables de transparencia en datos abiertos. El cuadro que sigue trae ejemplos de lo que podrían ser considerados datos personales en el contexto de políticas educativas.

---

[1] La "Carta de Derechos Humanos y Principios de Internet" puede ser consultada en: https://internetrightsandprinciples.org/charter/. Último acceso 09/11/2020.

[2] Referencias sobre las definiciones y la legislación correspondiente disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt#referncias. Último acceso 29/10/2020.

¿QUÉ DATOS SON RELACIONADOS A PERSONAS EN LAS INSTITUCIONES EDUCATIVAS?

La definición de datos personales depende del contexto en el cual están inseridos. De forma general, son datos relacionados a una persona y que, aislados o en conjunto, permiten identificarla. Este cuadro lista tipos de datos que pueden ser recolectados por las tecnologías implementadas, adoptadas o contratadas por instituciones educativas. Algunos pueden ser anonimizados y, con tratamiento adecuado, tornarse bases de datos abiertos o agregados para investigaciones, por ejemplo. Sin embargo, si son expuestos o desviados de la finalidad original, representan serios riesgos a los individuos.

Categorias	Tipos de datos recolectados y almacenados	Ejemplos de tecnologías que los captan
Biometría	Registros como imágenes del rostro, impresiones digitales y grabación de la voz.	Herramienta que certifica presencia de educandos por reconocimiento facial; molinetes de acceso a la unidad educacional con impresión digital.
Registro	Nombre del/de la educando/a y responsables, dirección, teléfono, matrícula etc.	Sistema de matrícula online; sistema de gestión de personas.
Identidad digital	Dirección de IP (protocolo de internet único da conexión); cookies (“testigos” de conexión); ID de publicidad del celular; dirección MAC de un dispositivo electrónico.	Registros hechos por plataformas de cursos EaD; Identificadores de notebooks y tablets distribuídos para cada estudiante o profesor.
Cotidiano escolar	Datos operacionales sobre las actividades educativas, tales como frecuencia escolar, asignación en grupos, transferencias y otros hechos.	Aplicación o sistema de diário de clase; aplicación para agenda o comunicación con responsables.
Evaluación	Datos sobre desempeño de estudiantes y docentes, tales como resultados de evaluación, notas, boletines escolares, flujo escolar etc.	Aplicación para corrección automatizada de evaluaciones; panel analítico de evaluación de desempeño.
Comporta miento	Historial de navegación por internet, aplicaciones instaladas, historial de desplazamiento (geolocalización).	Perfil de usuario en Google; sensores de smartphones.
Personalidad y actitudes	Datos recolectados o inferidos con aparatos digitales, tales como emociones, concentración, dispersión, relaciones.	Cámaras en sala de clase o ambiente escolar; navegación en el “feed” de las redes sociales (Facebook, Instagram).
Identidad personal y preferencias	Datos recolectados o inferidos con aparatos digitales, tales como convicción religiosa, origen étnico o racial, identidad de género, orientación sexual, opinión política, salud.	Registro de intereses manifestados en red social (Facebook) o búsquedas.

Fuente: Elaboración propia.

Entre todos estos datos personales que deben ser protegidos, dos dimensiones merecen especial atención: los llamados datos sensibles y los datos cuyos titulares son niñas, niños y adolescentes. Para estos datos, la legislación reserva condiciones de tratamiento específicas y capas de protección extra.

Datos personales sensibles[3] son aquellos que muestren:

- el origen racial o étnico o convicciones políticas, religiosas o filosóficas;
- filiación sindical;
- datos genéticos y biométricos;
- datos relacionados a la salud;
- datos relativos a la identidad de género, vida sexual u orientación sexual.

El tratamiento de **datos de niñas, niños y adolescentes** debe ser analizado bajo la óptica del marco normativo de protección de sus derechos, como la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de la ONU en 1989. El principio del **interés superior**, previsto en la Convención y reafirmado por las constituciones nacionales y Estatutos del Niño y Adolescente, deben guiar las decisiones sobre cómo tratar estos datos. Estos prevalecen sobre eventuales conflictos — en caso que el uso de datos de un niño contrarie su interés superior, debe ser cohibido, aunque haya consentimiento de los responsables. El límite de edad se ajusta al reglamento local.

Al contrario de lo que se pueda imaginar, el marco normativo de protección de datos no versa solamente sobre violaciones como situaciones de filtración, invasión de sistema o intercambio indebido de datos. El debate legal sobre privacidad se viene pautando con frecuencia en las nociones de **tratamiento de datos y consentimiento**.

El *tratamiento de datos* es un conjunto amplio de operaciones efectuadas sobre datos personales, por medios manuales o automatizados. Básicamente, es **todo lo que se pueda hacer con información**: recolección, registro, organización, estructuración, conservación, adaptación, alteración, recuperación, consulta, utilización, divulgación, cruces, limitación, borrados o destrucción de datos personales[4].

Las instituciones educativas son consideradas **responsables por el tratamiento,** siempre que determinen la finalidad y los medios de una de esas operaciones con datos personales de la comunidad educativa. Inclusive si optaran por la contratación de terceros. O sea, no debe solamente demandarse a los gobiernos y secretarías/departamentos públicos de educación como responsables por políticas de protección de datos personales. Cada unidad que operacionaliza la política pública de educación y que lidia con tecnologías, administrativas o pedagógicas (véase ejemplos en la tabla anterior), también lo es. La comunidad educativa debe saber exactamente lo que se hace con sus datos. De ahí la necesidad de que el tratamiento

[3] De acuerdo con la normativa europea, disponible en: 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 acceso 29/10/2020.

[4] Definición y referencias en la legislación europea disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_pt. Último acceso 29/10/2020.

sea, siempre, acompañado de políticas de transparencia y rendición de cuentas (*accountability*).

El papel del **consentimiento** también viene ganando prominencia en el debate. Acostumbra ser definido como la "manifestación de voluntad, libre, específica, informada e inequívoca, por la que la persona titular de los datos acepta, ya sea mediante declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"[5]. Es en las **políticas de privacidad** — los contratos en "letra chica" de aplicaciones y servicios online — que este consentimiento acostumbra ser recolectado.

Finalmente, se llama **violación de datos personales** a una brecha de seguridad que provoque, de modo *ilícito* o incluso *accidental*, destrucción, pérdida, alteración, divulgación o acceso no autorizados, a datos personales transmitidos, conservados o sujetos a cualquier otro tipo de tratamiento[6].

PARA RECORDAR: CONCEPTOS E IDEAS CLAVE

Datos personales	Datos que permitan identificar directa o indirectamente a un individuo de forma inequívoca
Datos sensibles	Revelan convicciones, aspectos de salud u origen étnico y racial, por ej.; reciben capas extra de protección.
Datos de niñas, niños y adolescentes	Deben ser tratados bajo la óptica del interés superior de los vulnerables; reciben mecanismos extra de protección, incluyendo consentimiento de responsables.
Tratamiento de datos	Básicamente toda operación que se pueda hacer con datos, desde la recolección al intercambio, pasando por el almacenaje.
Consentimiento	Manifestación de concordancia informada y explícita del usuario con relación al tratamiento específico de sus datos.
Responsables por el tratamiento	Instituciones o personas que definen la finalidad y la forma de tratar los datos personales en cuestión. Puede ser una unidad educacional, un director de escuela o una secretaría de gobierno.
Violación de datos personales	Situación ilícita o accidental en la que los datos personales reciben cualquier tratamiento no autorizado, por mala fé o ineptitud.

Fuente: elaboración propia.

II. Telón de fondo

[5] Definición presente en el Artículo 4º, Inciso XI, de la GDPR europea; el concepto es replicado en diversas normativas nacionales.
[6] Definición presente en el Artigo 4, Inciso XII, de la GDPR europea.

Los datos obtenidos y monetizados por medio de vigilancia tecnológica se volvieron tan centrales para el funcionamiento de esta "nueva economía" basada en internet que inspiraron un nuevo ropaje para el capitalismo: el **capitalismo de vigilancia** (ZUBOFF, 2015). Este sistema tiene como uno de sus principales insumos los flujos de atención individual, y los datos recolectados son materia prima para analizar y prever gustos, intereses y deseos (SILVEIRA, 2017).

En los últimos años, de forma bastante acelerada, este mercado se viene tornando más complejo, generando estudios sobre la "microeconomía de la interceptación de datos personales" (SILVEIRA, 2017, 832:834). Existen, por ejemplo, agentes especializados en hacer el "corretaje" o negociación de estos datos (*data brokers*), sustitutos más lucrativos y legalizados de los vendedores ambulantes que vendían CDs con datos filtrados. La tabla que sigue a continuación resume este mercado en cuatro camadas de funcionamiento.

EL FUNCIONAMIENTO DEL MERCADO DE DATOS EN CAMADAS

1. Recolección y almacenamiento	Plataformas de relaciones online, sites, mecanismos de investigación y de rastreamiento de navegación, formularios online, sensores esparcidos por las ciudades, antenas de celulares etc.
2. Procesamiento y mineración	Tratamiento y agregado de los datos recopilados y almacenados, reuniéndolos con otros disponibles públicamente o suministrados por diferentes fuentes. Pretende perfeccionar y enriquecer un perfil personal más detallado, por medio de algoritmos y tentativas de uso de softwares de inteligencia artificial.
3. Análisis y formación de muestras	Usadas por departamentos de marketing de empresas y por las plataformas que organizan la venta de los públicos segmentados y de las llamadas audiencias similares ("lookalikes")
4. Modulación	Oferta de productos y servicios a partir de las estrategias de venta trazadas después de los análisis. Incluye los dispositivos de filtro, formación de burbujas o *clusters* de consumidores. También está incluida la actividad de venta final de los productos considerados adecuados a públicos específicos.

Fuente: elaborado a partir de las definiciones y tipología propuesta por Sérgio Amadeu da Silveira (2017, 892:921)

La idea de que "la privacidad murió" es evocada por actores de la industria de tecnología para justificar la recolección indiscriminada de datos personales. Este discurso, cada vez más común, se tornó uno de los mayores inconvenientes para reivindicar el derecho a la protección de datos en el debate público. Para el público

en general, esta negociación puede sonar justa: ¿cuál es el problema en suministrar informaciones personales a cambio de servicios gratuitos como juegos y aplicaciones de comunicación que me son útiles? *Al final* — también se dice con frecuencia — "*no tengo nada para esconder*".

El problema es que las personas **no acostumbran saber la extensión de los datos que están siendo recolectados** sobre ellas. Más aún, **desconocen los usos** que se les puede dar, y las consecuencias inmediatas y futuras de esa concesión.

Estos datos son muchas veces usados para *data profiling* — procesos automatizados para construir perfiles individuales detallados destinados a "prever" e inducir comportamientos. Esto ocurre por medio de la recolección y análisis de "huellas digitales" durante la navegación por internet y el uso de aplicaciones.

El perfil digital se construye por medio del mercado presentado en el cuadro anterior que clasifica a las personas individualmente en decenas de miles de categorías, de acuerdo con atributos y puntuaciones ("scores") de educación, empleo, visiones políticas, intereses de salud, religión y origen étnico, usos de medios, consumo, ingreso, estabilidad económica y personalidad. También incluyen análisis de sus comportamientos online, inclusive tipos de sites y contenidos visitados, intereses, incluyendo tópicos sensibles. Una de las empresas con la mayor base de datos sobre consumidores del mundo, Acxiom ya decía tener, en el 2013, hasta 3 mil atributos sobre 700 millones de personas. Oracle, gigante de tecnología, dice suministrar más de 30 mil elementos sobre 2 billones de perfiles (CHRISTL; KOPP; RIECHERT, 2017).

A esta altura, ya es evidente que este mercado y sus técnicas de "perfilamiento" no sirven solamente para fines publicitarios. El mundo del trabajo y del empleo, el sector imobiliário, las compañías de seguro y de crédito, hasta incluso las dinámicas de la democracia y del debate electoral, del sistema de justicia y del estado de bienestar social — todos estos campos comienzan a ser afectados por el uso de tecnologías, de los algoritmos y de las decisiones automatizadas que se alimentan de estos datos. Y es por eso que, cuando son direccionadas a grupos tradicionalmente marginalizados, estas tecnologías pueden acentuar la desigualdad, creando un verdadero "*feedback loop* de injusticia" (GANGADHARAN, 2017). Ejemplos de estos efectos serán tratados en la siguiente sección.

En la educación, este proceso se encuentra y se potencializa con otro en curso en las últimas décadas: las diferentes formas de **privatización de las políticas educativas**, así como la imbricada relación entre el sector público y el privado en las redes de enseñanza latinoamericanas. En un mapeo de la literatura que abarcó el período de 1990 a 2014, que trataba las formas recientes de la privatización de la educación básica en Brasil y otros países, Adrião (2018) señaló la "compra o adopción de tecnologías educativas y demás insumos escolares desarrollados por el sector privado" como un tipo específico de privatización de los procesos pedagógicos/currículo.

Por "tecnologías educativas"[7] se entiende la oferta de "libros, contenidos digitales, accesos a plataformas y sistemas de información para redes públicas y escuelas privadas" (p.15). En la línea de este proceso, surge una nueva cara de estos mercados: las *edtechs*. La sigla, del inglés *Education and Technology*, denomina de forma amplia a las empresas de productos para el sector educacional — tanto de hardware (equipamientos), como de software (aplicaciones, programas y sistemas). La moda de juntar el sufijo "tech" al prefijo de la "industria" (*agro*, *gov*, *ad*, *fin*, *legal*, *health*) en general pretende resaltar el aspecto de innovación de las tecnologías del segmento, sean startups (empresas nacientes) o no.

En Chile, por ejemplo, se estiman 100 edtechs en un mercado valuado en 50 millones de dólares, volumen semejante a la inversión del Ministerio de Educación chileno en libros didácticos. Un "marketplace" gubernamental facilita la compra pública de las tecnologías por las escuelas (OMIDYAR, 2019b). En Brasil, el mapeo más reciente del CIEB (2020) indica que hay en el país cerca de 449 edtechs activas, siendo que el 70,6% de ellas ofrecen tecnologías para la enseñanza básica (*infantil*, *fundamental*, *médio*). En el mapeo del año anterior (CIEB, 2018), 47% de las 364 entonces existentes declaraban operar en este segmento.

Para prosperar, este mercado depende de la **infraestructura** de telecomunicaciones, electricidad e internet. Por eso, acostumbra a venir acompañado de fuerte *lobby* para la expansión de programas público-privados de este tipo, para uso de las tecnologías dentro y fuera de las escuelas. Un ejemplo de cómo el programa de universalización de la infraestructura permitió el surgimiento del mercado de edtechs es el programa de conectividad Enlaces, de Chile (OMIDYAR, 2019b).

"Habilitar infraestructura" es una de las categorías necesarias en el modelo de Omidyar Network[8] (2019a, p.11) para "escalar el impacto" de edtechs, con cuatro recomendaciones para el escenario ideal:

- individuos usan aparatos personales y servicios móviles en casa y en sus comunidades;
- hay acceso universal a internet para toda la población por medio de tecnología sin cable, cableada u otros medios;
- hay infraestructuras de redes específicas para las escuelas para una conectividad confiable con costos accesibles e

[7] No se pretende discutir, en este texto, las potencialidades y desafíos del uso de las tecnologías educativas para los procesos de enseñanza y aprendizaje. Ciertamente hay buenas propuestas e intenciones entre las aplicaciones en debate. El enfoque de este artículo son los procesos de recolección y tratamiento de datos personales que acompañan los usos de las tecnologías, así como la necesidad de pensar formas transparentes y responsables para que la comunidad educativa opte o no por la adopción de las herramientas.

[8] La fundación Omidyar Network expandió recientemente su iniciativa de educación y creó, a comienzos de 2020, un brazo llamado "Imaginable Futures" para actuar exclusivamente en el sector. Desde 2009, dice ya haber invertido 200 millones de dólares en 100 organizaciones *for-profit* y *nonprofit* en el campo, como Khan Academy. Uno de sus focos será América Latina, al lado de África. Sobre el tema, ver: "Omidyar Network Spins Off Education Portfolio Into Independent Investment Firm", del site Edsurge.com, disponible en: https://www.edsurge.com/news/2020-01-23-omidyar-network-spins-off-education-portfolio-into-independent-investment-firm. Último acceso 29/10/2020.

- iniciativas de govtech conectan escuelas a plataformas administrativas (por ejemplo, de compras online o de gestión escolar) cuya infraestructura pueda ser aprovechada por las edtechs.

La trampa aquí no está en la idea de **ampliar el acceso a la conexión de internet**; este **también es un derecho fundamental** que debe ser garantizado. El riesgo es transformar la infraestructura aún menos transparente y sujeta a las prácticas de violación de privacidad. Las medidas de privatización de las infraestructuras de datos, no solo en el campo de la educación, son un aspecto central en la discusión. Su gobernanza pública o privada define aspectos *informacionales* (¿Quién accede a qué? ¿Qué debe estar abierto o sigiloso?) e *institucionales* (¿De quién es la propiedad de los datos? ¿Pueden ser explotados económicamente o son un bien público?)[9].

Una vez más, es importante colocar este debate en el campo más amplio de las discusiones sobre la **gobernanza de internet**. La infraestructura, o sea, la elección de tecnologías por medio de las cuales estos datos deben transitar, es decisiva para obtener un ambiente más o menos democrático. Cuanto más abiertas y transparentes sean las tecnologías, más universal y no discriminatorio puede ser el acceso.

La falta de materiales adecuados en las escuelas y el cuadro de financiación insuficiente de la educación enfrentado por los países de la región tornan a las escuelas más susceptibles a la adopción poco criteriosa de herramientas tecnológicas "gratuitas" que recolectan datos de la comunidad escolar. Ante esto, se hace difícil también la defensa del desarrollo de softwares propios o soluciones personalizadas, ya que estas traen posibles costos que serán vistos como más altos que el de herramientas "donadas".

Por último, si esta ya era una tendencia en curso, la pandemia de Covid-19 abrió oportunidades[10] para los que pretenden acelerar el proceso. La siguiente sección trae algunos ejemplos de cómo, dependiendo del modo en el que son implementadas, las tecnologías de la educación pueden poner en riesgo la privacidad de la comunidad educativa.

III. Casos en la educación

Todavía no hay un mapeo general y sistemático publicado sobre las prácticas de colecta de datos y de vigilancia sobre el campo de la educación, especialmente en América Latina y el Caribe. La literatura ya ha planteado preocupaciones sobre el espacio que la indústria edtech ha ganado en las escuelas, yendo más allá de la violación de la privacidad e interfiriendo en procesos de enseñanza y aprendizaje. El papel creciente de proveedores y la falta de regulación sobre este flujo de datos "dentro y fuera de las salas de clase es visto como amenaza a la autonomía, libertad de pensamiento, equidad y oportunidad" (CARMEL, 2016, p. 10).

[9] Sobre la privatización de infraestructuras digitales y la noción de privacidad que deduce de la distinción público-privado, ver Hoeyer (2020).

[10] Ver, por ejemplo, "Why COVID-19 is an EdTech opportunity for Latin America", articulo en el site del Fórum Económico Mundial publicado el 15 set. 2020. Disponible en: https://www.weforum.org/agenda/2020/09/what-covid-19-means-for-edtech-latin-america

La preocupación con la privacidad de los estudiantes y la concentración de datos en manos de actores privados en infraestructuras poco claras es un tema planteado con una frecuencia cada vez mayor (LINDH & NOLIN, 2016; PARRA et al., 2018; STULPIN, 2015; WILLIAMSON, 2015; HARTONG & FÖRSCHLER, 2019). En general, investigadores y grupos que realizan el control social de estas iniciativas se han dedicado a estudiar los casos de implementación en las escuelas y universidades de los paquetes y herramientas de "Big Techs", o gigantes de tecnología — Google, Apple, Facebook, Amazon y Microsoft. El grupo también es conocido por el acrónimo GAFAM o "Big Five", por representar a las cinco mayores empresas de la indústria de Estados Unidos y en el mundo.

Pero, como fue visto anteriormente, los engranajes del mercado de datos personales no son movidos solamente por los gigantes. Empresas más pequeñas del ramo de las edtechs también pueden tener su modelo de negócios calcado en la recolección y en la transferencia de datos personales a terceros, o en el direccionamiento de anuncios y contenido personalizado a los usuarios. Este objetivo no siempre es explícitamente declarado. Estas herramientas pueden ser adquiridas directamente por las escuelas o adoptadas por los departamentos de educación. Muchas veces, la adopción es ofrecida de forma gratuita para uso en las redes públicas, por medio de términos de cooperación entre las redes e instituciones como fundaciones o institutos privados. Justamente por no estar todavía en el radar de los estudios sobre la vigilancia en la educación, es necesario redoblar la atención.

Como fenómeno más reciente, entran en este mercado como inversoras las "venture philanthropy" (ADRIÃO & DOMICIANO, 2018). Son actores privados que no ocultan su interés en lucrar directamente con la actuación en áreas sociales y que, por esa razón, se diferencian de los tradicionales 'brazos sociales' de los grupos empresariales" (ADRIÃO, 2018, p.15). Acumulan capital invertido en la producción y en el desarrollo de las edtechs, articulandose a segmentos de la economía financiarizada, como fondos de inversión y bancos.

En resumen, este breve panorama del campo de las tecnologías educativas permite distinguir los siguientes actores privados actuando y colaborando entre sí:

- **Big Techs**, en su condición de gigantes corporaciones de tecnología, ofrecen gratuitamente paquetes de aplicaciones e infraestructura a las escuelas y también venden a gran escala equipamientos para redes de educación por el mundo (ex.: Google, Microsoft, Apple).
- **Edtechs** desarrollan productos y servicios para el campo educacional, sea de software o hardware, con variados modelos de negócio, recolectando y procesando datos a lo largo de todo el proceso.
- **Corporaciones del campo educacional** ya operan en el sector público y privado con el desarrollo de sistemas de enseñanza, material didáctico etc. Pasan a interactuar con el ramo edtech al producir tecnologías de enseñanza y aprendizaje, además de equipamientos, que pueden ser introducidos en la educación pública a partir de procesos que son parte de lo que se entiende por privatización de la educación. Los datos recolectados de forma masiva también pueden ser usados para diseño y planificación estratégica de sus propias operaciones.
- **Fundaciones e institutos de naturaleza privada** se asocian con gobiernos para donación de productos de edtechs, desarrollan investigaciones y

proyectos piloto para facilitar la contractualización de edtechs en las redes públicas y financian el segmento;
- **inversores de *venture capitalou venture philantropy*** financian startups para dar escala a sus negocios — lo que les permite, por ejemplo, ofrecer inicialmente el producto de forma gratuita a redes enteras de enseñanza, hasta obtener retornos financieros de sus productos.

Los casos que siguen ilustran cómo estas interacciones ocurren en la práctica y cuáles son los riesgos que plantean para la privacidad y la protección de los datos de la comunidad educativa.

Paquetes "classroom"

Microsoft, Apple y Google crearon paquetes con el mismo nombre, "Classroom", ofrecidos gratuitamente a escuelas de todo el mundo. Por medio de ellos, profesores pueden crear y aplicar evaluaciones y tests, los estudiantes pueden hacer trabajos colaborativos online, responsables por los estudiantes pueden obtener información y todos pueden comunicarse, inclusive por medio de videoconferencias, además de otras funcionalidades. Además de los programas, que acostumbran sincronizar contenidos en la nube para poder ser accedidos desde otros dispositivos, como celular, las empresas también comercializan sus marcas de notebooks y tablets.

Google afirma tener, hoy, 90 millones de usuarios por el mundo en su programa "For Education". Otros 30 millones de personas usan el Chromebook[11], una laptop simplificada y más barata que depende de conexión constante a internet. Con una estrategia más agresiva de oferta gratuita, es la marca que captó más usuários entre las tres gigantes[12]. La empresa ofrece cursos y programas de certificación en el uso de sus herramientas para docentes, y también sugiere currículos y planes de clase. Entre los contenidos disponibles, un curso de "ciudadanía digital" adapta a niñas y niños a la navegación segura por internet — todo basado en las herramientas de la propia empresa. Una de las preocupaciones relatadas por profesores, y escuelas que adoptaron el paquete, es que este énfasis habitúe a los niños a confiar en estas herramientas de una sola empresa "por padrón"[13].

Electronic Frontier Foundation (EFF) realizó un *survey* y una serie de entrevistas sobre privacidad de estudiantes involucrando a más de mil estudiantes, profesores, familiares, bibliotecarios y otros integrantes de la comunidad educativa en los Estados Unidos (ALIM et al., 2017). Casos involucrando los paquetes de "Big Five", en especial de Google, fueron menciones frecuentes — aunque la investigación haya identificado el uso de 152 *apps* distintas, muchas de ellas de empresas pequeñas y medias. La siguiente tabla resume los problemas más comunes.

---

[11] La empresa no detalla en cuales países. Números generales para Google Suite y Chromebook en la página inicial: https://edu.google.com/partners/. Último acceso 30/10/2020.

[12] Ver "Teachers across America are obsessed with Google products — here's how Apple and Microsoft plan to win them back", disponíble en: https://www.businessinsider.com/google-apple-microsoft-competing-dominate-education-technology-market-2018-11. Último acceso 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?", disponible en: https://www.businessinsider.com/google-classroom-free-ed-tech-teacher-reaction-2018-11. Último acceso 30/10/2020.

PROBLEMAS MÁS COMUNES RELACIONADOS A LA PRIVACIDAD

Falta información para la comunidad educativa	Responsables reciben poca o ninguna información sobre nuevos equipamientos o cuentas de email o plataformas que educandos reciben en las escuelas.
No hay consentimiento	Profesores, funcionarios y estudiantes tienen nuevas cuentas (por ejemplo, de email o servicios en la nube) creadas en sus nombres sin haber dado consentimiento o al menos conocer la respectiva política de privacidad.
No hay alternativa	La mayor parte de las veces, no hay "opt-out", o sea, la tecnología es adoptada oficialmente por la red de enseñanza y pasa a ser obligatoria para todos.
Prácticas inseguras de gestión de la información	Cuando los accesos son generados en masa para la comunidad educativa, muchas veces son usados padrones inseguros de claves (por ej., fecha de cumpleaños o matrícula).

Fuente: elaboración propia, a partir de la compilación de casos de EFF (ALIM et al., 2017)

En Brasil, la iniciativa "Educação Vigiada"[14] identificó que el 72% de las universidades públicas y secretarías estaduales de educación del país ya firmaron alianzas con Google o Microsoft para control de sus servidores de emails.

Aplicaciones de gestión educacional

Usando acuerdos de cooperación o términos de donación, redes públicas de enseñanza municipales y estaduales en por lo menos 15 entes federativos brasileños adoptaron, entre 2017 y 2019, la aplicación "Mira Educação"[15]. Sus funcionalidades incluían: 1) sustituir el diario de clase por una versión digital, con notas de alumnos, observaciones sobre comportamiento y frecuencia; 2) envío de mensajes SMS a los responsables y 3) corrección automatizada de evaluaciones padronizadas.

Desarrollado por una edtech y autodefinido como "negocio de impacto social", la aplicación recolectó, según la propia empresa, datos personales de más de 2,3 millones de estudiantes y familiares, además de más de 140 mil docentes. Sobre su alcance e implementación, solo se conocen los números declarados por la propia empresa en su site o notas de prensa de las secretarías de educación colaboradoras.

La empresa desarrolladora se presentaba como una startup, pero tenía entre sus socios un ex vice presidente de la corporación Kroton Educacional, hoy llamada Cogna. Se trata de un grupo brasileño que se convirtió en la mayor corporación privada de servicios de educación del mundo. Además de él, socios inversores habrían

[14] Mapeo completo disponible en: https://educacaovigiada.org.br. Último acceso 30/10/2020.

[15] La misión y objetivos del Mira Educação fueron registrados en su website, ya no publicado en internet. El texto se puede obtener en Internet Archive, que ofrece "screenshots" de la página en diversos momentos desde su creación. La última versión, de 15/03/2019, está en: https://web.archive.org/web/20190110014638/https://miraeducacao.com.br/quem-somos. Último acceso 29/10/2020.

inyectado 10 millones de dólares desde el exterior, habiendo optado por permanecer ocultos[16].

El intercambio de datos en estas alianzas ocurría de varias formas, como la conexión directa con los sistemas de gestión, envío de planillas u otros. Solo en el caso de los profesores, que deberían instalar la aplicación en sus aparatos personales, había una política de privacidad[17] — exigencia de Apple Store y de Google Play, los mayores *marketplaces* de aplicaciones. En el documento, la empresa informaba que los datos podían ser compartidos con asociados y que el usuario autorizaba el uso de estos datos por otras fuentes de información para la construcción de un perfil.

El 31 de marzo de 2019, la empresa repentinamente comunicó a las secretarías el cierre de sus actividades y, el 1º de abril, dejó de funcionar, sin ningún tipo de soporte, manutención u ofrecimiento de alternativa a las redes[18]. Además de la falta de transparencia sobre la gestión de la información — antes, durante y después de la sociedad — el caso llama la atención por la precariedad de los instrumentos de contractualización (términos de donación) y por la situación de "aprisionamiento tecnológico" (*vendor lock-in*) que ocurre cuando los gobiernos no se convierten en titulares de los bancos de datos y de los códigos de las soluciones que contratan.

Clases a distancia

Con la pandemia de Covid-19 y la flexibilización de las reglas de compras públicas, redes de enseñanza por el mundo se apresuraron en adoptar soluciones tecnológicas que pudiesen sustituir las clases presenciales. Los cuestionamientos a las políticas de privacidad de las grandes plataformas ya son conocidos y fueron tratados anteriormente, pero recurrir a soluciones desconocidas e igualmente poco transparentes puede hacer surgir una nueva clase de riesgos.

En Brasil, cuatro estados fueron objeto de cuestionamiento de la prensa[19] al utilizar herramientas de una pequeña empresa hasta entonces desconocida para dar clases a más de siete millones de alumnos de la red pública. Para ir a las clases, los estudiantes deben hacer un registro y, así como los profesores, estar de acuerdo con la política de privacidad. La regla dice que el usuario autoriza el acceso a datos como el álbum de fotos del celular, de conexión de red WiFi e intercambio de mensajes en grupos de chat — que pueden estar guardados hasta por seis meses. La aplicación incluso puede ofrecer otros contenidos y exhibir publicidad a los usuarios.

---

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

[17] El documento estaba disponible para download en Apple Store en el link https://s3-sa-east-1.amazonaws.com/web-mira/politica-de-privacidade.pdf , pero fue removido luego de la discontinuidad de la aplicación anunciada el 01/04/19. El download del documento fue realizado por la autora el 05/02/2019.

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

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

De acuerdo con un relevamiento de The Intercept Brasil, la empresa IP.TV tenía en su currículo, hasta la pandemia, un único producto bien logrado. Se trata de "Mano", una aplicación de streaming de videos creada en 2018 para que la campaña a presidente de Jair Bolsonaro pudiese transmitir a sus seguidores todos los videos que quisiese, incluyendo los eliminados por las redes sociales por contener noticias falsas. De esta forma, se hace, en vísperas de elecciones, una conexión directa de un banco de datos de más de 7 millones de usuarios (los dispositivos de familias en situación de vulnerabilidad raramente son usados solamente por el niño) a un proveedor que tiene, entre sus clientes, a un grupo político conocido por escándalos de difusión de *fake news*.

Juegos "educativos" y publicidad

En la dura rutina que se estableció para las familias bajo cuarentena, es muy probable que la exposición de niñas, niños y adolescentes al uso de tablets y smartphones haya aumentado. Los juegos online — y especialmente los autodenominados "educativos" — son objeto especial de atención de investigadores del tema de la protección de datos. La mayor parte de las veces son ofrecidos gratuitamente, a cambio de exhibición de publicidad e intercambio de datos.

Aunque el mercado de la publicidad dirigida al público infantil en los medios de comunicación tradicionales haya sido regulado en las últimas décadas en los países de la región, todavía hay poco control de lo que ocurre en una infinidad de sitios como YouTube y aplicaciones dirigidas a niñas y niños. Un análisis de las políticas de privacidad de las "apps" más populares para el público infantil en Brasil (BRITO CRUZ; SOUZA ABREU; LUCIANO, 2018) manifestó que la mayoría afirma recolectar "datos de uso", que revelan patrones comportamentales e intereses, además de compartirlos con terceros.

La magnitud de lo que se recoge sobre niñas y niños en estas plataformas puede sorprender. Un extraño estudio sobre el tema fue conducido por una empresa del sector de jugos. Según los resultados, un niño que comenzó a utilizar internet a los tres años habrá tenido hasta los 13 años de edad 72 millones de puntos de datos recolectados sobre sí solamente por empresas especializadas en anuncios (adtechs). Esto, afirma, es probablemente subestimado, ya que que excluye rastreadores de redes sociais[20].

DATOS PERSONALES EN LA EDUCACIÓN: UN RESUMEN DE LOS RIESGOS

En caso que los datos personales no reciban tratamiento adecuado, hay diversos riesgos de mal uso y amenazas a la privacidad de la comunidad educativa. Este cuadro resume, para rápida referencia, los principales problemas que fueron abordados en este documento.

Riesgos en el sector público	Riesgos en el sector privado
Filtración de datos	Filtración de dados Venta de datos a terceros

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

Margen de error en algoritmos de políticas públicas Vigilancia y persecución política (en contextos autoritarios) Apropiación indebida para fines electorales	Data profiling (construcción de perfiles) Anúncios direccionados Modulación de comportamientos Margen de error en algoritmos de servicios privados (empleo, crédito, consumo etc)
Cuando el público y el privado se "encuentran"	
Intercambio no transparente de datos para fines diversos de aquellos para los cuales fueron recolectados Donación de aplicaciones y sistemas privados para uso gratuito con recolección de datos de los usuarios	

Fuente: Elaboración propia.

IV. Una propuesta de agenda para el campo

En este breve panorama, se buscó mostrar por qué y cómo la educación es terreno fértil para el mercado de datos personales. Esta cara de la nueva economía digital, que algunos estudiosos llama "capitalismo de vigilancia", recolecta, analiza, usa y explota económicamente datos de la comunidad educativa.

Declarada "muerta" por la industria de la tecnología, la privacidad respira y está más viva que nunca en el campo de los derechos digitales. La protección de datos personales viene ganando nuevo impulso con una nueva onda de aprobación de leyes específicas en la última década. También en el campo de los derechos humanos, las organizaciones que actúan con la defensa de la educación pública no pueden ser indiferentes al embate.

Como el objetivo de este documento es iniciar un debate, esta sección no presenta conclusiones, sino caminos que pueden ser explorados en futuras investigaciones. También abre un primer conjunto de propuestas de incidencia en la agenda. En esta encrucijada de derechos, la reflexión propuesta es cómo traer la protección de datos personales y la ampliación de la transparencia hacia el centro de la rueda de la defensa de la educación en América Latina.

Investigación

- **Mapeo.** Una investigación más exhaustiva y sistemática puede capturar otras formas de actuación de las edtechs en el campo de la educación pública en América Latina y el Caribe y sus modelos de negocio, identificando los riesgos para la privacidad de la comunidad educativa — no solo entre las Big Techs — y matices regionales específicos.
- **Implicaciones para el derecho a la educación.** Las prácticas de apropiación de datos personales de la comunidad educativa por parte de actores privados — muchas veces contratados con recursos públicos, traen consecuencias para el propio concepto de derecho a la educación y de sus garantías. Los "contenidos" y herramientas introducidos, el conocimiento

construido y el propio sentido de la educación pueden verse afectados por la lógica de esta nueva "economía de los datos".

- **"Comoditización" de los datos**. Es prometedor establecer un diálogo entre la literatura sobre la privatización de la educación y el campo de estudios críticos de datos (ILIADIS & RUSSO, 2016). Los datos, que pueden ser un bien común o un derecho individual a ser protegido, dependiendo de la situación, pasan a ser nuevo foco de privatización y explotación económica (además de los objetos ya conocidos y estudiados en el campo de la privatización de la educación).
- **Inteligencia artificial**. El uso creciente de algoritmos de aprendizaje de máquina para creación, implementación y focalización de políticas públicas educativas merece especial atención. Los datos personales son insumos necesarios para alimentar los modelos matemáticos de los algoritmos. Cuando son implementados de forma poco transparente y en escala, generan distorsiones y profundizan desigualdades (O'NEIL, 2016). En Reino Unido, la implementación desastrosa de un algoritmo de evaluación sesgado de estudiantes provocó protestas en todo el país incluso en medio de la pandemia[21].

Advocacy

- **Transparencia de contratos y donaciones**. Recurrir a pedidos de acceso a la información para obtener instrumentos firmados con edtechs y sus políticas de privacidad es una forma de empezar a entender y mapear los riesgos que implican. Aunque se constate la falta de esta información o de respuestas, la falta de transparencia es un tema importante que debe ser pauta en el debate público.
- **Gobernanza de datos**. La transparencia del tratamiento de datos también es un tema que merece seguimiento: ¿quiénes son los responsables del tratamiento? ¿Existen documentos con evaluación de riesgos? ¿Cuáles son las políticas de seguridad que los departamentos de educación están siguiendo? Son algunas de las categorías de asuntos que pueden ser demandados al poder público.
- **Tecnologías abiertas**. La pauta del software libre y de los códigos abiertos es esencial para la privacidad y la protección de datos personales, ya que amplía la participación ciudadana sobre la infraestructura digital de los gobiernos. Los softwares deben ser desarrollados desde el inicio con el principio "privacy by design", o "privacidad por padrón". Experiencias de código abierto (*open source*) en la educación pueden ser ampliadas y replicadas en la región — no solo las aplicaciones usadas en la punta por la comunidad educativa, sino también los sistemas de gestión educativa.

Litígio estratégico

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

- **Denuncias formales**. La mayor parte de los países de América Latina tiene en su constitución nacional la previsión del derecho a la protección de datos personales. Varios de ellos ya poseen leyes específicas para su reglamentación, en etapas distintas de implementación: Chile (1999), Argentina (2000), México (2010), Perú (2011), Colombia (2012), Brasil (2018), Barbados (2019) y Panamá (2019). Las organizaciones que ya actúan con litigio estratégico en derechos humanos pueden apropiarse de este marco normativo naciente para articular el tema a las pautas del derecho a la educación — por ejemplo, la gratuidad.
- **Casos colectivos**. Así como en las experiencias de litigio en derecho a la educación, es posible pensar desde el punto de vista estructurante de las políticas públicas de protección de datos personales, demandando en el poder judicial la implementación de acciones preventivas y de planificación del poder público en la materia. Por ejemplo, cuestionar la inexistencia de evaluaciones de riesgo sobre datos personales.

Formación y articulación

- **Nuevos vocabularios**. Es necesario construir capacidades en las organizaciones del campo educativo para analizar y comprender los términos de servicio y las políticas de privacidad que se presentan ya incorporadas en las aplicaciones, sistemas y equipamientos que no dejan de surgir. Este nuevo vocabulario también ayuda a hacer las preguntas correctas para actuar en investigación y advocacy. Por eso, es necesaria una agenda de formación para los derechos digitales que contemple los desafíos específicos del campo de la educación.
- **Sumar fuerzas**. Las organizaciones del campo de los derechos digitales han actuado, en diversos países, de manera intensa en investigación, advocacy y litigio en la temática de protección de datos personales y acceso a la información, pero no necesariamente conocen las amenazas prácticas que recaen sobre las políticas educativas. Esta alianza estratégica puede generar oportunidades de acción para ambos campos.

Referencias 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. 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.