Jóvenes, transformación digital y formas de inclusión en América Latina

FundaciónCeibal

DEBATE

JÓVENES, TRANSFORMACIÓN DIGITAL Y FORMAS DE INCLUSIÓN EN AMÉRICA LATINA

JÓVENES, TRANSFORMACIÓN DIGITAL Y FORMAS DE INCLUSIÓN EN AMÉRICA LATINA

Penguin Random House
Grupo Editorial

FundaciónCeibal

2018, Centro de Estudios Fundación Ceibal

Edición a cargo de: Penguin Random House Grupo Editorial
Editorial Sudamericana Uruguaya S.A.
Yaguarón 1568 C.P. 11.100 Montevideo

Cómo citar este libro: Cobo, C; Cortesi, S; Brossi, L; Doccetti, S; Lombana, A; Remolina, N; Winocur, R, y Zucchetti, A. (Eds.). (2018). *Jóvenes, transformación digital y formas de inclusión en América Latina*. Montevideo, Uruguay: Penguin Random House.

Cómo citar un capítulo de este libro: Apellido, A. A., y Apellido, B. B. (2018). Título del capítulo. En C, Cobo; S, Cortesi; L, Brossi; S, Doccetti; A, Lombana; N, Remolina; R, Winocur; y A, Zucchetti. (Eds.) *Jóvenes, transformación digital y formas de inclusión en América Latina* (pp. xx-xx). Montevideo, Uruguay: Penguin Random House.

Encuentre esta y otras publicaciones en el Repositorio institucional del Centro de Estudios Fundación Ceibal: digital.fundacionceibal.edu.uy

Acceda al sitio de la publicación y conozca los detalles de la convocatoria: jovenes.digital

Conozca las creativas destacadas durante la convocatoria:
jovenes.digital/postulaciones-creativas

Diseño de tapa: Gabriela López Intrioni
Diseño interior: Claudio de los Santos

Pliego de imágenes: Limonada Bandida @limonadabandida

ISBN: 978-9974-888-23-4
Depósito legal: 373.192 / 18
Edición amparada en el decreto 218/996

Impreso en Zonalibro S.A.
San Martín 2437 - Tel. (+598) 2208 78 19

fundacion@ceibal.edu.uy
fundacionceibal.edu.uy
@fundacionceibal

Equipo de editores

Alessia Zucchetti
Andrés Lombana
Cristóbal Cobo
Lionel Brossi
Nelson Remolina
Rosalía Winocur
Sandra Cortesi
Sofia Doccetti

Equipo de colaboradores académicos

Andrea Valdivia
Ezequiel Passerón
Cristóbal Suárez
Cristian Maneiro
Mariel García
Maureen Berho
Pablo Rivera
Rocío Rueda Ortiz
Sebastián Benítez Larghi
Sofía Doccetti

La publicación de esta obra ha sido posible gracias a la colaboración entre el Centro de Estudios Fundación Ceibal (Uruguay), la red Digitally Connected integrada por el Berkman Klein Center de la universidad de Harvard y Unicef (Estados unidos), el Instituto de Comunicación e imagen de la Universidad de Chile (Chile), la Facultad de Información y Comunicación de la Universidad de la República (Uruguay), y el GECTI (Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática de la Universidad de Los Andes) (Colombia).

Agradecemos a los casi 400 participantes provenientes de más de 20 países quienes hicieron llegar sus propuestas a lo largo de la convocatoria. A los autores, sin los cuales este libro no sería posible. Al equipo de colaboradores académicos quienes aportaron sus conocimientos a los editores y retroalimentaron las distintas contribuciones. Al equipo de editores y las instituciones participantes, quienes lideraron este proyecto en base a los más altos estándares de calidad. Finalmente agradecemos al Plan Ceibal, particularmente a Sebastián Cabrera quien trabajó en el diseño del sitio web, así como en su funcionamiento junto a Guillermo Silva. Por último, a todas y cada una de las distintas instituciones nacionales e internacionales que apoyaron en la difusión de la convocatoria.

Introducción

La presente publicación, escrita colectivamente entre muchas miradas, es una invitación a reflexionar acerca de los desafíos y oportunidades que surgen de las prácticas digitales por parte de las nuevas generaciones. Se gesta a partir del trabajo colaborativo entre el Centro de Estudios Fundación Ceibal (Uruguay), la red Digitally Connected integrada por el Berkman Klein Center de la Universidad de Harvard y Unicef (Estados Unidos), el Instituto de Comunicación e Imagen de la Universidad de Chile (Chile), la Facultad de Información y Comunicación de la Universidad de la República (Uruguay) y el Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) de la Universidad de Los Andes (Colombia).

El proyecto nace hace más de un año y medio cuando el equipo editorial se propuso construir un libro que sirviera como espacio de diálogo y material de apoyo al público interesado en las prácticas digitales de niños, niñas, adolescentes y jóvenes. Nuestra idea era elaborar un texto que fuese accesible, de fácil lectura y que representara las múltiples voces del contexto latinoamericano. Establecimos que el eje central de la publicación debía ser la inclusión social. La heterogeneidad socioeconómica y la riqueza cultural y geográfica que caracteriza nuestro continente podía permitirnos reunir diversas prácticas, estrategias e iniciativas para explorar nuevas formas de inclusión social.

Comenzamos con los procesos de transformación que observamos en nuestras sociedades a partir de la expansión de las tecno-

logías de la información y de la comunicación. Buscamos contemplar las distintas dimensiones asociadas a dichas transformaciones que tienen a los jóvenes como principal agente social. Entre dichas dimensiones identificamos las siguientes: nuevas formas de socialización y de construcción de identidad; nuevas formas de participación y organización; nuevas estrategias para enseñar y aprender; nuevas ocupaciones e interrelaciones entre la economía y la cultura; nuevas formas de pensar la privacidad y seguridad en línea y nuevos derechos y responsabilidades que surgen a partir de un concepto de ciudadanía en constante cambio.

De este modo el grupo editorial definió las seis temáticas que estructuran el libro. Cada una presenta preguntas específicas, sin embargo, las mismas se interrelacionan y dialogan entre sí. El trabajo de revisión y selección de los artículos correspondiente a cada temática, fue coordinado por un editor experto en el tema, en colaboración con coordinadores académicos. El trabajo de revisión implicó distintas instancias de intercambio con los autores, con el objetivo privilegiar la pertinencia, calidad y contribución de cada propuesta al contenido final.

Esta publicación se compone de distintos abordajes y tipos de contribuciones que esperamos que permitan al lector acercarse a los distintos contextos latinoamericanos. A lo largo de los 37 artículos se identifican ensayos, investigaciones y experiencias de trabajo. Los autores cuentan con perfiles diversos: investigadores y académicos, estudiantes, hacedores de políticas públicas, docentes, profesionales, representantes de organizaciones de la sociedad civil, padres y ciudadanos interesados en aportar su visión sobre el tema.

Finalmente, es relevante destacar la participación de los casi 400 proponentes de 29 países, quienes nos hicieron llegar sus pro-

puestas tanto escritas como creativas con una alta participación de jóvenes.

Confiamos en que el libro constituirá un insumo para la reflexión y el conocimiento acerca del rol que ocupan las nuevas generaciones en la sociedad actual. De este mismo modo invitamos a la difusión y promoción de las iniciativas con el objetivo de continuar activando procesos de inclusión social mediada por tecnologías digitales en un continente que queremos ver cada día más conectado.

Prólogo

Hablar desde una perspectiva de inclusión digital, implica pensar de qué manera es posible asegurar que los y las jóvenes no solo tengan acceso a equipamiento, conectividad y alfabetización, sino también que tengan la posibilidad de participar plenamente en la sociedad, de influir activamente en temas que les conciernen a ellos y a sus comunidades y que sean tenidos en cuenta.

La inclusión digital de las juventudes en países de América Latina y el Caribe, debe pensarse desde las oportunidades para su integración en los procesos de desarrollo con especial atención a los contextos, dada la diversidad cultural y económica de la región.

Según el Estado Mundial de la Infancia 2017 de UNICEF, los jóvenes entre 15 y 24 años, son el grupo más conectado a Internet y se estima que uno de cada tres niños y adolescentes menores que 18 años son usuarios de la red. Cada vez más jóvenes están siendo empoderados a través del uso de herramientas digitales: a través de iniciativas gubernamentales, en centros de educación formal e informal, de manera autodidacta o a través de aprendizaje entre pares, con sus familiares o amigos.

Hace unos años, gran parte de la conversación pública sobre juventud y tecnologías se centró en los riesgos y en la seguridad; este enfoque luego se integró con las oportunidades asociadas al uso de las tecnologías. En la actualidad se ha convertido en un debate más abarcador en el que se consideran los intereses, las competencias, las habilidades, las actividades y las formas creativas, significativas, éticas y participativas de realizarlas. Este escenario ofrece una opor-

tunidad para los tomadores de decisión para promover políticas inclusivas, integrales e intersectoriales de ciudadanía digital.

Las tecnologías de la información y de la comunicación (TIC) habilitan mayores oportunidades a los jóvenes para aprender y educarse, especialmente a aquellos de sectores más excluidos o remotos. Sin embargo, en América Latina muchos jóvenes aún no acceden a los beneficios que las tecnologías digitales pueden brindarles, encontrando a menudo barreras que no solo se asocian a lo tecnológico, sino también a procesos de inclusión/exclusión social. Factores como el contexto sociocultural y económico donde se sitúan las juventudes, su condición de migrantes, su discapacidad, su origen étnico, su orientación sexual así como el acceso a conectividad y equipamiento tecnológico, las posibilidades de alfabetización digital e incluso el acceso a educación, son algunas de las variables que inciden en las oportunidades que los y las jóvenes, tienen para participar en la sociedad digital.

Para transformar las oportunidades en beneficios concretos, es clave tener en cuenta los contextos en los cuales tienen lugar las experiencias vinculadas al mundo digital, y generar entornos inclusivos.

Las políticas sociales, especialmente las educativas, han impulsado acciones a lo largo de toda la región, para reconocer los derechos de las poblaciones más excluidas, a través de estrategias de educación inclusiva, que implantaron distintos procesos de alfabetización y aprendizaje en relación con el uso de internet y las tecnologías digitales, con foco en comunicación, participación, expresión, construcción y proyección de la identidad, participación cívica y política, seguridad y privacidad y abordaje crítico de contenidos, entre otros temas.

Resulta central realizar una investigación rigurosa, evidencia, análisis sustantivo que permita comprender el impacto de la tecnología en los procesos de inclusión, especialmente vinculados con niños, niñas, adolescentes y jóvenes de contextos vulnerables en América Latina.

En ese sentido, el Centro de Estudios Fundación Ceibal, la red de colaboración Digitally Connected (integrada por el Berkman Klein Center for Internet & Society y UNICEF), el Instituto de la Comunicación e Imagen de la Universidad de Chile, la Facultad de Comunicación e Información de la Universidad de la República (Uruguay) y el GECTI de la Facultad de Derecho de la Universidad de los Andes (Colombia), se unen para la publicación de este libro colectivo que es un aporte sobre las prácticas digitales y procesos de inclusión social que las nuevas generaciones están desarrollando en los diversos contextos latinoamericanos.

Los capítulos que siguen, trazan un recorrido a partir de diferentes voces y contextos, que permite visualizar oportunidades y limitaciones en relación con experiencias de inclusión digital entre los niños, niñas y jóvenes en América Latina. En ellos se presentan reflexiones e iniciativas en torno a temas como la participación cívica y política de las juventudes promovida por soportes digitales; la construcción y proyección de identidades en espacios virtuales; los derechos y responsabilidades asociados al uso de internet; la privacidad y seguridad en línea y los abordajes sobre juventudes y economía digital.

A partir de estas preguntas: ¿Cuáles son los principales logros y limitaciones de las experiencias de inclusión digital entre los niños, niñas y jóvenes en América Latina?; ¿Cuáles son las estrategias más adecuadas para que niños y jóvenes cultiven y generen prácticas

responsables de convivencia en los entornos digitales?; ¿Qué tipo de prácticas pueden estimular el desarrollo de nuevas formas de inclusión en los entornos digitales en pro de niños, adolescentes y jóvenes? y ¿Cómo pueden padres, educadores y adultos en general favorecer nuevas formas de convivencia en entornos digitales en beneficio de niños, adolescentes y jóvenes? un colectivo de autores brinda su innovadora mirada sobre el tema.

El libro Jóvenes, transformación digital y nuevas formas de inclusión en América Latina es un trabajo colaborativo y allí radica su riqueza ya que permite realizar un recorrido por las distintas visiones que diversos referentes de América Latina tienen en relación con la inclusión digital.

María José Ravalli
Especialista en Comunicación,
UNICEF Argentina

Privacidad

Presentación de la temática

Sandra Cortesi
scortesi@cyber.law.harvard.edu[127]

Nelson Remolina
nremolin@uniandes.edu.co[128]

Mariel García
faeriedevilish@gmail.com[129]

Aunque el discurso predominante sobre la juventud y la privacidad en línea ha crecido a través de los años estableciendo que los jóvenes consideran y se preocupan por la privacidad, sucede que los jóvenes siguen entendiendo la privacidad de manera diferente a aquellos cuya edad y posición les permiten conducir la conversación. La ausencia de voces y miradas juveniles en las conversaciones que involucran privacidad es evidente al mismo nivel en que el concepto es discutido y definido. Por ejemplo, en una investigación realizada por el equipo de Juventud y Medios en el Berkman Klein Center para Internet y Sociedad, encontramos que en lugar de

127. Miembro del Centro Berkman Klein para el Internet y la Sociedad de la Universidad de Harvard. Es directora de los programas "Digitally Connected" y "Youth and Media", iniciativas de colaboración entre el Centro Berkman Klein y UNICEF.

128. Director del GECTI –Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática– y del Observatorio Ciro Angarita Barón de Protección de Datos. Universidad de los Andes, Colombia.

129. Asistente de investigación del Center of Civic Media, del MIT. Afiliada al Centro Berkman Klein para la Internet y la Sociedad de la Universidad de Harvard.

concebir la privacidad como un asunto de desafíos institucionales que involucra a terceros, los jóvenes a menudo ven el concepto como una preocupación social que tiene que ver con gestionar su privacidad en relación con personas que ya conocen ("¿qué pueden ver mis amigos y familiares?"). Por lo tanto, la gestión de la privacidad a menudo es asociada a la decisión personal de qué publicar y qué no publicar, precisamente porque los jóvenes tienden a ser conscientes de la apertura y la permanencia de la información compartida en línea, que por su parte los adultos están tan interesados en cuestionar.

Cuando encontramos que los jóvenes aprenden sobre la privacidad mediante la búsqueda de información y el aprendizaje intuitivo, quizás valga la pena reconsiderar cómo "educamos" a los jóvenes sobre los controles, las preocupaciones referentes a la temática privacidad. A medida que los adultos exploran los problemas de investigación dominantes que afectan a los jóvenes en línea, solicitar su participación puede permitirles adaptar mejor los diseños y las líneas de investigación pertinentes, comprendiendo en mayor medida cómo los jóvenes perciben las prácticas de intercambio de información con sus familias y compañeros. La posibilidad de incluirlos en dichos espacios puede permitir conocer las percepciones que influyen en su comportamiento en línea. De este modo, su participación posibilitaría a los investigadores conocer el intercambio que realizan los jóvenes entre el control y la conveniencia; cómo caracterizan su alfabetización digital y sus habilidades digitales asociadas a la privacidad; y finalmente cómo los jóvenes articulan su entusiasmo por la "privacidad social" con la fastidiosa adaptación a las políticas de acceso a la información, y el desinterés por la "privacidad institucional" que surge por el uso de su información personal por parte de terceros.

Reconocer que los jóvenes perciben y aprenden sobre la privacidad de manera diferente a los adultos no disminuye las preocupaciones de los adultos, las cuales son válidas. Hoy en día, la información digital sobre los jóvenes se busca, recoge y almacena a un ritmo sin precedentes. Ni los jóvenes ni sus responsables tienen control sobre cómo esta información es manejada por terceros, ya que los datos son frecuentemente recopilados, sistematizados, revelados y vendidos sin consentimiento y/o conocimiento.

Mientras tanto, la reputación en línea tiene una influencia cada vez mayor sobre las perspectivas futuras de los jóvenes a nivel académico, profesional y social en general. Si bien los jóvenes pueden sentirse seguros (con razón) de utilizar los controles granulares de una red social para asegurarse de que ciertos posteos no lleguen a los oficiales de admisión de sus centros educativos, familias y abuelos, continúan teniendo poca jurisdicción sobre lo que la propia plataforma puede generar a partir de la información revelada y cómo puede dar forma a la misma, tanto "en línea" como "fuera de línea". Los filtros de internet y las tecnologías de monitoreo instalados en escuelas y hogares para mitigar el riesgo, cuando no son fácilmente evitados por la juventud, a menudo terminan contribuyendo a la información personal administrada por terceros. Un monitoreo "desde abajo", más popular antes que técnico, puede promover aportes juveniles en línea altamente innovadores, pero deben ser cuidadosamente diseñados de modo de no impactar de forma negativa en la autoexpresión y la construcción de identidades saludables, adecuadas a su propia generación.

A medida que analizamos el futuro de la privacidad en línea y evaluamos los marcos recientes propuestos para la clasificación y regulación de estas problemáticas, la incorporación de las

perspectivas de los jóvenes se vuelve clave, tanto para identificar los desafíos y oportunidades contemporáneos asociados a la multiplataforma, como para lograr mayores niveles de credibilidad por parte de los jóvenes que crecerán haciendo uso de las mismas. Mayores niveles de cercanía y familiaridad con las percepciones y preocupaciones de los jóvenes en línea permitirán a los padres, educadores y políticos desarrollar estrategias de trabajo conjuntas, que los ayuden a reflexionar acerca de los hábitos actuales y construir técnicas de gestión para el abordaje de la privacidad.

No obstante lo anterior, debe tenerse presente que la privacidad en línea no depende únicamente de la perspectiva de los jóvenes sino de la labor de otros actores (usuarios de internet, las empresas, los Estados, entre otros). En internet, por ejemplo, es notorio cómo algunas empresas definen el alcance de los derechos de las personas. Esto lo hacen a través de los términos o condiciones de uso o las notas legales de las App, dispositivos móviles, las redes sociales digitales o motores de búsqueda en las que unilateralmente las empresas establecen los alcances de la protección de los derechos de las personas. Adicionalmente, los fabricantes de tecnologías o desarrolladores de *software* diseñan sus productos sin tener presente, en algunos casos, la incidencia de los mismos en la vida privada de las personas.

Estamos en plena eclosión de la economía digital en donde la información de las personas es un activo muy importante y la persona está siendo tratada más como una cosa o bien que como un ser humano. Por eso, existe un apetito, a veces insaciable, de la información de las personas porque la misma se ha convertido en la moneda de oro del siglo XXI. Asignarle un valor económico a los datos personales y a los derechos de las personas hace que sea

mucho más difícil alcanzar la protección efectiva de los derechos de los jóvenes en internet.

Visto lo anterior, resulta muy necesario pensar y repensar sobre el internet de las empresas (*internet of corporations*) y la privacidad desde el diseño y, por defecto, junto con el tratamiento ético de la información y el desarrollo de nuevas tecnologías y proyectos como, entre otros, la robótica y la inteligencia artificial. Por eso, siempre vale la pena reflexionar si todo lo tecnológicamente posible es socialmente deseable y definir los límites de la sociedad que queremos buscando un punto de equilibrio entre innovación, desarrollo tecnológico, seres humanos y derechos humanos.

La realidad sociotecnológica del siglo XXI hace necesario repensar permanentemente sobre la protección de los derechos de los jóvenes. Ya no solo convivimos en un mundo fronterizo y territorial sino principalmente en un mundo transfronterizo y global denominado, entre otras formas, ciberespacio. Los retos del ciberespacio son de mayor calado –piénsese que más de 56% de la población mundial tiene acceso a internet– y las autoridades nacionales es muy poco o nada lo que pueden hacer porque sus normas locales no las facultan para actuar transfronterizamente. Actualmente tiene mayor incidencia y campo de aplicación la política de una empresa privada que las normas locales de cualquier país. Un ejemplo de ello es la política de privacidad de Facebook, la cual vincula jurídicamente a más de 2,1 billones de personas que viven en diferentes países del mundo, provienen de diferentes culturas sociales, lingüísticas y jurídicas.

En otras palabras, internet cambió el mundo, pero el mundo no ha cambiado frente a internet. Si seguimos haciendo más de lo

mismo no lograremos los resultados que necesitamos frente a la protección de los derechos de los jóvenes en el ciberespacio.

Visto lo anterior, es necesario replantear muchas cosas. Una de ellas es, precisamente, convertir a los jóvenes en los principales protagonistas de la defensa de sus propios derechos. Aunque en algunas partes se está siguiendo ese camino a través de la educación (en casa y en los centros educativos) es necesario reforzar ese aspecto. No podemos quedarnos esperando la acción de las autoridades porque no es suficiente y muchas veces no es oportuna. Por eso, debemos cambiar el enfoque represivo/sancionatorio de las autoridades por un preventivo de la vulneración de derechos que consolide una cultura de protección de la privacidad y demás derechos de los jóvenes en el ciberespacio.

Millennials Privacy

Danilo Doneda
danilo.doneda@gmail.com
Cedis/IDP

Yasodara Córdova
ycordova@cyber.harvard.edu
Digital Harvard Kennedy School Fellow

Palabras clave:
privacidad - internet - niños

Tecer considerações sobre a privacidade de crianças implica em projetar-se para um futuro que bate à nossa porta a cada like no Facebook, a cada página lida por um estudante em seu livro didático eletrônico e em outros tantos pequenos atos que são registrados. Atos que eram essencialmente efêmeros, praticados por crianças na busca do desenvolvimento de suas capacidades e personalidades, hoje são registrados, com consequências que podemos apenas especular. Para o direito, é um desafio garantir a plena liberdade destes futuros cidadãos, considerando os efeitos pessoais, sociais e até econômicos do registro de seus dados, reconhecendo a importância fundamental de seu uso estar vinculado apenas ao seu interesse – e, se considerarmos que muitos dos efeitos de decisões tomadas agora em relação a crianças irão se projetar para daqui a dez ou quinze anos, no momento em que adentrar a idade adulta, esta tarefa ganha contornos ainda mais complexos. Proporcionar à crianças as

vantagens do desenvolvimento tecnológico, ao mesmo tempo em que a liberdade, condição fundamental para o livre e completo desenvolvimento da sua personalidade, é mantida íntegra, é um difícil desafio e a abordagem dessas questões exige multidisciplinaridade e agilidade, que devem estar refletidas tanto nas abordagens regulatórias quando na implementação e design de ferramentas à disposição de crianças e cuidadores.

A pervasividade da tecnologia, entre outros fatores, faz com que enfoques que proponham meramente restringir o acesso de crianças a tecnologias sejam não raro alvo de críticas, ao reconhecer na internet uma realidade constante e parte integral da vida das crianças e dos contextos familiares de hoje. O ambiente digital não deixará de fazer parte das vidas de crianças e adultos. Para a criança, estar conectada é se inserir em contextos sociais de maneira adequada às suas potencialidades e necessidades e, em diversas circunstâncias, é mais uma dimensão na qual explorar suas potencialidades. É entendimento inclusive de muitos pais que a convivência de crianças em redes sociais é necessária, o que faz com que não seja raro que os próprios pais até mesmo as ajudem a contornar alguns dos mecanismos que possam impedi-las de exercitar a experiência digital de maneira completa.

Pode-se sintetizar três grandes problemas relacionados à privacidade infantil para os próximos anos em (i) Proteção da identidade e da personalidade; (ii) Tutela dos dados; (iii) Gestão de históricos de dados. Todas eles merecem reflexões aprofundadas, porém é premente que seja realizada uma reflexão inicial sobre as próprias bases nas quais serão construídos os instrumentos regulatórios e técnicos para balizar o contato da criança com a tecnologia –especialmente com a internet.

A proteção da criança na internet há de levar em conta que a Web existe em estado constante de evolução e a necessidade de se adaptar às suas mudanças. Durante os primeiros anos da Web era comum que as pessoas tivessem a iniciativa de criar seus próprios sites e espaços, de modo a gerenciar de forma direta a sua presença digital, detendo na grande maioria das vezes o poder sobre quais informações compartilhar. Chats e salas de bate-papo ainda não estavam integrados e permitiam presenças totalmente diferentes entre si, independentes uma da outra, assim como fóruns e grupos temáticos, garantindo extrema flexibilidade na gestão da identidade digital, inclusive para as crianças que tinham acesso à rede. A existência desses espaços foi, aos poucos, diminuindo, à medida em que se desenrolava um conjunto de acontecimentos: o desenvolvimento da interoperabilidade por meio de uso de metadados estruturados sobre recursos digitais, implementado com sucesso, por exemplo, pelo Facebook (Van Dijck, 2012); o aumento do uso de redes sociais, a migração do uso de fóruns e chats isolados para ferramentas integradas de conversação, como o Facebook Messenger, integrado ao Facebook, por exemplo e o desenvolvimento de interfaces intuitivas, permitindo que crianças tenham acesso de maneira mais natural às redes sociais e portanto dispensem a construção de sites próprios.

Grande parte da regulação sobre o uso da internet por crianças passa pelas normas impostas em tais plataformas. A facilidade de utilização destes espaços "fechados" fez com que essas plataformas atraíssem para si a atenção das crianças, que aderiram às plataformas de redes sociais massivamente. Isso acaba por submeter as interações das crianças aos termos e condições de uso das plataformas. Além das consequências para a produção intelectual das crianças, que, como ocorre com os adultos, acabam por aderir

a termos de uso capazes de limitar seus direitos sobre a própria produção intelectual, existem ainda futuras consequências para a apresentação da sua personalidade, já que é possível que um verdadeiro histórico online seja formado e mantido à revelia do indivíduo quando se tornar adulto, tais como fotos postadas por parentes ou amigos, por exemplo.

Dentre as soluções regulatórias mais usuais para a proteção de dados da criança está a ênfase no instituto do consentimento do pai ou responsável para a utilização da rede, em particular pela influência da legislação norte-americana (COPPA) sobre o tema. Esta legislação, aplicável a crianças abaixo de 13 anos sob jurisdição norte-americana, acaba por ter efeito reflexo até mesmo fora desta jurisdição, visto que em regras as plataformas online largamente utilizadas por crianças são controladas por empresas com sede nos Estados Unidos e com termos de uso que refletem os condicionamentos da sua legislação. O COPPA, em resumo, estabelece que dados de crianças abaixo de 13 anos somente possam ser coletados com autorização dos pais ou responsáveis e que determinados padrões de privacidade, segurança e restrições para conteúdo publicitário devam ser observados – o que faz com que, de fato, algumas destas plataformas simplesmente não aceitem crianças como usuários ou então desenvolvam versões especialmente adaptadas para crianças (Doneda y Rossini, 2012).

Ainda que se reconheça no COPPA um importante marco ao proporcionar limites claros para a coleta e uso de dados de crianças, é necessário vislumbrar que ele aborda apenas parcialmente a problemática da privacidade para crianças e que alguns de seus paradoxos devem ser descortinados para que estes limites sejam considerados como ponto de partida para novas iniciativas.

Em primeiro lugar, a gramática que acompanha a aplicação de regras de privacidade e proteção de dados –que está presente no COPPA– está baseada ao paradigma do segredo e do controle sobre a própria informação como ferramenta principal. Não surpreende que seja esta a abordagem, visto que a regulação do fluxo de dados pessoais foi, desde suas primeiras proposições, idealizada a partir dos instrumentos que se podiam conceber, que faziam sentido em situações nas quais este fluxo de dados era de volume mais visível e controlável. Assim, opções contratuais, a autorização e consentimento por muito tempo foram os principais vetores para autorizar o tratamento de dados com o fim de "proteção da privacidade".

Estes instrumentos de natureza contratual, porém, são marcadamente formais e usualmente pouco compreensíveis para usuários mais jovens por conta da sua abstração –muito embora o problema que eles procuram enfrentar seja essencialmente o controle sobre o uso dos dados pessoais. No caso de crianças, especificamente, há de se notar que o problema aumenta de magnitude ao se colocar sob a responsabilidade dos pais decisões sobre cujas consequências, em muitas ocasiões, possam ir além da capacidade de discernimento até mesmo deles –um problema crônico dos termos de uso. Outro fator de extrema relevância é que tais instrumentos podem ter seu caráter meramente formal acentuado pela discrepância entre seu conteúdo e a praxis da utilização das plataformas por crianças. A existência de tal discrepância é sugerida, por exemplo, pelos dados da pesquisa TIC Kids Brasil 2015, ao identificar que 63% das crianças entrevistadas entre 9 e 10 anos possuem perfil em redes sociais, percentual este que sobre para 79% entre crianças de 11 a 12 anos (CETIC, 2015).

Algumas das soluções em desenvolvimento, como por exemplo o Link, da Google, (ainda não disponível para brasileiros),

procura colocar as responsabilidades de identificação, monitoramento e rastreamento das atividades das crianças sob a tutela dos pais por Design. O sistema do consentimento dos responsáveis, a bem da verdade, traz para esta área algumas das contradições que o sistema do consentimento apresenta na matéria geral de proteção de dados e, inclusive, exacerba-os em alguns pontos. Um caso a ser considerado, neste ponto, é o do YouTube, que exige que seus usuários registrados possuam a idade mínima de 18 anos ao mesmo tempo em que pesquisa indica que 48 dos 100 canais de maior audiência no YouTube Brasil abordam conteúdo direcionado ou consumido para/por crianças até 12 anos (Correa, 2016). Para tal, experiências como o do Link podem ser positivas, uma vez que a decisão sobre dados e atividades interativas das crianças pode ser mais responsável. Ainda assim, estamos falando de um sistema que tende apenas repassar a responsabilidade sobre o consentimento do rastreamento e registro de dados de crianças para os pais. Evidentemente, o futuro dirá se ferramentas que transferem a propriedade dos dados na maioridade para o próprio indivíduo que gerou os dados, bem como o direito à deletar conteúdos pregressos à vida adulta, serão reivindicadas com a mesma força que os controles parentais. Fica evidente que só a regulação, ainda que em termos de uso, não surte efeito se não for traduzida em estudos sofisticados o suficiente para gerarem ferramentas e um design mais eficaz e útil, que possibilitem o uso responsável de aplicações online.

Proporcionar às crianças uma experiência rica e variada com as possibilidades trazidas pelas tecnologias encontra obstáculos tanto nas abordagens excessivamente protecionistas dos problemas quanto no fato de que muitas das novas possibilidades trazidas pelas tecnologias são capitaneadas por interesses corporativos que não

costumam levar em conta os interesses e direitos das crianças. A construção e consolidação de ferramentas e institutos técnicos, educacionais e regulatórios que evitem tais derivações tão óbvias quanto perigosas, considerados os riscos de se privar a criança de liberdades fundamentais em cenários nos quais as privações de liberdade assumem novas formas e potencialidades, não é uma opção, porém parte essencial do legado para as gerações futuras.

Referências

CETIC (2015). TIC Kids Online Brasil 2015. Recuperado de: http://cetic.br/tics/kidsonline/2015/criancas/C1/

Correa, L. (2016). Geração YouTube: Um mapeamento sobre o consumo e a produção infantil de vídeos para crianças de zero a 12 anos. *ESPM Media*. Recuperado de: http://pesquisasmedialab.espm.br/criancas-e-%20tecnologia/

Doneda, D.; Rossini, C. (2013). A proteção de dados de crianças e adolescentes na internet. En: *TIC Kids Online Brasil 2012: pesquisa sobre o uso da internet por crianças e adolescentes*. (Coord. Alexandre F. Barbosa). São Paulo. 37-48.

Van Dijck, J. (2012). Facebook as a tool for producing sociality and connectivity. *Television & New Media*, 13(2). 160-176.

Los datos de niños, niñas y adolescentes en el flamante Reglamento Europeo de Protección de Datos

Oscar Puccinelli
opuccine@unr.edu.ar

Universidad Nacional de Rosario, Argentina

Palabras clave:
cyberbulling - *grooming* - grupos vulnerables

En 2016 –y con vigencia plena desde 2018– el Parlamento Europeo y el Consejo (UE) aprobó el Reglamento N.º 2016/679, "relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" (mejor conocido como "Reglamento general de protección de datos"), en reemplazo de la Directiva 95/46/CE, y a cuya diferencia no requiere para su entrada en vigencia de normas de transposición nacionales.

Entre sus disposiciones contiene una serie de reglas específicamente aplicables al tratamiento de los datos personales de niños, niñas y adolescentes, las cuales han sido incorporadas en función de la especial protección que requiere este sector de la población debido a su especial situación de vulnerabilidad.

Ya desde sus considerandos, se destaca primeramente que esa imprescindible y específica protección de los datos personales de este colectivo se requiere debido a que por su juventud pueden desconocer tanto los riesgos y consecuencias que se derivan del tratamiento de la información que a ellos se refiere, como cuáles son los derechos y garantías que les conciernen con respecto a dichos tratamientos. Se agrega además que tal protección específica debe aplicarse en ciertos ámbitos que presentan mayores riesgos, en particular, cuando tales datos se utilizan con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y cuando sus datos se obtengan al utilizar servicios ofrecidos directamente a ellos, afirmándose que el consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños (considerando n.º 38).

Más adelante, cuando se refiere al funcionamiento de los principios relativos al tratamiento de los datos personales, y concretamente al mencionar el principio de transparencia, destaca que cuando el tratamiento afecte a niños, toda información y comunicación debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender (considerando n.º 58).

Luego, al tratar los derechos emergentes de la aplicación de tales principios, y más puntualmente al referirse a los derechos de rectificación de los datos personales, al olvido, supresión y oposición al tratamiento, y en lo relativo a la retractación del consentimiento para el tratamiento, expresa como particular situación a ponderar la de quien lo otorgó siendo niño, "cuando no se es plenamente consciente de los riesgos que implica el tratamiento", y especialmente "cuando se trata de datos obrantes en internet" (considerando n.º 65).

Finalmente, en los considerandos se alerta de manera general acerca de la existencia de riesgos –de gravedad y probabilidad variables– para los derechos y libertades de las personas físicas, y se menciona específicamente a los casos de tratamientos de datos personales de personas vulnerables, en particular los de los niños (considerando n.º 75).

Ya en su articulado, al referirse al principio de licitud del tratamiento, expresamente exige que en los casos en que los tratamientos se realicen por resultar necesarios para la satisfacción de intereses legítimos del responsable del tratamiento o de un tercero –excepto que se trate de autoridades públicas en ejercicio de sus funciones–, para que dicho tratamiento sea lícito debe verificarse si sobre tales intereses no prevalecen intereses, derechos o libertades fundamentales del interesado que requieran protección, en particular cuando este sea un niño (art. 6, inc. f).

Más adelante, al abordar las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, establece que cuando se ofrezca directamente a niños estos tipos de servicios, el tratamiento de sus datos personales se considerará lícito siempre que tenga como mínimo 16 años, aclarando que: a) los Estados miembros podrán establecer por ley una edad inferior que no se menor a los 13 años; b) si fuera menor de la edad requerida, se debe contar con el consentimiento del titular de la patria potestad o tutela, que solo habilitará el tratamiento en la medida de tal autorización, y c) cuando el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, el responsable del tratamiento debe hacer esfuerzos razonables, teniendo en cuenta la tecnología disponible, para verificar que quien lo dio o autorizó es el titular de la patria potestad o la

tutela. Finalmente, en este punto deja a salvo que todo lo anteriormente reglado "no afectará a las disposiciones generales del derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño" (art. 8).

Ya al referirse al principio de "transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado", indica que el responsable del tratamiento debe tomar medidas oportunas para que al proporcionar información o al comunicar cuestiones relativas al tratamiento, lo sea en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño (art. 12).

Luego, al ocuparse las herramientas disponibles para la mejor tutela de los datos personales, abordando las reglas dirigidas a la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del Reglamento, indica que los Estados miembros, las autoridades de control, el Comité Europeo de Protección de Datos y la Comisión Europea promoverán su elaboración, y que las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento pueden elaborarlos, modificarlos o ampliarlos con objeto de especificar la aplicación del presente reglamento, mencionando que deben abordar especialmente "lo que respecta a la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño" (art. 40).

Finalmente, al referirse a las funciones de la autoridad de control principal, expresa que le compete a esta promover la sensibilización del público y su comprensión de los riesgos, normas, garantías

y derechos en relación con el tratamiento, destacando que las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención (art. 57).

Como puede verse, todas las referencias específicamente contenidas en el Reglamento, ya sean las volcadas en sus considerandos como en su articulado, apuntan a reforzar la protección de datos de este especial y vulnerable sector, y en realidad no constituyen más que especificaciones normativas de principios específicos que fueron largamente tratados por la doctrina especializada, la jurisprudencia, y en especial por las disposiciones y resoluciones de las autoridades de control y de las redes especialmente integradas por estas, que se preocuparon todavía más fuertemente de la temática a partir del auge de las redes sociales y consecuentemente de la internet 2.0.

Así, por ejemplo, en el marco de las actividades de la Red Iberoamericana de Protección de Datos, el 02/12/09 se aprobó en México una serie de recomendaciones elaboradas por un grupo de expertos latinoamericanos en julio de ese año y que fueron volcadas en el Memorándum de Montevideo ("Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes", elaborado precisamente en la ciudad de Montevideo, Uruguay), donde se destacó que internet es un medio de comunicación al que los menores acceden cada vez con mayor facilidad y que más allá de los obvios beneficios que tal acceso conlleva para los derechos de acceso a la sociedad de la información y del conocimiento, existen también riesgos potenciales para los niños, niñas y adolescentes que son inherentes al uso de tecnologías de la información, de modo que resulta necesario brindar una adecuada protección a la infancia, que por su complejidad e importancia demanda una aproximación

holística de todos los actores involucrados, atendiendo a la diversidad social, cultural, política y normativa existente en la región.

La principal razón de la adopción de estas reglas se ubica no solo en que los niños, niñas y adolescentes, por ser tales, están más expuestos a los riesgos generalmente derivados del tratamiento de los datos personales, sino en que este grupo social quedó en mayor situación de vulnerabilidad a partir de la aparición de las redes sociales, las que han potenciado y diversificado los casos no solo de aprovechamiento sino de delitos dirigidos contra estos (por ejemplo, pornografía infantil, *grooming*, *cyberbullying* y muchas otras formas de afecciones), máxime cuando se presenta como característica diferencial de los denominados *millenials* –aunque como van las cosas, parece ser solo por ahora– el vivir no ya "con" internet sino "en" internet, situación que lejos de pensarse en retroceso, tiende a consolidarse cada vez con mayor fuerza, en especial si se piensa que estamos transitando la era de internet 3.0 y con la mirada puesta en la internet 4.0, que estará caracterizada por una inmersión prácticamente total de nuestras vidas en el ámbito de la red y donde ya no solo se tiene claro que llevaremos internet en nuestros cuerpos sino que también cualquier objeto que no sea conectable a esta será lisa y llanamente obsoleto, de modo que parece que ya no habrá vida más allá de internet.

En tal contexto, si ya de por sí al calor de estos permanentes desarrollos habidos y por haber en la red pueden imaginarse los importantes riesgos que se presentan para las personas adultas, mucho más lo serán, si no se toman las prevenciones necesarias, para los grupos especialmente vulnerables –en especial, entre ellos, para los niños, niñas y adolescentes–, y por ello se resalta la necesidad de atender a las recomendaciones emanadas de los organismos y

entidades especializados, entre los cuales, como se dijo, merecen especial atención las emanadas del Memorándum de Montevideo, que contiene importantes recomendaciones que son dirigidas tanto a los Estados (acerca del marco legal; de la aplicación de las leyes y de los criterios para la formulación de políticas públicas) como a la industria.

Big Data en la educación: un riesgo necesario

Armando Guío
a.guio139@uniandes.edu.co

Universidad de los Andes, Colombia

Palabras clave:
Big Data - educación - privacidad

Introducción

Los retos que enfrentarán las futuras generaciones latinoamericanas requieren de enormes esfuerzos en el campo social y educativo. La región enfrentará una nueva revolución económica impulsada por las tecnologías de la información. Sin embargo, esta misma región deberá superar conflictos sociales producto de la inequidad social que ha generado distintas formas de violencia (Marczak y Engelke, 2016).

Uno de los sectores que mayores contribuciones debe hacer a estos cambios es el de la educación. Son varios los retos que enfrenta la educación en Latinoamérica y en especial en países como Colombia. El objetivo de este sector ya no es necesariamente obtener la mayor cobertura, sino la mejor calidad posible. Esta calidad no solo debe ser vista en términos de conocimientos técnicos, sino de valores, convivencia y la capacidad de construir tejido social e integración (Bellei, 2013).

Para obtener dicho fin, es claro que los Estados y los líderes del sector educativo tendrán que valerse del uso de tecnologías como el Big Data y la minería de datos para realizar una distribución de los pocos recursos disponibles, identificando las deficiencias del sector y logrando resolver los verdaderos problemas del sector. Hay riesgos intrínsecos y propios del uso de nuevas tecnologías, pero es necesario asumirlos y enfrentarlos debido a los beneficios que puede traer a la educación de millones de niños y niñas (National Academy of Education, 2017). Asimismo, Latinoamérica tiene una carrera en contra del tiempo y debe superar de manera rápida un rezago de varias décadas, por lo que se requiere una transformación del sector y no hay tiempo que perder en este sentido (Arocena y Senker, 2003).

A continuación, se presentarán algunos de los cambios que puede introducir el Big Data en el sector de la educación en la región, los retos que impondría y la forma de resolverlos.

De saberlo todo a saber lo esencial

Las instituciones de educación primaria y secundaria han venido recolectando diversa información sobre sus estudiantes. Dentro de los colegios los estudiantes comparten con sus profesores, psicólogos y compañeros de clase, entre otros, información sobre su rendimiento escolar, sus habilidades intelectuales, sus sentimientos, su estado de salud, sus pensamientos políticos y sus orientaciones sexuales.

El acceso a toda esta información y el uso que se le ha dado ha variado según los cambios que se han presentado en los modelos educativos en las últimas décadas. Así las cosas, el sistema educativo de principios y mitades del siglo XX impuesto en Latinoamérica se basaba, en términos generales, en figuras de autoridad y repre-

sión de los comportamientos que no eran socialmente tolerados. La autoridad en los colegios se traducía en la superioridad moral e intelectual de los educadores y en un modelo hegemónico (Puiggrós, 1991). El mantenimiento de las estructuras de poder utilizaba diversos mecanismos para controlar al menor y corregirlo, cuando se encontraba en situaciones consideradas como irregulares (García Méndez, 1998). Aunque es claro que este modelo educativo ha venido cambiando, todavía permanecen algunas de sus características haciendo de muchas instituciones educativas verdaderos campos de batallas, donde la información se utiliza como medio de defensa y control del estudiante. Unido a lo anterior, la alta cantidad de información hace que mucha de esta contenga errores y presente datos equivocados sobre los menores. El acceso a información errada constituye una de las principales amenazas a la privacidad y libertad de los estudiantes, pues conservar información equivocada puede ser completamente destructivo para su vida y futuro desarrollo.

La introducción del Big Data dentro de los colegios daría un cambio sustancial a esta aproximación en cuanto al tratamiento de la información de los estudiantes. Aunque esta es una tecnología basada en el acceso a un número elevado de datos, su verdadera eficiencia no se basa en la cantidad de información disponible, sino en la calidad de la misma y en criterios claros de recolección (UNECE Big Data Quality Task Team, 2015). El acceso masivo e indiscriminado a la información tendría que reducirse, ya que se prioriza la calidad a la cantidad. Este es un beneficio del Big Data que asegura la protección de los datos personales de los menores.

El Big Data también permite reevaluar el papel de actividades relacionadas con exámenes estandarizados y pruebas internacionales, ya que establece qué tipo de información debe extraerse de

este tipo de exámenes y los fines sociales de dichas pruebas (Mayer-Schönberger y Cukier, 2014). Al estudiante se le evalúa no solo con el fin de entender su desempeño integral, sino que aporta información vital sobre el sistema educativo al que pertenece y que puede ser de utilidad en la creación de políticas públicas. La evaluación pasa de un sentido netamente individualista a ser esencial en todo un sistema de análisis de información público. Aunque los Estados ya utilizan esta información para definir la calidad de un sistema lo hacen en números totales. En este caso lo relevante es poder extraer de un solo examen un sinnúmero de información que después se procesa con la información extraída de otras pruebas, dando unas conclusiones vitales para el futuro de la educación en cada país.

Los riesgos del Big Data

Ahora bien, el Big Data también presenta riesgos intrínsecos, ya que es una herramienta de acceso a información que de no tener control puede prestarse para abusos, expone información de menores de edad, que son sujetos de especial protección y puede ser utilizada para fines distintos al mejoramiento de la educación, como el mercadeo y la comercialización. Igualmente, existe una exposición de los menores a los peligros de filtración y exposición de la información como producto de deficientes medidas de seguridad de la información (National Academy of Education, 2017).

Una de las principales formas de limitar estos riesgos es mediante una regulación comprensiva, especial y sectorial, que proponga incluso un nuevo paradigma sobre la protección de datos en Latinoamérica y en el mundo.

El paradigma de Montevideo y una deuda pendiente

El Memorándum de Montevideo (2009) es una de las principales fuentes sobre la protección de la información personal de los menores de edad en la región. Este documento expresa de forma clara los peligros que se empezaban a evidenciar para los menores de edad dada la irrupción de las nuevas tecnologías de la información y las redes sociales. Por esto, el mismo documento señalaba una serie de principios que debían inspirar la regulación de cada uno de los países del continente al respecto, principalmente el interés superior de dicha población (Schiavi, 2013).

No obstante, este memorando fue adoptado por algunos países de forma excesiva, generando muchos de los miedos que existen hoy frente a la tecnología y los datos de los niños y niñas. Ejemplo de lo anterior es la legislación colombiana, que señaló una prohibición general para tratar datos personales de niños, niñas y adolescentes. Esta prohibición fue moderada por la reglamentación posterior de la ley y por la revisión hecha por la Corte Constitucional de Colombia. No obstante, la prohibición dejó un claro mensaje en cuanto a las limitaciones que tenía el acceso a este tipo de información y los riesgos que significaba. Esto claramente ha repercutido en el acceso del sector educativo a las tecnologías de la información y al miedo a ser expuesto a millonarias sanciones (Said-Hung, Montoya Lemus, y Durán Ruiz, 2016).

De esta forma, en países como Colombia y en el resto del continente hay una deuda pendiente, y es la de lograr una regulación específica y sectorial que permita un balance entre la protección adecuada de los menores y el uso eficiente de recursos que mejoren todo el sector. Es claro que esta regulación no debe desconocer los principios que rigen la protección de datos en la región, pero debe

tener en cuenta las necesidades y beneficios que la tecnología aportaría al sector.

Una nueva regulación

El eje central de la regulación del Big Data en el sector educativo debe ser la protección de la privacidad. Sin embargo, en este caso la privacidad no debe ser vista como una protección de los datos personales de los niños, sino como un medio de control del excesivo poder que da el Big Data a las personas e instituciones que tienen acceso a esta tecnología (Ulbricht y Von Grafenstein, 2016). Lo importante es democratizar las reformas de la educación y el sector. Por esta razón, una nueva regulación debe proponer que, por ejemplo, los resultados de la minería de datos sean redistribuidos dentro de todos los interesados del sector educativo y debe permitir el acceso de diversos sectores a esta información. Solo de esta forma se justificará asumir los riesgos del Big Data.

Por lo tanto, la regulación propuesta debe caracterizarse por contener al menos los siguientes dos elementos:

Participación democrática

El Big Data debe ser un elemento que permita obtener una participación democrática en la reforma de la educación. Por eso, la regulación del acceso a información personal procesada debe permitir el acceso a distintas fuentes de información, control sobre la información utilizada y el derecho a decidir qué información se hace pública y cuál debe ser anonimizada. La regulación debe propender entonces a que la información utilizada para este tipo de investigación y análisis sea publicada de forma anónima, salvo que pueda verificarse que los beneficios del análisis realizado influyan a una

persona o grupo de personas específico y que por esto requiere dicha identificación. Además, si la información utilizada es anónima, los resultados pueden ser compartidos con mayor facilidad, e incluso entre distintos países de la región y, por qué no, del mundo. Asimismo, es esencial que la información utilizada para el Big Data sea obtenida de fuentes transparentes y hasta un punto objetivas que no desvíen los resultados obtenidos.

Dadas las condiciones anteriormente mencionada, el Big Data será una herramienta efectiva para democratizar el sector educativo y permitir que la ciudadanía se enriquezca de la información obtenida.

Perfilamiento no discriminatorio

Los perfilamientos que se realicen mediante el Big Data deben garantizar que no haya discriminación ni elementos prejuiciosos o tendenciosos dentro del sector educativo. Por esto, el uso de cierta información sensible (raza, religión, orientación sexual, etc.) para el análisis de Big Data debe permitirse si fuera beneficioso para la población de la cual se extrae esta información. Dicho beneficio debe traducirse en una diferenciación positiva que se verá traducida en la implementación de acciones afirmativas dentro del sector educativo y dirigidas a miembros de ciertos grupos sociales diferenciados (Celis-Giraldo, 2009).

Conclusión

El Big Data es una herramienta esencial para tomar decisiones importantes en la creación de presupuestos fiscales para la educación y mejorar el direccionamiento de los recursos propios de este sector. Asimismo, puede permitir encontrar fallas generalizadas

dentro del sector y elementos a mejorar. Sin embargo, esta no es la única herramienta para mejorar la educación de la región y este tipo de tecnologías no puede dejar de lado el poder de otras actividades que se centran en el caso de cada estudiante y en sus necesidades y preocupaciones propias. El Big Data es solo una herramienta para dirigir las políticas públicas de la educación, y no necesariamente para definir la labor de los maestros dentro de sus aulas. Los resultados de este tipo de análisis deben ser vistos como una ayuda, mas no una forma de reemplazar el trabajo de los profesionales de la educación.

Sin embargo, el uso del Big Data en el sector educativo es necesario dado que permite generar nuevos principios frente al uso de la información en los colegios y desarrollar un nuevo paradigma sobre el uso de la información en la región. Ante todo, el Big Data permite que la educación sea vista como un sector al cual las tecnologías de la información pueden llegar a brindar importantes beneficios, desde que se regule su uso y se utilice por ende de manera responsable. Este puede ser el inicio de una nueva y propia concepción de la privacidad para los latinoamericanos, una en que más que tener un derecho, tengamos la posibilidad de democratizar las estructuras de poder existentes que direccionan la educación y otros sectores. Por esto, el Big Data, más que un riesgo, es una fuente de posibilidades.

Referencias

Arocena, R.; Senker, P. (2003). Technology, Inequality, and Underdevelopment: The Case of Latin America. *Science, Technology, & Human Values,* 28 (1), 15-33.

Bellei, C. (2013). *Situación Educativa de América Latina y el Caribe: Hacia la educación de calidad para todos al 2015.* Santiago, Chile: Oficina Regional de Educación para América Latina y el Caribe/UNESCO.

Celis-Giraldo, J. (2009). Las acciones afirmativas en educación superior: el caso de los Estados Unidos. *Educación y Educadores,* 12 (2), 103-117.

García Méndez, E. (1998). *Derecho de la infancia - adolescencia en América Latina: De la situación irregular a la protección integral.* Bogotá, Colombia: UNICEF.

Marczak, J.; Engelke, P. (2016). *Latin America and the Caribbean 2030: Future Scenarios.* Washington, USA: Inter-American Development Bank.

Mayer-Schönberger, V.; Cukier, K. (2014). *Learning with Big Data. The Future of Education.* Estados Unidos: Houghton Mifflin Harcourt.

National Academy of Education. (2017). *Big Data in Education: Balancing the Benefits of Educational Research and Student Privacy.* Washington: National Academy of Education.

Puiggrós, A. (1991). Teoría y política en la pedagogía latinoamericana. En: A. Puiggrós, *Democracia y autoritarismo en la pedagogía argentina y latinoamericana*. 2.ª Edición, pp. 11-37. Buenos Aires, Argentina: Editorial Galerna.

Said-Hung, E.; Montoya Lemus, C.; Durán Ruiz, F. (2016). Aproximación normativa de protección de datos y los derechos de los menores de edad en Colombia. *Revista Linhas, 17* (33), 158-175.

Schiavi, P. (2013). La protección de los datos personales en las redes sociales. *Revista de Direito Administrativo & Constitucional*. 13 (52), 145-178.

Ulbricht, L.; von Grafenstein, M. (2016). Big Data: big power shifts?, *internet Policy Review.* 5 (1).

UNECE Big Data Quality Task Team (2015). *A Suggested Framework for the Quality of Big Data.* UNECE/HLG.

Contratación de servicios educativos en la nube: Riesgos y recomendaciones desde la perspectiva de la protección de datos personales

Patricia Díaz Charquero
pdiaz@oce.edu.uy

Mariana Fossatti
mfossatti@gmail.com

DATYSOC*[130]*, Uruguay

Palabras clave:
protección de datos personales - instituciones educativas - contratación de servicios educativos *cloud*

Introducción

Actualmente se observa una enorme irrupción de servicios de tecnología educativa basados en el *cloud computing o computación en la nube*, así como la creciente interoperabilidad de estos servicios. De estas tecnologías surgen muchas posibilidades de innovación en el ámbito educativo, pero también diversas incertidumbres y desafíos. El almacenamiento y la posibilidad de tratamiento masivo

130. DATYSOC es un grupo de investigación que busca proporcionar una evaluación del estado actual del arte de la vigilancia de las comunicaciones, de la privacidad y de la ciberseguridad en Uruguay (http://datysoc.org/).

de datos de estudiantes permiten acumular información y generar perfiles personales desde la temprana edad en que comienzan la actividad escolar y durante todo su tránsito educativo. En este nuevo contexto surge la disyuntiva entre confiar ciegamente en las soluciones tecnológicas o analizarlas con una mirada crítica que permita evaluar sus implicancias legales y éticas. En este artículo brindamos elementos para responder, al menos, estas preguntas: ¿qué es la computación en la nube?, ¿qué aspectos evaluar al momento de optar por las diferentes soluciones de tecnología educativa disponibles?, ¿cuáles son los principales riesgos en materia de privacidad y protección de datos personales al momento de contratar servicios de educativos en la nube?

¿Qué es la computación en la nube?

Si bien no existe una definición universalmente aceptada de computación en la nube, existen organismos internacionales cuyos objetivos son la estandarización de tecnologías de la información, y específicamente de las tecnologías basadas en la nube. El Information Technology Laboratory del NIST[131] se encarga de los estándares de las tecnologías de la información y define a la computación en la nube como:

> Un modelo que permite el acceso bajo demanda a través de la red a un conjunto compartido de recursos de computación configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor del servicio (Mell, Grance *et al.*, 2011, traducción nuestra).

131. Más información en: https://www.nist.gov/

Este modelo implica la posibilidad de que los diferentes recursos físicos (como por ejemplo almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales) sean asignados y reasignados dinámicamente, de modo que el cliente, normalmente, no tiene control ni conocimiento sobre la posición exacta de los recursos proporcionados.

Modelos de computación en la nube según tipo de acceso

De las diferentes clasificaciones de modelos de computación en la nube realizadas por el NIST, nos interesa particularmente describir la clasificación relacionada con el tipo de acceso, ya que este condiciona la posibilidad de control efectivo de los datos.

De acuerdo a esta clasificación, encontramos que los centros de datos virtualizados pueden utilizar modelos de nube privada, nube pública o nube híbrida.

La "nube privada" es una infraestructura informática (máquinas, redes, almacenamiento, centros de datos, etc.) dedicada a una organización individual; está situada en las instalaciones de la propia organización o bien su gestión está subcontratada a un tercero (normalmente a través de alojamiento de servidores). Una de las características que hace atractivo este tipo de nube para una organización es el grado de control y de privacidad de los datos, ya que los recursos se encuentran bajo el estricto control de la propia organización (no nos referimos al grado de seguridad pues la seguridad depende de varios factores).

Una "nube pública", por el contrario, es una infraestructura propiedad de un proveedor especializado en la prestación de servicios de nube que pone a disposición (y, por consiguiente, comparte) sus sistemas con los usuarios u organizaciones que contratan sus

servicios. Se accede al servicio a través de internet, lo que implica la transferencia de actividades de tratamiento de datos a los sistemas del proveedor de servicios. Desde el punto de vista de la protección de datos personales, la consecuencia más destacable del uso de este tipo de nube es que el responsable del tratamiento está obligado a transferir una parte importante del control que ejerce sobre dichos datos y el proveedor de servicios desempeña un papel clave en lo que refiere a la protección eficaz de los datos personales almacenados en sus sistemas.

Por último, además de las nubes "públicas" y "privadas" encontramos "nubes híbridas", donde el usuario es propietario de parte de la infraestructura y combina esta modalidad con servicios adquiridos en nubes públicas.

Como mencionamos anteriormente, entendemos que las soluciones tecnológicas no son neutras y, si analizamos la estructura de cada modelo, encontramos una tensión importante entre las soluciones orientadas a optimizar costes (perdiendo el control sobre la infraestructura y los datos) y las soluciones orientadas a garantizar los derechos de los usuarios. Lamentablemente, para muchas instituciones no es viable o sostenible a largo plazo el uso de una nube privada, principalmente por razón de costes. Consideramos que, al Estado, a través de las Unidad Reguladora y de Control de Datos Personales (URCDP)[132], le corresponde apoyar a las instituciones educativas (IE) al momento de tomar este tipo de decisiones y proporcionar elementos para evaluar opciones.

132. Acceda al sitio: https://www.datospersonales.gub.uy/

Las grandes corporaciones de la información y los servicios educativos en la nube

El campo de las tecnologías educativas parece estar reclamando en la actualidad la denominación de "industria" por derecho propio. Se habla de un mercado potencialmente gigantesco que no es tan solo un subsector dentro de la industria del *software*. Según el informe de EdTechXGlobal[133], aunque se calcula que solamente el 2% de la educación está digitalizada, el mercado actual estaría creciendo a una tasa de 17% anual y alcanzaría el valor de 252 mil millones de dólares en 2020. Cifras millonarias similares a estas se repiten en los medios especializados de este sector, con considerables variaciones en su magnitud, pero siempre desde una narrativa que pone énfasis en el potencial de este codiciado mercado educativo.

Dentro de esta industria destacan algunas compañías nacidas como *empresas emergentes* educativas, como Udacity, Coursera, Edmodo y otras, valoradas en millones de dólares. El sector también comprende tecnologías y proyectos libres con modelos de negocio abiertos, como Moodle, de amplio uso para la gestión de aulas virtuales. Sin embargo, también están desarrollando sus negocios en esta área grandes corporaciones: Google, Apple, Amazon, Microsoft y Facebook, que desarrollan productos con sus marcas o adquieren y financian empresas emergentes.

Una y otra vez, en informes y análisis de consultoras, se repite que estas corporaciones aprovecharán "sus potentes plataformas", "su ecosistema", "su enorme base de usuarios" para imponerse en el ámbito educativo. No siempre se comenta que también se basan en una importante capacidad de *lobby* para ganarse grandes clientes

133. Más información: http://edtechxeurope.com/

institucionales, tanto de la educación pública como privada (Singer, 2017).[134] Además, en muchas ocasiones las ofertas de productos de tecnologías educativas por parte de las corporaciones vienen acompañadas de una narrativa filantrópica. Los vínculos comerciales entre ellas y los gobiernos se inician muchas veces como acciones de cooperación para mejorar la educación y brindar acceso universal a herramientas e incluso conectividad a poblaciones con carencias. Como antecedentes podemos nombrar la estrategia de la compañía Google que provee la Suite Google Apps for Education de forma gratuita al sistema educativo público de varios países en desarrollo (Islands in the cloud, s. f.; Magdirila, 2013; Koetsier, s. f.; Patodiazgnu, 2015).

La preocupación por la privacidad y la protección de datos en educación ha surgido como debate público a partir de la irrupción de estas grandes corporaciones en educación. Estas preocupaciones, expresadas por distinto tipo de actores, se ven reflejadas en informes gubernamentales, como el realizado por la Agencia Española de Protección de Datos Personales, o en análisis críticos desarrollados por organizaciones no gubernamentales, como las preguntas frecuentes acerca de servicios educativos en la nube y dispositivos en las escuelas de la Electronic Frontier Foundation (2015) o las campañas activistas de la Parent Coalition for Student Privacy (2017) en Estados Unidos. En Uruguay este debate surgió por primera vez en la opinión pública a raíz de un acuerdo entre el Plan Ceibal y Google por el cual el primero accedía gratuitamente a los servicios de Google Apps For Education (Patodiazgnu, 2015).

---

134. En un informe de la periodista de tecnologías Natasha Singer, publicado en el *New York Times* el 13 de mayo de 2017, se explican detalladamente estas prácticas de *lobby* a distintos niveles, desde los docentes hasta las autoridades educativas locales y estatales en EE. UU.

Estos debates ponen de relieve que, aunque los servicios educativos en la nube tienen grandes ventajas, también son notables sus riesgos desde la perspectiva de la protección de datos, exponiendo a los estudiantes a niveles de vigilancia difíciles de percibir y controlar.

Principales riesgos relacionados con la contratación de servicios en la nube

Las tecnologías educativas que se utilizan en las escuelas y universidades comprenden un amplio espectro de herramientas: desde dispositivos hasta aplicaciones, pasando por servicios de nube. Estos servicios pueden consistir en campus y aulas virtuales, de carácter específicamente educativo, así como en servicios de redes sociales, *webmail* y almacenamiento en la nube. Las grandes corporaciones de internet, como expusimos previamente, están fuertemente implicadas en este mercado, a través de servicios de nube como Google Apps For Education o Microsoft in Education.

Como vimos, hay diversos modelos de implementación de estos servicios, que pueden ser provistos por la IE o subcontratados. Si bien en ambos casos, los servicios tienen que respetar la legislación vigente en materia de protección de datos, la subcontratación a terceros implica riesgos que hay que tener en cuenta especialmente. El Grupo de Trabajo sobre Protección de Datos del Artículo 29[135] (en adelante GT 29-UE) detecta dos riesgos principales que habrá que evaluar de acuerdo al volumen de datos personales que se maneje, los usuarios alcanzados y el tipo de institución contratante de servicios de nube, estos son:

135. El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, reúne a todas las autoridades de Protección de Datos de los países de la UE.

1) Pérdida de control. Esta puede expresarse de la siguiente manera: a) falta de disponibilidad (dependencia respecto del proveedor); b) falta de integridad (causada por la puesta en común de los recursos en la nube); c) falta de confidencialidad; d) falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación; e) falta de posibilidad de intervención; f) falta de poder de negociación de las cláusulas contractuales (ya que las ofertas normalizadas son una característica de los servicios de computación en la nube).
2) Falta de información sobre el tratamiento (transparencia). La ley obliga a que los interesados cuyos datos personales sean objeto de tratamiento en la nube sean informados acerca de la identidad del responsable del tratamiento y de los fines del tratamiento. La principal consecuencia de la falta de transparencia es que la IE que contrata el servicio en la nube, muchas veces no es consciente de las amenazas y riesgos potenciales y, por tanto, no podrá adoptar las medidas de protección apropiadas. Los datos personales de los usuarios se encuentran en riesgo si la IE, por ejemplo, no conoce:
    - la composición de la cadena de los múltiples encargados del tratamiento y los subcontratistas;
    - si se transmiten datos personales a terceros países que pueden no proporcionar un nivel adecuado de protección de datos;
    - si las transferencias no cuentan con las medidas de protección adecuada.

Pero las IE, los estudiantes, los padres y los docentes encaran un problema mayor que el del control de proveedores de servicios educativos basados en la nube. Se trata de la falta de adecuación de los actuales sistemas de protección de datos personales al tratamiento masivo de datos en el ámbito educativo o al Big Data en educación.

Har Carmel (2016) resume los principales problemas que enfrentan los actuales sistemas de protección de datos:

> La reidentificación: el sistema no protege los datos de estudiantes de la reidentificación. Si definimos datos personales como datos que identifican o hacen identificable a una persona, basta con anonimizar esos datos para que la ley deje de ser aplicable. El problema aquí es que resulta bastante cuestionable la anonimización cuando hablamos de Big Data debido a que las técnicas de agregación, derivación contextual y correlación cruzada de grandes volúmenes de información hacen que el riesgo de reidentificación sea muy grande.

Para Solove (2013):

> La imposibilidad del real consentimiento informado (*opt-in*): el principio rector de estos sistemas de protección de datos es el principio del previo consentimiento informado. Aunque excluyamos la posibilidad de ambigüedad en la información proporcionada a los usuarios (o los adultos a cargo en caso de ser menores) por parte de empresas proveedoras de servicios, difícilmente podremos hablar de consentimiento informado frente a la actual capacidad de usos secundarios basados en minería de datos, inclusive cuando se utilizan con fines de mejora en los procesos educativos. Será simplemente demasiado complicado para un estudiante o una madre o padre promedio hacer elecciones conscientes frente al uso inesperado de los datos.

La imposibilidad de negarse a dar el consentimiento (*opt-out*): por último, Har Carmel (2016) plantea la imposibilidad de madres y padres de negarse (*opt-out*) a brindar su consentimiento, debido a las consecuencias que deberá afrontar si deciden no acompañar la decisión de la IE en cuanto a la selección de proveedores y a la política de privacidad de estos proveedores, ya que no todas las familias tienen la posibilidad de cambiar de IE a sus hijos.

Podemos concluir que estamos frente a un cambio de paradigma y que, sin lugar a dudas, nos enfrentamos a la necesidad de superar el enfoque de autogestión. Solove (2013) y Har Carmel (2016) plantean la reevaluación del equilibrio de intereses entre sujetos de datos y usuarios de datos mediante un enfoque que considera la privacidad y la protección de datos personales como un nuevo interés colectivo que requeriría una nueva combinación de regulación pública y gestión privada para aumentar el nivel real de protección de la privacidad de los estudiantes.

Recomendaciones para la contratación de servicios en la nube para educación

Las IE, como responsables del tratamiento de los datos de estudiantes y docentes, deben cerciorarse de que sus datos personales sean tratados conforme a la Ley 18.331 de Protección de Datos Personales (LPDP, 2008).[136] Esto implica que tienen la responsabilidad de garantizar que su proveedor de servicio en la nube cumple con la LPDP (principio de responsabilidad, artículo 12). Será fundamen-

136. Nuestra LPDP considera como dato personal a cualquier tipo de información referida a una persona que la pueda identificar directamente o indirectamente (como nuestro nombre, dirección, teléfono, cédula de identidad, RUT, huella digital, etc.) y regula de forma particular aquellos datos considerados sensibles (artículo 18).

tal entonces que presten especial atención a las características de los contratos y a las cláusulas relativas al procesamiento de datos. A continuación, planteamos las recomendaciones para la contratación de servicios en la nube en educación:

Necesidad de evaluar impacto en privacidad. Antes de contratar las IE deberían efectuar una evaluación de conveniencia e impacto. Para ello cuentan con el mecanismo de consulta que ofrece la URCDP de AGESIC, siendo recomendable la solicitud de asesoramiento previo a la contratación de servicios en la nube.

Contratos con garantías. Los centros educativos deberán formalizar la contratación de servicios en la nube de forma que puedan acreditar su celebración y la incorporación de las garantías adecuadas para la protección de datos personales, incluidas las exigibles en caso de subcontratación. Asimismo, el prestador de servicios en la nube debe garantizar la portabilidad de la información y la no conservación de los datos al término del contrato (borrado seguro).

Ubicación de los datos y subprocesadores. Es necesario que los centros educativos conozcan las entidades que intervienen en la prestación de servicios en la nube, su ubicación y las garantías adoptadas en caso de que vayan a realizarse transferencias internacionales de datos.

Posibilidad de auditoría. Es preciso que en el contrato se establezca el método o, al menos, la posibilidad de que el centro educativo realice auditorías. El responsable del tratamiento debe mantener el control sobre los datos.

Responsabilidades en materia de seguridad. Es preciso especificar claramente las responsabilidades de todos los intervinientes (IE, servicios de alojamiento y plataformas educativas) en la implantación de las medidas de seguridad. En particular, hay que asegurar la

adecuada asignación de permisos de acceso a los datos personales y concienciar a los usuarios sobre los peligros de utilizar contraseñas que no sean suficientemente robustas.

Referencias

Electronic Frontier Foundation (2015). FAQ About Cloud Education Services and Devices in Schools. *Electronic Frontier Foundation.* Recuperado de: https://www.eff.org/issues/student-privacy/faq

Har, Y. (2016). Regulating "Big Data Education" in Europe: Lessons Learned from the US. Browser. *Internet Policy Review. Journal on internet regulation* 5(1). DOI: 10.14763/2016.1.402.

Koetsier, J. (2013). Google: 10 million Malaysian students, teachers, and parents will now use Google Apps for Education. *Venture Beat*. Recuperado de https://venturebeat.com/2013/04/10/google-10-million-malaysian-students-teachers-and-parents-will-now-use-google-apps-for-education/

Laguda, R. (2012). Islands in the cloud: Philippines' Department of Education goes Google. *Google Cloud Official Blog.* Recuperado de https://cloud.googleblog.com/2012/09/islands-in-cloud-philippines-department.html

Magdirila, P. (2013). Are Google Apps the New Way to Learn in Philippine Universities? *Techinasia*. Recuperado de: https://www.techinasia.com/google-apps-learn-philippine-universities

Mell, P.; Grance, T. *et al.* (2011). The NIST definition of cloud computing. Recuperado de: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Parent Coalition for Student Privacy (2017). Parent Toolkit for Student Privacy. *Parent coalition for student privacy*. Recuperado de: https://www.studentprivacymatters.org/toolkit/

Parlamento de la República Oriental del Uruguay (2008). Protección de Datos Personales y acción de Habeas Data, Pub. L. N.º Ley 18.331. IMPO. https://www.impo.com.uy/bases/leyes/18331-2008

Patodiazgnu (2015). Sobre el acuerdo Google-ANEP-Ceibal y sus diferentes dimensiones. *Protección de datos para la educación en Uruguay.* Recuperado de: https://nogoogleappsedenuy.wordpress.com/2015/07/30/mas-sobre-el-acuerdo-google-anep-ceibal/

PR Newswire (2016). Global Report Predicts EdTech Spend to Reach $252bn by 2020. *CISIÓN PR Newswire*. Recuperado de: http://www.prnewswire.com/news-releases/global-report-predicts-edtech-spend-to-reach-252bn-by-2020-580765301.html

Presidencia de la República (2015). Ceibal suma herramientas de Google para potenciar el trabajo de docentes y estudiantes. *Presidencia de la República*. Recuperado de: https://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/ceibal-suma-herramientas-google-potenciar-trabajo-docentes-estudiantes

Singer, N. (2017). How Google Took Over the Classroom. *The New York Times.* https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html

Solove, D. (2013). Autogestión de la privacidad y el dilema del consentimiento. *Revista Chilena de Derecho y Tecnología*, 2(2). https://doi.org/10.5354/0719-2584.2013.30308

URCDP (2017). Unidad Reguladora y de Control de Datos Personales. Recuperado de: https://www.datospersonales.gub.uy/

Percepciones sobre privacidad entre los adolescentes brasileños: Desafíos y contradicciones

Monica Barbovschi
moni.barbovski@gmail.com
Institute of Sociology, Romanian Academy

Tatiana Jereissati
tatiana@nic.br

Javiera Macaya
javiera@nic.br

Stefania Lapolla Cantoni
stefania@nic.br
Núcleo de Informação e Coordenação do Ponto, Brasil

Palabras clave:
jóvenes - privacidad - Brasil

Introducción

La privacidad en la comunicación en línea ha sido relacionada con tareas de desarrollo en la adolescencia, es decir, la tarea de crear vínculos significativos con otros; la función de establecer una comunicación limitada y protegida a través de espacios mutuos de divulgación voluntaria vinculados a la tarea de desarrollo de la cons-

trucción de relaciones íntimas (Peter y Valkenburg, 2011; Westin, 1967).

El proceso de divulgación y presentación en línea del "sí" es condicionado por restricciones que pueden ser entendidas a través de las lentes de la teoría de la gestión de la comunicación de la privacidad (Petronio, 2002, 2010). Tal teoría discutió la gestión de la información privada tomando en cuenta tres elementos: apropiación, control y turbulencia de la privacidad, relacionados con la forma cómo las personas gerencian el acceso y la protección de sus informaciones (Petronio, 2010). Como un proceso dinámico, dialéctico (Walrave *et al.*, 2016), la gestión de la privacidad puede ser vista como un acto de equilibrio entre apertura y cierre para grupos, personas o situaciones de contextos específicos (Archer *et al.*, 2015). Este proceso, sin embargo, es deteriorado por riesgos relacionados con la privacidad, exposición no deseada y uso indebido de datos personales.

No obstante, los riesgos recientemente emergentes relacionados con el mal uso de los datos personales de adolescentes, en el contexto de las redes sociales (por ejemplo, pirateando perfiles, compartiendo información o etiquetando a pares sin permiso, compartiendo fotos de desnudos sin permiso, etc.) (Barbovschi y Velicu, 2014; Haddon y Vincent, 2014) están vinculados con el contexto más amplio relacionado con las percepciones y prácticas de los jóvenes en torno a la privacidad.

Este artículo lo diseñamos con base en datos cualitativos para explorar cómo jóvenes entre 11 y 17 años piensan la privacidad, cómo negocian y personalizan la información que comparten en línea dependiendo de la plataforma y de las audiencias pretendidas, y cómo navegan por las cuestiones de confianza (por ejemplo, en

casos de intercambiar las contraseñas con pares). También reflexionamos sobre diferencias de género percibidas en relación con la privacidad en línea, así como con los riesgos relacionados. Para esto, nos basamos en los datos de un estudio cualitativo conducido por el Centro Regional de Estudios para el Desarrollo de la Sociedad de la Información (Cetic.br), realizado a partir de 12 grupos focales con jóvenes de edades entre 11-12, 13-14 y 15-17 años, en la región metropolitana de São Paulo (Brasil), en setiembre de 2016. Los criterios de selección de las muestras incluyeron el sexo de los respondientes, la clase social, la composición étnica-racial y el tipo de escuela (pública o privada).

Resultados

Aunque de difícil definición, entre los jóvenes entrevistados existe una percepción generalizada de la privacidad como algo extremadamente personal, del foro íntimo y particular, o incluso secreto –asociada comúnmente al espacio físico del cuarto de baño. También es lugar común entre niños, niñas y adolescentes definir a la privacidad por su falta, esto es, por situaciones que representan ausencia de privacidad. En este sentido, algunos jóvenes definen privacidad en oposición a la idea de intromisión o de persecución –a veces indicada como práctica ejercida por los padres o responsables– siempre relacionada con la falta de consentimiento, una violación a esa intimidad que para ellos significa la privacidad.

> Mi papá siempre toma mi celular, y un día lo encontré leyendo mis conversaciones y me enojé mucho porque si él me pregunta qué pasa, yo le voy a contar. Él me lo saca de mi mano, ni siquiera me deja bloquearlo (13-14, niñas, escuela privada).

Si bien los jóvenes tienen dificultad para reconocer las fronteras entre el mundo en línea y fuera de línea y con ello las diferencias entre privacidad dentro y fuera de internet –que para algunos sería idéntica– esa percepción es luego relativizada al ser señalado que en el ambiente virtual se presentan más limitaciones a la privacidad, pues las comunicaciones y contenidos dejan registros que pueden fácilmente ser capturados y esparcidos en la red como un todo, como los *prints* de conversaciones, por ejemplo. Así, si para algunos internet aparece como un espacio que permite mayor libertad para decir lo que se piensa, esa libertad viene amarrada a un registro inextinguible. Otro argumento en torno a la idea de ausencia de privacidad en el mundo en línea deriva del uso de las redes sociales, pues hay una asociación implícita entre "estar en la red social" y exponerse, es decir, una exposición en las redes sociales al compartir informaciones, fotos y contenidos. Para algunos adolescentes esa exposición es incentivada por la propia plataforma:

> [La privacidad en internet] no existe (13-14, adolescentes varones, escuela privada).

> Las propias redes sociales [...] ellas ven que las personas se exponen y se ponen a dar más oportunidades para que se expongan. El Face hace mucho eso. Parece que ellos van dando cuerda para que las personas se ahorquen (15-17, adolescentes mujeres, escuela privada).

Sobre todo, entre los adolescentes de 15 a 17 años, hay una percepción de que la privacidad también es más frágil en el ambiente en línea debido a que los contenidos, conversaciones e informaciones intercambiados están vinculados a plataformas privadas que pueden comercializar tales datos; es decir, existe una preocupación sobre la violación de esa privacidad en el mundo en línea por parte de los *dueños* de las redes sociales.

> Estoy hablando con una chica en WhatsApp, no estamos solamente nosotros en la conversación, creo que esas informaciones también son vendidas (15-17, adolescentes varones, escuela pública).

> [Yo me preocupo] sobre postear fotos mías, en cualquier red social, porque nosotros decimos que es privado, pero de algún modo no lo es, porque cualquiera, uno que tenga Facebook, si googlean tu nombre, todos tus registros aparecen (15-17, adolescentes varones, escuela privada).

Si por un lado muchos jóvenes expresan que puede haber ausencia de privacidad tanto por el accionar de padres, responsables e incluso pares, así como por las propias redes sociales, los niños, niñas y adolescentes hacen una gestión de las plataformas que utilizan de acuerdo con el contenido que quieren publicar, teniendo en cuenta cuáles son las personas que están presentes en cada una de las plataformas. Esto quiere decir que los jóvenes hacen uso de varias plataformas considerando cuáles son sus características, condiciones, funcionalidades –por ejemplo, si les permite publicar una foto por tiempo predeterminado (por ejemplo, Snapchat) o no. Junto con la de plataformas, los jóvenes realizan la gestión de sus *redes*, identificando qué contenidos pueden publicar considerando quiénes forman parte de su red de amigos en determinada plataforma. Esta gestión es intensificada cuando toman en cuenta la presencia o no de sus padres y/o familiares en las plataformas, llevándolos a no postear contenidos específicos o a bloquearlos cuando publican tales contenidos.

> Yo voy a postear alguna cosa, ahí bloqueo a toda la familia. Tipo, amigos excepto familia [...] porque si no van a decir "qué ropa es esa con la que saliste de casa ayer (15-17, adolescentes mujeres, escuela privada).

> Si posteo video fumando narguile, a mi mamá no le gusta, pero mi papá es más tranquilo. Por eso yo posteo más en el Snap, ya que no tengo a mi mamá en el Snapchat (15-17, adolescentes varones, escuela privada).

Entre los jóvenes, gran parte relató ya haber compartido sus contraseñas con sus padres, sobre todo entre los más chicos, para verificación del contenido de las redes sociales.

> [...] es regla de la casa. Mi [mamá] entra de vez en cuando para ver si no estoy haciendo nada errado (11-12, adolescentes varones, escuela pública).

Muchas veces, el hecho de compartir la contraseña es visto como una importante prueba de confianza y transparencia, y señal de que no hay nada a ser escondido:

> [Compartir] la contraseña de mi celular está bien, porque yo no tengo nada que esconder. Pero mis redes sociales son más privadas (15-17, adolescentes varones, escuela privada).

Esta práctica también es bastante común entre parejas que intercambian sus contraseñas, no siempre de manera voluntaria. Sin embargo, sabiendo que otros tendrán acceso a sus conversaciones y contenidos, sean sus padres o parejas, muchos relataron borrarlas.

> Él [exnovio] medio que me obligó. Yo ya borraba todas las conversaciones del día (13-14, adolescentes varones, escuela privada).

La preocupación sobre las consecuencias en torno de la violación de la privacidad para adolescentes varones y adolescentes mujeres es percibida de manera distinta: entre los adolescentes varones, hay un recelo en que alguien invada su perfil y coloque en duda su

heterosexualidad mientras que, para las mujeres, hay preocupación con su seguridad física.

> Porque es peligroso. Supe de una chica que dejó un celular en tal lugar de la escuela, se lo robaron y descubrieron su dirección y asaltaron la casa de la chica. Y hay también tipos que van y secuestran niñas; hay pedofilia también, es peligroso, y yo no veo que eso pase con los chicos. Pasa, pero es muy poco. Lamentablemente las chicas tienen que preocuparse más, los chicos corren menos riesgos (11-12, adolescentes mujeres, escuela pública).

Otra gran preocupación entre ellas es la divulgación no consentida de sus fotos íntimas, semidesnudas y/o desnudas, denominadas *nudes*, generalmente enviadas a otra persona de confianza. En todos los grupos focales hubo relatos de experiencias de ese tipo y, de modo general, fotos de adolescentes mujeres son esparcidas sin consentimiento, con consecuencias negativas para ellas, relatos que van desde la salida de su escuela hasta intentos de suicidio. Las experiencias más recurrentes se refieren a la filtración de fotos por quienes las recibieron en confianza, generalmente (ex) parejas, amigos o amigas.

> En mi escuela hay una chica, ella mandó *nudes* para un chico, el chico la posteó, y ella se cambió de país; la mamá de ella quería matar al chico, ella quería matarse y casi se mató tirándose en la línea del tren (11-12, adolescentes mujeres, escuela pública).

> Mi amiga mandó un *nude*, para un chico que a ella le gustaba, y él no estaba ni ahí con ella. Ahí él mandó para todas las amigas de ella, y lo esparcieron por toda la escuela. Hasta los padres terminaron sabiendo, le sacaron el celular (13-14, adolescentes mujeres, escuela pública).

> Conozco a una niña que salió del otro colegio porque mandó un *nude* para un niño, el colegio entero lo vio y ella tuvo que salir del colegio (13-14, adolescentes mujeres, escuela privada).

Discusión y conclusiones

En nuestro estudio, los jóvenes comparten sus percepciones sobre la privacidad como algo importante y muchas veces definido por sus limitaciones, algo que se les es quitado; algo frágil, o incluso inexistente en línea. A respecto de las plataformas, los jóvenes hacen uso de características particulares de cada una de ellas y personalizan las configuraciones de privacidad de modo a gestionar las audiencias pretendidas (para seleccionar y excluir categorías específicas), según el contenido posteado. Por lo tanto, es perceptible que los jóvenes tienen cierta preocupación con cuestiones de privacidad y hacen uso de los propios mecanismos y herramientas que cada plataforma les ofrece para gestionarla.

Las amenazas a la privacidad fueron identificadas en forma de personas conocidas, generalmente padres/adultos que no respetan su intimidad, que se entrometen o forzosamente violan su privacidad (verifican sus conversaciones en sus teléfonos, por ejemplo), compañeros y/o parejas, que también violan la privacidad al acceder y esparcir contenidos su consentimiento; o entidades comerciales anónimas que recopilan y usan sus informaciones sin permiso. Hay un sentimiento generalizado que los jóvenes transmiten sobre la exposición inexorable y la pérdida de privacidad que viene como un precio por el uso de las redes sociales.

Además, nuestro estudio pone luz sobre diferencias de género en relación con la privacidad y las consecuencias de su violación, pues según reportaron los jóvenes, es más probable que las adoles-

centes sean objeto de comportamientos no consensuales de terceros, así como más propensas a que sufran consecuencias negativas.

Considerando los puntos brevemente abordados a lo largo del artículo, es relevante que nuevos estudios sean realizados en otros contextos geográficos e institucionales de modo a entender mejor este fenómeno, como también para ampliar y llevar el debate a otros actores e instituciones.

Referencias

Archer, K.; Christofides, E.; Nosko, A.; Wood, E. (2015). Exploring disclosure and privacy in a digital age: Risks and benefits. En: L. D. Rosen, N. A. Cheever, L. M. Carrier (Eds.), *The Wiley handbook of psychology, technology and society* (pp. 301-320). Wiley Blackwell.

Barbovschi, M.; Velicu, A. (2015). Fraped selves: hacked, tagged and shared without permission: challenges of identity development for young people on Facebook. En: Lorentz, P.; Metykova, M.; Smahel, D.; Wright, M. (eds.) *Living in the Digital Age: Self-Presentation, Networking, Playing, and Participation in Politics* (pp. 15-32). República Checa: Masaryk University Press.

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 8(1), article 9.

Haddon, L.; Vincent, J. (2014). European children's and their carers' understanding of use, risks and safety issues relating to convergent mobile media. *Report D4.1*. Milano: Unicatt.

Peter, J.; Valkenburg, P.M. (2011). Adolescents' online privacy: Toward a developmental perspective. En: S. Trepte, L. Reinecke (Eds.), *Privacy online: perspectives on privacy and self-disclosure in the social web* (pp. 221-233). London: Springer.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* Albany, NY: State University of New York Press.

Petronio, S. (2010). Communication privacy management theory: what do we know about family privacy regulation? *Journal of Family Theory and Review.* 2, 175-196.

Walrave, M.; Utz, S.; Schouten, A. P.; Heirman, W. (2016). Editorial: The state of online self-disclosure in an era of commodified privacy. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 10(1), article 1.

Derecho al olvido de niños, niñas y adolescentes en la era digital: Una visión desde México

Olivia Mendoza
olivia.mendoza@infotec.mx

Centro Público de Investigación e Innovación en Tecnologías de la Información y Comunicación, México

Palabras clave:
derecho de protección de datos personales - principio del interés superior del menor - derecho al olvido

Introducción

El vertiginoso desarrollo tecnológico y la gran oferta de servicios en internet nos hacen hablar de nuevos derechos configurados desde la economía digital, y un ejemplo de ello es el denominado derecho al olvido.

En este sentido, el uso masivo de internet ha propiciado que conceptos como el derecho al olvido tengan un especial auge y, con ello, se haga pertinente su estudio, particularmente cuando se trata de una oportunidad para que la información concerniente a niños, niñas y adolescentes, que vulnere su bienestar físico o psicológico, simplemente no sea pertinente o haya perdido su trascendencia, pueda ser eliminada del ciberespacio.[137]

137. El ejercicio del derecho al olvido nos lleva a la necesidad de ponderar los derechos humanos involucrados en un caso particular, ya que si bien el prin-

Resulta importante señalar que actualmente existe un debate en torno a la naturaleza jurídica de este derecho, ya que, para algunos doctrinarios, podría ser un derecho autónomo y, para otros, una manifestación del derecho de cancelación o del de oposición,[138] previstos en el derecho tradicional de protección de datos personales.[139]

Desde una perspectiva técnica, debemos señalar dos momentos de ejercicio del derecho al olvido: si la solicitud de eliminar determinada información se formula a la fuente original que generó la misma, hablamos del ejercicio del derecho al olvido.

No así, si la solicitud de ejercicio del derecho al olvido se formula ante un buscador en internet, ya que, en esta situación, estaríamos frente a un derecho de desindexación de la información.

En ninguno de los dos casos mencionados anteriormente se podrá garantizar un verdadero olvido, dado que cualquier usuario de internet puede descargar la información y compartirla con terceros.

En opinión de la autora, la concepción del derecho al olvido tiene su origen fundamental en el derecho de protección de datos personales –reconocido en diversas legislaciones de Iberoamérica– encuentra su pertinencia de análisis en la reciente postura de algunos

---

cipio del interés superior del menor, los tratados internacionales y la legislación nacional, nos llaman a cumplir con esta prerrogativa cuando se trata de datos de niños, niñas y adolescentes, no estamos ante la misma situación cuando existen solicitudes para eliminar, por ejemplo, información derivada de actos de corrupción o sustentada en el ejercicio profesional periodístico.

138. Podemos entender como derecho de cancelación de datos personales a la prerrogativa que tienen los titulares de datos para solicitar la cancelación de dichos datos de los archivos, registros, expedientes, sistemas electrónicos o plataformas digitales, a fin de que la información ya no esté en posesión de quien la tenía originalmente y dejen de ser tratados.

139. En el caso de México, se reconocen como parte del derecho de protección de datos personales los derechos de acceso, rectificación, cancelación y oposición, frente al tratamiento de datos personales.

tribunales y en la necesidad de incorporarlo bajo esa denominación a las normativas nacionales; sin embargo, algunas particularidades deben resaltarse cuando se configura el derecho al olvido respecto a datos personales de niños, niñas y adolescentes en el ámbito digital, puesto que su garantía resulta primordial, atendiendo a principios como el del interés superior del menor.

Consideraciones previas

Cuando hablamos de derecho al olvido, debemos recordar que esta figura tiene su origen en la sentencia T-414 del 16 de junio de 1992, dictada por la Corte Constitucional de la República de Colombia, así como su incorporación en legislaciones nacionales, como el caso del artículo 10 de la ley 787 de 2012 de la República de Nicaragua y el artículo 11 del decreto 37.554 de 2012 de la República de Costa Rica (Remolina, 2017, p. 199).

Por otro lado, si bien no se reconoce el derecho al olvido, el derecho a la desindexación tiene su origen en dos fuentes principales: el caso Google España de 2014,[140] resuelto por el Tribunal de Justicia de la Unión Europea (en el que se exigió al buscador eliminar determinados resultados de información) y recientemente en el Reglamento General de Protección de Datos de la Unión Europea (derecho de supresión).

A partir de ese momento, el tema cobró importancia en los espacios de opinión y en los poderes legislativos de algunos países de Latinoamérica, como en el caso de México, en donde, a partir de la discusión surgida en Europa, se analizó la necesidad de incluir el

140. El derecho al olvido adoptado por el TJUE, refiere al derecho a ser removido de determinados motores de búsqueda, sin que haya una referencia si este derecho alcanza una extensión a las fuentes originales en las que se encuentra la información.

derecho al olvido de manera expresa en los ordenamientos jurídicos en materia de protección de datos personales.[141] Motivado, entre otras cosas, por la necesidad de lograr niveles óptimos de protección de la información, requisito deseable, para realizar transferencias de datos o establecer relaciones comerciales.

El derecho al olvido está relacionado directamente con la concepción del derecho de protección de datos personales que se tiene desde los países que integran la familia jurídica romano-germánica, por lo que la dimensión del derecho al olvido será distinta en lo que respecta a los países que conforman la familia jurídica del *common law*, porque para ellos la protección de datos no es un derecho humano o fundamental, sino un derecho del consumidor, regulado sectorialmente. Se debe considerar que la mayoría de buscadores en internet tienen su origen en países de esta última tradición jurídica.

Por otro lado, el primer antecedente del derecho al olvido en México (interpretado como un derecho de desindexación), se encuentra en la postura del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) respecto a una solicitud de protección de derechos –particularmente el de cancelación–, formulada por un empresario mexicano, quien primero solicitó a Google la eliminación de varios resultados de búsqueda relacionados con su nombre –argumentando que la información afectaba su esfera más íntima y también sus relaciones financieras actuales, ya que uno de esos enlaces direccionaba al reportaje periodístico "Fraude en Estrella Blanca alcanza a Vamos

141. Del análisis a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se desprende que el objetivo del derecho al olvido se encuentra previsto, a través del derecho que tienen los titulares de datos personales, de solicitar la cancelación de datos personales o, en su caso, del poder de oponerse al tratamiento de la información.

México", publicado en 2007 por la revista *Fortuna*–. En esta nota, el empresario es mencionado como uno de los implicados en presuntos actos de corrupción.

En este sentido, la legislación mexicana en materia de datos personales en el sector privado establece que en caso de que la solicitud de derecho de cancelación no sea atendida por el particular (Google), el titular del dato podrá acudir a través de la denominada solicitud de protección de derechos ante el órgano garante, a fin de iniciar una investigación y de ser el caso, iniciar un procedimiento sancionatorio contra el particular.

En este caso planteado, el INAI sancionó a Google por no atender la solicitud de cancelación del dato, sin contar que la fuente original –la revista *Fortuna*– se ampararía, ya que no fue escuchada dentro del procedimiento.

Hoy día en el país se discute cuáles son los límites del derecho al olvido frente a derechos como la libertad de expresión, el derecho de acceso a la información o el derecho a la verdad, porque no resulta lo mismo solicitar eliminar información que es de interés de la colectividad y que refiere a un servidor público que la solicitud de borrar información que atenta contra la dignidad humana, siendo posiblemente relacionada a una persona que no es figura pública, o a información concerniente a niños, niñas y adolescentes.

En este mismo sentido, surge el debate de los límites de la libertad de expresión y el grado de exposición de personas públicas, en los cuales no existe cabida a preguntarnos si los datos de niños, niñas y adolescentes deberían ser borrados o no, atendiendo al mandato del principio del interés superior del menor, por lo cual se desarrollarán los siguientes elementos de análisis.

Derecho al olvido de niños, niñas y adolescentes en México

Cuando hablamos del derecho al olvido, encontramos fuertes críticas relacionadas con el atentado que el ejercicio de este derecho constituye a derechos como el acceso a la información, la libertad de expresión o a la verdad; sin embargo, estas críticas se matizan cuando estamos ante la necesaria urgencia de eliminar información relativa a niños, niñas y adolescentes que propicie, por ejemplo, revictimización, discriminación, acoso o vulneración a su esfera de bienestar.

Desde el punto de vista de la autora, este es uno de los casos excepcionales en donde el derecho al olvido no encuentra lugar a discusión, ya que su garantía protege desde una concepción amplia los derechos de los niños, niñas y adolescentes.

En este sentido, podríamos hablar de la necesaria inclusión de aspectos éticos en la difusión de información por parte de las fuentes periodísticas, puesto que la Declaración Universal de Derechos Humanos y la Convención sobre los Derechos de los Niños dictan las obligaciones de salvaguardar la dignidad de las personas, garantizar la no injerencia en la vida privada de las mismas, y la responsabilidad de los Estados de velar por la recuperación física y psíquica de niños, niñas y adolescentes y garantizar una reinserción social.

Derivado de lo anterior, de una ponderación de derechos –libertad de expresión, protección de datos personales y acceso a la información–, podríamos concluir que, en algunas noticias de interés público resulta necesario informar, pero no así exhibir, por ejemplo, la imagen o los datos personales que identifiquen a los niños, niñas y adolescentes. En este caso, la revictimización puede darse al ser un niño el que esté involucrado en un delito o que este haya sido la víctima del mismo.

Es importante decir que el marco legal mexicano contiene pocas disposiciones concretas relativas a los datos de niños, niñas y adolescentes; sin embargo, existe un marco de protección general en las siguientes legislaciones: Ley Federal de Protección de Datos Personales en Posesión de Particulares, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[142] y la Ley General de los Derechos de Niños, Niñas y Adolescentes[143].

Conclusiones

El entorno digital en el que los niños, niñas y adolescentes se desarrollan trae consigo muchos beneficios en su vida diaria, como el acceso infinito a la información, a materiales educativos y recreativos y la posibilidad de establecer diversas formas de comunicación; sin embargo, este entorno también supone riesgos, principalmente para los más jóvenes, por lo que es necesario hacer un uso responsable de las nuevas tecnologías y brindar educación, no solo en la utilización de la tecnología, sino en el empoderamiento a través de su uso, y las formas de hacerlo de manera segura.

Por otro lado, es importante destacar que el entorno digital tiene como materia prima la información de las personas, por lo que debe existir sentido de responsabilidad en lo que los niños, ni-

142. El derecho de cancelación en el sector público y en el privado puede ejercerse por el titular del dato personal o, en su caso, el tutor del niño.

143. De acuerdo al artículo 77 de este ordenamiento jurídico, se considerará violación a la intimidad de niñas, niños o adolescentes cualquier manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación que cuenten con concesión para prestar el servicio de radiodifusión y telecomunicaciones, así como medios impresos o en medios electrónicos de los que tenga control el concesionario o medio impreso del que se trate, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez.

ñas y adolescentes deciden compartir puesto que, atendiendo a las características de internet, una vez que la información se pone a disposición de terceros, es difícil tener un control sobre su uso, destino y fin.

No obstante lo anterior, figuras como derecho al olvido permiten borrar, cancelar, suprimir o, en su caso, desindexar información de los buscadores en internet, por lo que los niños, niñas y adolescentes pueden acudir a esta figura cuando exista información relativa a su persona que los ponga en una situación de vulnerabilidad; asimismo, existen mecanismos de protección y de responsabilidades civiles, penales o administrativas que pueden hacerse valer cuando se vulneran derechos propios o de terceros en el entorno digital.

La forma de actuar en el entorno digital debe permitir el empoderamiento a través del uso de las TIC, explotar sus máximos beneficios y configurar, a su vez, un espacio seguro para todos. Un ejemplo de ello es el uso de redes sociales con una configuración adecuada de privacidad, en las que los niños, niñas y adolescentes tengan el control de las personas que pueden acceder a su información.

Los niños, niñas y adolescentes como actores clave del entorno digital deben hacer un uso seguro y responsable de las nuevas tecnologías y no permitir acciones que supongan la vulneración de la dignidad de otros usuarios, tales como el ciberacoso, la discriminación, la publicación de fotografías, información de la vida privada y videos de otras personas sin su consentimiento, y la difusión de discursos de odio o difamación de terceros. Se destaca que el entorno digital no es un espacio sin normas, impune o sin responsabilidades, por lo que los sucesos en el entorno digital pueden traer consecuencias legales en el mundo físico.

En este sentido, el entorno digital será un espacio más seguro cuando padres de familia y educadores emprendan acciones preventivas y de educación, a fin de identificar los riesgos inherentes a la utilización de nuevas tecnologías, y se promueva la participación activa de los niños, niñas y adolescentes, considerando en todo momento el principio del interés superior del menor.

En conclusión, es tarea de todos los actores del entorno digital, particularmente de los padres de familia y de los educadores, enseñar a los niños, niñas y adolescentes a hacer un uso responsable y seguro del entorno digital a través de políticas educativas que incluyan estrategias de información y formación, a fin de determinar los beneficios y riesgos de su utilización, de comprender la importancia de la vida privada y de la protección de datos personales.

Referencias

Remolina, N. (2017). *¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas*. Argentina: Centro de Estudios en Libertad de Expresión y Acceso a la Información y Universidad de Palermo.

El libro *Jóvenes, transformación digital y nuevas formas de inclusión en América Latina* es un trabajo colaborativo escrito a muchas manos. Allí radica su riqueza. Ofrece un recorrido por las distintas visiones que múltiples actores de América Latina tienen sobre la inclusión digital. Integra experiencias, reflexiones y debates basados en investigaciones rigurosas que ilustran la diversidad cultural de esta región. Constituye un análisis actualizado que ayuda a comprender el impacto de la tecnología en los diversos procesos de inclusión (política, democrática, ciudadana, educativa, entre otras). En especial, en aquellos ámbitos donde niños, niñas, adolescentes y jóvenes de contextos vulnerables de América Latina son los protagonistas.

María José Ravalli
Especialista en Comunicación, UNICEF Argentina

El libro constituye una apuesta a la reflexión acerca de los procesos de transformación que observamos en nuestras sociedades a partir de la expansión de las tecnologías de la información y de la comunicación. Surge del trabajo colectivo de diversas instituciones que comparten distintos abordajes y miradas sobre nuestros niños y jóvenes en la era actual. La publicación se estructura en grandes áreas temáticas. Cada una de ellas permitirá al lector aproximarse a los múltiples contextos latinoamericanos en su relación con las distintas formas, tanto de exclusión como de inclusión. Aquí son las nuevas generaciones las protagonistas de las transformaciones actuales. Esta obra presenta más de 30 artículos entre los que se encuentran ensayos, investigaciones y experiencias de trabajo. Confiamos en que el libro constituirá un insumo relevante para el debate, tanto de investigadores, docentes, hacedores de políticas públicas, padres y como del público en general.

JÓVENES, INCLUSIÓN, IDENTIDADES, PRIVACIDAD, CULTURA *MAKER*, DERECHOS Y RESPONSABILIDADES, APRENDIZAJE Y TIC, PARTICIPACIÓN

FundaciónCeibal · DEBATE · FIC Facultad de Información y Comunicación · Universidad de la República Uruguay · GECTI · DIGITALLY CONNECTED · Universidad de Chile Instituto de la Comunicación e Imagen ICEI

ISBN: 978-9974-888-23-4