**La encrucijada de derechos digitales en la educación**

*Es necesario abogar por el rescate de la noción de datos públicos como un bien común.*

* [*Fernanda Campagnucci*](https://www.alainet.org/es/autores/fernanda-campagnucci)

15/12/2020

* Análisis



Foto: Alexander ReyesNicaragua

-A+A

|  |  |  |  |
| --- | --- | --- | --- |
| Artículo publicado en la Revista América Latina en Movimiento No. [**551: Derecho Humano a la Educación: horizontes y sentidos en la post pandemia**](https://www.alainet.org/es/revistas/551) 10/12/2020 |  |  |  |

La pandemia de Covid-19 impuso la adopción más rápida y amplia ya vista 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 en cuestión. Esta situación colocó al campo del derecho a la educación delante de una verdadera “encrucijada” de derechos: transparencia versus privacidad. Al mismo tiempo en que es necesario reafirmar el derecho y contener retrocesos acerca de 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 de la infraestructura digital, en la que el Estado se coloque como garante de estos derechos digitales.

Existe hoy un complejo mercado de datos personales en el mundo, del cual todos somos partícipes activos — estemos o no conscientes de nuestro papel. Nuestras “huellas digitales” son recolectadas a cada instante y lugar en cada aparato, dispositivo fijo o móvil, en los sitios en los que navegamos. Tal flujo constante de datos es almacenado y compartido entre diferentes actores institucionales y corporativos, formal e informalmente, en una compleja cadena de valor de un mercado lucrativo e invisible.

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).

La educación, especialmente pública, es un territorio codiciado. En primer lugar, porque el Estado reúne gran cantidad de datos de ciudadanos para operacionalizar políticas y servicios. 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 (Adrião & Domiciano, 2018). La posibilidad de recolectar datos personales y atención pasa a valer más que el propio *software.*Estos productos llegan a ser “donados” por empresas interesadas.

Tales mecanismos de usurpación y desvío de finalidad de datos personales de la comunidad educativa tienen potencial de profundizar desigualdades y tornar todavía más vulnerables a los grupos históricamente expuestos a procesos de exclusión y discriminación.

**Derecho a la protección de datos**

El sentido del debate sobre la privacidad vive de manera inequívoca en el campo de los derechos y libertades fundamentales. Desde la Declaración Universal de los Derechos Humanos de 1948, los textos buscan proteger el derecho a la intimidad y resguardar 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).

Este principio se mantiene, pero hoy 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. Los **datos personales** son aquellos que se refieran a persona viva, identificada o identificable, incluso los que, en conjunto, puedan llevar a su identificación[1](https://www.alainet.org/es/articulo/210199?utm_source=email&utm_campaign=alai-amlatina" \l "sdfootnote1sym). El tema viene ganando nuevo impulso con una nueva onda de aprobación de leyes específicas en la última década.

Entre todos los 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.

La idea de que “la privacidad murió” —propagada por la industria de la tecnología— es uno de los mayores inconvenientes para reivindicar el derecho a la protección de datos. 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 suelen saber la extensión de los datos que son recolectados sobre ellas. Más aún, desconocen los usos que se les puede dar, y las consecuencias inmediatas y futuras de esa concesión.

**Riesgos del tratamiento inadecuado**

En los mercados digitales, 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 clasifica a las personas individualmente en categorías, de acuerdo con “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, incluyendo tipos de sites y contenidos visitados, intereses. 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).

Este mercado y sus técnicas de “perfilamiento” no sirven solamente para fines publicitarios. El mundo del trabajo y del empleo, el sector inmobiliario, 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).

Por eso la 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 consentimiento y tratamiento de datos. Con el **consentimiento**, los ciudadanos que rindan sus datos declaran estar de acuerdo con la recolección y tratamiento que se pretenda darles a ellos. Es en las **políticas** **de privacidad** —los contratos en “letra chica” de aplicaciones y servicios online— que este consentimiento suele ser recolectado. 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 optaron por la contratación de terceros.

**Tecnologías educativas**

Esos terceros son actores cada vez más presentes en el escenario: las *edtechs.*La sigla, del inglés *Education* *and* *Technology*, denomina de forma amplia a las empresas de productos para el sector educacional — hardware (equipamientos) y 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, había 100 empresas así. En Brasil, 449 (CIEB, 2020; Omidyar, 2019). Para prosperar, este mercado depende de la **infraestructura** de telecomunicaciones, electricidad e internet. Por eso, suele 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.

Todavía no hay un mapeo general y sistemático publicado sobre las prácticas de colecta de datos y de vigilancia en el campo de la educación, especialmente en América Latina y el Caribe. Mucho se discute el papel de las big techs en la violación de la privacidad digital, pero empresas más pequeñas del ramo de las edtechs también pueden tener su modelo de negocios 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. Las 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.

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”.

El pago por tales servicios es normalmente hecho en la forma de datos personales de estudiantes y maestros, algo no raro considerado por los responsables por las instituciones de enseñanza un precio justo por un servicio costoso. 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, también lo es.

La comunidad educativa debe saber exactamente lo que se hace con sus datos. De ahí la necesidad de que el tratamiento sea, siempre, acompañado de políticas de transparencia y rendición de cuentas (*accountability*). Desde que no expongan individuos, los datos deben ser tratados con la máxima transparencia, como bien común — 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. Especialmente en tiempos de pandemia, van a ser fundamentales para la plena garantía del derecho a la educación en el ambiente digital.

**Fernanda Campagnucci** es directora ejecutiva de Open Knowledge Brasil. Graduada en Periodismo y con maestría en Educación, es doctoranda en Administración Pública por la FGV-SP. <https://twitter.com/fecampa>

**Referencias**

Adrião, T. & C. A. Domiciano. (2018). “A Educação Pública e as Corporações: Avanços e Contradições Em Uma Década de Ampliação de Investimento No Brasil.” FINEDUCA - Revista de Financiamento Da Educação 8.

CIEB. (2020). *Mapeamento Edtech: Investigação sobre as tecnologias educacionais no Brasil 2019*.

Christl, W., Kopp, K. & Riechert, P. U. (2017). *Corporate surveillance in everyday life*. Cracked Labs.

Comparato, F. K. (2010). A Afirmação Histórica Dos Direitos Humanos. 7. ed. São Paulo: Saraiva.

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

Omidyar (2019). Scaling Access & Impact: Realizing the Power of EdTech. Chile Country Report.

Silveira, S. (2017). Tudo Sobre Tod@s: Redes Digitais, Privacidade e Venda de Dados. São Paulo: Edições Sesc SP.

Zuboff, S. (2015). “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30(1): 75–89.

[1](https://www.alainet.org/es/articulo/210199?utm_source=email&utm_campaign=alai-amlatina" \l "sdfootnote1anc) La normativa europea es referencia de otras legislaciones en la materia. Disponible en:

<https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt#referncias>.

Último acceso 29/10/2020.

https://www.alainet.org/es/articulo/210199