

Marzo
2021

Privacidad y datos personales: una mirada desde el periodismo

Del qué al por qué. Aportes de un periodista
para una construcción colectiva

Asociación por los Derechos Civiles



Con el apoyo de:



Marzo 2021

adc.org.ar

Redacción: Xavier Ibarreche

Diagramación: Matías Chamorro

Diseño de tapa: El Maizal



Este informe es de difusión pública y no tiene fines comerciales. Se publica bajo una licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0). Para ver una copia de la misma visite: creativecommons.org/licenses/by-nc-sa/4.0/deed.es

1. Introducción	4
2. La privacidad y la protección de datos personales en entornos digitales	6
El determinismo tecnológico	
La explotación de los datos personales	
Los datos personales, los algoritmos y ¿después?	
3. Periodistas y comunicadores frente a la privacidad y la protección de datos personales	16
Promoción de buenas prácticas en medios de comunicación	
Difusión de información sensible	
Protección de niñas, niños y adolescentes	
4. La privacidad y la protección de datos personales como interés público	23
5. Notas	24

1. Introducción

En la última década, las tensiones y conflictos entre sociedad, tecnología, privacidad y protección de datos personales han estado a la orden del día, cobrando mayor notoriedad en la agenda pública y, por lo tanto, en la agenda periodística. Se trata de un universo de temas que en menor o mayor medida afecta a prácticamente toda la población. Sólo hace falta echar un vistazo a la hemeroteca: desde escándalos vinculados con la filtración masiva de datos personales, pasando por la masificación de tecnologías de reconocimiento facial hasta el uso de aplicaciones de rastreo por el COVID-19. Al mismo tiempo, también se detecta una consistente publicación en medios de comunicación de información vinculada a protagonistas de las noticias que no están lo suficientemente resguardadas y que requiere especial atención.

Los datos personales, la biometría y los algoritmos forman parte de nuestros paisajes -físicos y digitales-. Aunque parezca exagerado, la desafortunada combinación de todos o algunos de estos elementos puede derivar en la pérdida de derechos fundamentales como la privacidad, la libertad de expresión, la libertad de reunión, el acceso a la salud o al trabajo.

Estamos ante un fenómeno de dimensiones globales que requiere domar algunos conceptos y clarificar ideas para explicar de la mejor manera posible de qué se tratan esas tensiones y conflictos. Sin embargo, el derecho a la privacidad y a la protección de los datos personales también pueden ser afectados en la práctica periodística si no se toman los recaudos necesarios.

La innovación constante de las tecnologías de la información y las comunicaciones (TIC) así como los desafíos que se presentan en la tarea cotidiana de los periodistas para informar sobre cuestiones en donde la privacidad y la protección de datos personales está presente exige a los profesionales -o en formación- de la

comunicación, adquirir y/o actualizar conocimientos. En ese contexto, en el horizonte de expectativas del oficio periodístico se encuentra la utilización ética de la información sin afectar a las personas, así como también el aporte de una mirada crítica sobre los usos de la tecnología.

El objetivo de este documento es ofrecer a periodistas y comunicadores algunas nociones básicas sobre qué es la privacidad y la protección de datos personales, aproximarse a los alcances políticos y económicos que conlleva para la democracia y la importancia de preservar los derechos de las personas a la hora de contar hechos de interés público.

En la primera parte de este documento se abordan los principales conceptos e impactos sociales vinculados con la privacidad y la protección de datos personales en entornos digitales. Se trata de uno de los debates globales más fervorosos en estos tiempos.

Luego se incluye una serie de recomendaciones prácticas para profesionales que deban comunicar historias en donde el uso de datos personales sea uno de los ejes de los hechos a informar sin pasar por alto los derechos de los protagonistas. Por último, se presenta una breve reflexión sobre el interés público que representa la privacidad y la protección de datos personales y los desafíos a los que se enfrentan los periodistas a la hora de comunicar hechos vinculados con este derecho.

Este trabajo es el primer paso de una iniciativa más amplia en la que se proyecta la redacción de una guía de buenas prácticas para periodistas sobre el derecho a la privacidad y la protección de los datos personales y un trabajo de investigación sobre los desafíos que plantea la masificación del uso de algoritmos en la toma de decisiones y sus impactos en la vida pública.

2. La privacidad y la protección de datos personales en entornos digitales

Según la Real Academia Española (RAE), la privacidad es una cualidad de lo privado; un ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Podríamos decir entonces que la privacidad es un principio ordenador de nuestra vida cotidiana, pero que no siempre es valorado como tal.

Comencemos derribando dos mitos vinculados con nuestra privacidad y más precisamente sobre la información generada por nuestras acciones. Cuántas veces habrán escuchado -o incluso pronunciado- frases como “si no tengo nada que ocultar no me importa que espíen” o “si ya tienen todos mis datos, qué me importa si saben algo más de lo que ya saben”.

¿Qué sucedería si las paredes de nuestra casa fueran de cristal? Alguien -o algo, una cámara de vigilancia o un dron, por ejemplo- podría observar desde la calle todo lo que hacemos en nuestro living, cocina o habitación sin ningún filtro que dificulte la visión hacia el interior de la vivienda. Con solo mirar a través de las paredes de cristal alguien -o algo- podría saber a qué hora nos despertamos, qué comemos, con quién nos juntamos, qué series miramos por las noches y, por supuesto, a qué hora nos vamos a dormir. Supone una gran cantidad de información sobre lo que hacemos a diario en manos de un tercero.

¿Cuántas casas conocen con paredes de cristal? ¿Por qué no construimos casas con paredes de cristal si no tenemos nada que ocultar? Pues la respuesta puede ser tan sencilla como demoledora: porque no nos comportamos de igual forma cuando sabemos que nos observan o nos vigilan.

La privacidad también modela nuestros comportamientos en entornos digitales. Debido a la revolución digital en la que estamos inmersos, el derecho a la privacidad también está estrechamente vinculado a nuestras acciones cuando visitamos páginas web y/o descargamos aplicaciones. ¿Tenemos idea de los permisos que otorgamos para acceder a información de nuestros aparatos de conectividad?

Cuando utilizamos los servicios de internet, la notebook, el celular, la tablet y cualquier otro aparato “inteligente” dejamos rastros digitales en el camino. Esa información se convierte en una huella digital que habla sobre nosotros: gustos, vínculos personales, los lugares a donde vamos a comer, los deseos de ir de viaje a algún sitio, etcétera.

Esa información que se recopila sobre nuestros gustos e interacciones es parte del motor que hace girar a las plataformas digitales. ¿Todos esos datos son tan relevantes para que sean recopilados por un tercero? ¿Sabemos a quién o a quiénes les estamos facilitando esa información? ¿Sabemos qué se hace con ella?

La privacidad es un derecho fundamental, consagrado en numerosos tratados internacionales, que en la Argentina tienen rango constitucional¹ y constituyen la base de cualquier sociedad democrática porque fortalece otros derechos consagrados como -por ejemplo- la libertad de expresión.

Si bien la Constitución Nacional no hace referencia a la privacidad en el sentido estricto, su artículo 18 menciona la inviolabilidad del domicilio y los papeles privados, mientras que el artículo 19 se refiere a las “acciones privadas”, siendo interpretado por la propia Corte Suprema como consagratorio del derecho a la intimidad o privacidad. Asimismo, en el artículo 43 de la Constitución se

consagra el derecho de los ciudadanos sobre los datos referidos a su persona, permitiendo “tomar conocimiento de los datos referidos y de su finalidad”.

Uno de los derechos asociados a la privacidad es la protección de los datos personales. Si bien en algunos casos ambos derechos pueden encontrarse relacionados, vale aclarar que existen distinciones conceptuales.

La privacidad se refiere a la protección de ámbitos no relacionados directamente con los datos personales, como el hogar, la autonomía individual o la vida familiar. La privacidad también es pensada como el deseo de una persona de evitar que algo que pertenece a su esfera íntima salga a la luz. Esto no es necesariamente el caso de la protección de datos personales, que ampara al ciudadano frente a ciertos usos que no pueden hacerse aún si la información fue aportada de manera voluntaria.

La protección de datos personales se vincula con el control que cada individuo debe tener sobre el uso que terceros pueden hacer con su información personal. El foco no está puesto solo en el carácter público o secreto del dato, sino que la utilización por parte de otras personas y entidades debe realizarse de modo que no afecte los derechos del titular del dato.

Por lo tanto, la protección de datos personales puede estar relacionada con violaciones al derecho a la educación, el derecho a la salud o el derecho a la vivienda, entre otros. En estos casos, la información personal puede ser mal utilizada para negar

injustamente una vacante escolar, impedir el acceso a un servicio de salud o calificar de manera negativa una postulación a un crédito hipotecario.

Actualmente, la protección de datos personales en Argentina es regulada por la Ley 25.326² –conocida como Ley de Protección de Datos Personales-, sancionada en el 2000 siguiendo estándares regulatorios internacionales de aquel entonces. La misma se aplica para el tratamiento de datos personales de parte de organismos públicos y de privados.

El determinismo tecnológico

Los principales debates globales sobre el derecho a la privacidad y el derecho a la protección de datos personales están centrados en las tensiones y conflictos que se generan alrededor de los entornos digitales. Al margen de las características propias de cada país en términos de privacidad, a nivel global somos miles de millones de personas empleando servicios provistos por compañías tecnológicas conocidas como las *big tech*, generando una gran cantidad de información al tiempo que cientos de organismos del Estado también recolectan datos sobre sus ciudadanos.

Esa información es utilizada por las empresas como principal insumo para desplegar su modelo de negocios, mientras que los Estados podrían utilizarla con fines maliciosos, más allá de las leyes de cada país y del efectivo cumplimiento de estas. Existe algo en común que facilita la recolección de información: la tecnología.

Habitualmente, la tecnología es presentada como la solución eficiente a problemas sociales en donde la desigualdad es moneda corriente. Aquellos que promueven este tipo de discursos fomentan lo que se conoce como solucionismo tecnológico o tecno-optimismo. Es decir, se piensa a la tecnología como un igualador de oportunidades sin detenerse en los contextos culturales, sociales y económicos que atraviesan a la sociedad.

En las últimas dos décadas, por ejemplo, internet evolucionó vorazmente y pasamos de utilizar un buscador que todo lo encuentra a un sinfín de aplicaciones para todo tipo de servicios: *delivery* de comida, mensajes a nuestros amigos y familiares; pagos con códigos QR, compras de todo tipo de productos, etcétera.

Desde una mirada ingenua, esa revolución digital supone una serie de consignas en donde la tecnología mejora a la sociedad *per se*, con promesas que van desde la ampliación del conocimiento hasta el mejoramiento de situaciones de desigualdades. Se trata de una cosmovisión para nada novedosa. A lo largo de la historia, el surgimiento de nuevas tecnologías estuvo acompañado por la idea de que la sociedad va a mejorar gracias a ellas.

Sin embargo, a lo largo de las últimas cinco décadas eso no ocurrió: la brecha entre ricos y pobres va en aumento,³ a pesar de las constantes innovaciones tecnológicas, una situación que se agravó con la pandemia derivada del COVID-19.⁴

Claro que esto no supone negar los beneficios, las potencialidades y los efectos virtuosos que tiene la revolución digital. ¿Acaso no resulta cómodo disponer de contenido audiovisual para mirar en el momento que deseamos en el lugar que queremos, encontrar esa ferretería que tiene el “coso del cosito” que estamos buscando para hacer un arreglo hogareño o enviar un meme viral al grupo de amigos o amigas? En definitiva, marcar los beneficios de la revolución digital no implica realizar un elogio acrítico del impacto de la tecnología en la vida cotidiana.

La explotación de los datos personales

Las empresas más valoradas del mundo como Facebook, Amazon, Apple, Netflix y Google –conocidas como las FAANG- junto a las

chinas Alibaba, TikTok y WeChat tienen algo en común: la enorme capacidad para procesar información. Los datos recopilados por sus plataformas se convierten así en la llave que hace girar la rueda de un modelo de negocios pensado y desarrollado para captar nuestra atención.

Esos datos son información en bruto que ha ocurrido en el pasado, pero gracias al procesamiento de esa información en el contexto en que sucedió se genera un conocimiento listo para convertirse en una oportunidad de negocios incluso sin que lo sepamos. Los rastros digitales se contextualizan y se convierten en una recomendación de una serie, una propuesta para financiar un viaje soñado o una cobertura de salud adaptada a nuestro ritmo de vida.

Ese modelo de negocios se basa en la extracción, recopilación, procesamiento y explotación de información vinculada a nuestras huellas digitales para ofrecer ese producto y/o servicio que deseamos sin saber que lo estábamos buscando. ¿Cómo se logra ese extraordinario y fenomenal “masajeo” de información? Gracias a técnicas de procesamiento de datos masivas vinculadas a tecnologías como la inteligencia artificial, la última joya de la llamada revolución digital.

El uso de grandes volúmenes de datos para la toma de decisiones por sistemas automatizados se extiende a prácticamente todas las ramas de la economía. Desde hace varios años, el sistema financiero, en el reclutamiento laboral, en los sistemas de salud -e incluso en cuestiones vinculadas a la seguridad ciudadana- se usan algoritmos que toman decisiones en base a la información masiva recopilada de diferentes fuentes.

La gran incógnita por develar, y que está en el centro del debate global, es cómo se procesan esos datos capturados de forma masiva. Es decir, cómo se genera el perfilamiento de millones de

personas en base a la gran cantidad de información recopilada. Lo que algunos académicos y expertos en tecnología denominan la “caja negra” de los algoritmos. No son pocos los que advierten que la poco transparente toma de decisiones automatizadas sin ningún tipo de control puede derivar en discriminación y exclusión.

Los datos personales, los algoritmos y ¿después?

El tratamiento masivo de información genera noticias que impactan en la agenda periodística. En la última década dos hechos vinculados con la (des)protección de datos personales marcaron la agenda periodística a nivel global.

Por un lado, las revelaciones de Edward Snowden en 2013, cuando expuso cómo la NSA -la agencia de seguridad de Estados Unidos- montó un amplio programa de espionaje⁵ sobre ciudadanos norteamericanos y extranjeros bajo el pretexto de la protección de la seguridad nacional.

Más acá en el tiempo, recordamos el escándalo derivado de Cambridge Analytica,⁶ el caso de una consultora política británica que utilizó información de usuarios de Facebook recopilada a través de un test de personalidad para modelar perfiles de posibles votantes en el Reino Unido y en otras partes del mundo. El objetivo de ese tipo de maniobras era influir en la decisión de votantes a través de campañas de desinformación.

Del otro lado del planeta los datos personales también son utilizados con una opacidad preocupante. En 2014, China puso en marcha un plan de crédito social que debía completarse en 2020. En la actualidad existe una docena de sistemas incompatibles entre sí, incumpliendo con reglas establecidas por el Gobierno, por lo que ya se planifica una reforma del programa.⁷

El sistema es impulsado por la inteligencia artificial de la mano de tecnología aportada por gigantes tecnológicos como Alibaba. Antecedentes penales, historia clínica y hasta costumbres de compras son evaluados por el sistema ideado por el Gobierno chino, implementando castigos si el sistema así lo considera. El abanico de causas para bajarle la puntuación social a la población va desde no pagar impuestos a cruzar un semáforo en rojo.

En la Argentina también tenemos ejemplos de la implementación de tecnología aún con el riesgo de facilitar la vigilancia masiva por parte del Estado. Tal es el caso del sistema de reconocimiento facial que se utiliza en las cámaras de vigilancia pública de la Ciudad de Buenos Aires con la excusa de hallar a quienes se encuentran fugados de la Justicia.

⁸El reconocimiento facial es un *software* montado sobre cámaras de vigilancia que detecta a una persona por sus datos biométricos, es decir, sus rasgos faciales. Se trata de una tecnología que se nutre de inteligencia artificial y que ya se implementó en varias ciudades del mundo, arrojando resultados errados debido a lo que se conoce como “sesgo algorítmico”.⁹ Uno de esos casos ocurrió en la Ciudad de Buenos Aires, cuando un hombre estuvo seis días preso porque el sistema de reconocimiento facial lo detectó como prófugo de la Justicia, pero no había cometido ningún delito.¹⁰ Sin embargo, no en todos lados el uso de tecnología de reconocimiento facial por parte de fuerzas de seguridad es tan bienvenida. En la ciudad de San Francisco (Estados Unidos), cuna de varias de las grandes empresas que dominan el mercado tecnológico, se prohibió el uso de esta tecnología para “combatir el delito” por parte de agencias públicas.¹¹

Los algoritmos no son objetivos, sino que reproducen los sesgos de las personas que los programan. En definitiva, quien programa los algoritmos alimenta al *software* para que haga foco en unos rasgos

sobre otros. Esta situación deriva en lo que se conoce también como falsos positivos, es decir, las veces que el algoritmo identifica a una persona como parte de su “lista negra”, pero la detecta como un hombre cuando era mujer, por ejemplo. Situación que no tardó en aparecer también en la Argentina cuando una mujer fue detenida por el sistema de reconocimiento facial por su “parecido” con una persona buscada por la Justicia.¹²

También existieron casos vinculados con el manejo de información vinculada a datos personales que tuvieron menor relevancia en la agenda periodística, pero no por ello fueron menos importantes ya que también afectaron, de alguna manera, el acceso a derechos básicos como la educación, a la información pública o al trabajo.

Una investigación realizada en 2020 detectó que Outlook -uno de los servicios de mailing gratuito más utilizados del mundo, propiedad de Microsoft- filtraba como *spam* (correo basura) mensajes que contenían las palabras “Nigeria”, “sexo” o “inversión”.¹³ Así, a un estudiante nigeriano se le bloqueó una solicitud de empleo, varios no se enteraron de un programa de educación sexual y miles de estudiantes estadounidenses se quedaron con las ganas de conocer las iniciativas del entonces candidato Joe Biden para alivianar sus deudas.

El acceso al trabajo también es uno de los derechos que se ve afectado por la automatización de decisiones mediante la explotación de datos personales. El más claro ejemplo es lo que sucede con las plataformas de *delivery*. En Italia, la Justicia determinó que Deliveroo, la app de entregas más utilizada en Europa, discrimina a los repartidores. El algoritmo clasificaba como menos confiables a quienes reportaban enfermedades. Según el fallo, si existe una discriminación involuntaria la empresa puede ser obligada a pagar por daños.¹⁴

En la misma sintonía, la Justicia de España ratificó que existe relación laboral entre los repartidores y las plataformas de delivery. Una sentencia contra Deliveroo en Barcelona consideró que la supuesta libertad del repartidor para ejercer su trabajo “no es tan amplia como se quiere aparentar”.¹⁵

Estos casos ejemplifican que la protección de datos personales forma parte de la agenda de interés público y por lo tanto es necesario abordar este tipo de temas desde el periodismo, investigando el funcionamiento de tecnologías digitales y alertando sobre los riesgos que conlleva su uso opaco a partir de la utilización de datos personales.

Por último, quienes deseen ampliar sus conocimientos sobre las tensiones y conflictos alrededor de la privacidad en entornos digitales recomendamos estas lecturas:

- *Privacidad amenazada*, de Helen Nissenbaum.¹⁶
- *Armas de destrucción matemática*, de Cathy O’Neil.¹⁷
- *Los dueños de internet*, de Natalia Zuazo.¹⁸
- *El enemigo conoce el sistema*, de Marta Peirano.¹⁹
- *La Locura del solucionismo tecnológico*, de Evgeny Morozov.²⁰
- *El filtro burbuja*, de Eli Pariser.²¹

3. Periodistas y comunicadores frente a la privacidad y la protección de datos personales

Aunque no lo parezca, la actividad periodística está estrechamente vinculada con la protección del derecho a la privacidad y la protección de datos personales. A menudo los periodistas y comunicadores publican información que es recomendable no difundir por el simple hecho de que puede perjudicar el control de las personas sobre sus datos personales, sobre todo en lo referido a información vinculada con la salud, menores de edad o víctimas de delitos.

Lejos de caer con la guillotina sobre los errores, este apartado tiene como objetivo brindar algunas menciones y recomendaciones útiles para periodistas y comunicadores vinculadas a la difusión de información personal para perfeccionar prácticas de un oficio cuyo objetivo es echar luz sobre los hechos de interés público.

Promoción de buenas prácticas en medios de comunicación

A menudo, en los medios de comunicación se difunde información personal vinculada con víctimas de delitos sin tener en cuenta que esa publicación podría afectar a quien ha sido vulnerado. Uno de los ejemplos más frecuentes es el tratamiento de información referida a mujeres víctimas de violencia de género. Si bien el deber del periodismo es darle visibilidad a este tipo de delitos con el objetivo de concientizar sobre la problemática, lo recomendable es no difundir información vinculada a las víctimas ya que por lo general no aportan a la prevención de la violencia de género, sino que pueden conducir a la revictimización.

Si la víctima cuenta con una abogada o abogado, lo ideal es ponerse en contacto con la persona que la representa para asesorarse

sobre qué información es conveniente difundir en público. En definitiva, se recomienda no publicar datos como el barrio en el que viven o el lugar en el que trabajan, por ejemplo, sin consultar a la fuente.

La información vinculada con personas acusadas de cometer un delito también debe ser tratada de forma rigurosa. La Justicia considera que es legítimo brindar información siempre y cuando se utilice el verbo en potencial al mencionar el delito o se mencione la fuente de quien realiza la acusación. Dicho esto, las buenas prácticas periodísticas sugieren no difundir los nombres de acusados que aún no hayan sido condenados en especial si se trata de delitos graves que pueden ser estigmatizantes, aunque después se demuestre su inocencia en la Justicia.

Sin embargo, cuando se trata de la difusión de información vinculada con funcionarios públicos, los periodistas tienen la potestad de publicar esa información amparados en el derecho a la libertad de expresión. Vale la pena repasar dos casos paradigmáticos.

En 1995, Carlos Menem demandó a la Editorial Perfil cuando la revista Noticias publicó que tenía un hijo extramatrimonial bajo el argumento de que se trataba de información privada que no tenía relación con sus funciones como presidente de la Nación. Si bien el entonces mandatario ganó el litigio en los tribunales locales, el caso llegó hasta la Corte Interamericana de Derechos Humanos (CIDH), tribunal internacional en el que se dirimen casos que afectan la libertad de expresión, que consideró que Noticias tenía derecho a publicar la noticia.²²

Por lo general, para la Justicia la ciudadanía tiene el derecho a conocer la vida privada de los políticos porque en cierta forma es información necesaria para poder controlarlos o evaluarlos

ya que los ciudadanos podrían considerar relevante saber cómo un candidato se comporta en su vida privada para decidir si lo vota o no.

También tenemos el caso excepcional en donde el derecho a la privacidad en figuras públicas prevalece por sobre la libertad de expresión. En 1981, la revista Gente publicó en tapa una foto del exdiputado Ricardo Balbín cuando estaba en terapia intensiva poco antes de fallecer. La viuda del líder radical demandó a la Editorial Atlántida. En 1984, la Justicia le dio la razón al considerar que la fotografía no tenía ningún valor desde el punto de vista de la libertad de expresión²³ y que por el contrario iba contra toda norma de respeto y decencia.

Difusión de información sensible

El COVID-19 supuso un cambio radical en la forma de relacionamiento social a nivel mundial. Tras ser declarada una pandemia global, las primeras semanas impusieron también un cambio radical en las rutinas laborales de toda la población, incluidos los periodistas y comunicadores, quienes se vieron ante un fenómeno de salud pública inédito para nuestra contemporaneidad.

Ninguno de nosotros cuenta con el manual de cómo actuar ante una pandemia global. Sin embargo, la detección del primer caso de Coronavirus en la Argentina puede servir de ejemplo para contextualizar el desafío al que se enfrentan los periodistas a la hora de narrar hechos noticiables sin vulnerar los derechos de los protagonistas.

Cuando las autoridades sanitarias dieron a conocer el primer contagio de COVID-19 en nuestro país, la inercia del oficio

periodístico llevó a varios medios a publicar información sobre quién había sido el primer argentino en contraer el virus y se montó una guardia periodística en la clínica privada donde estaba internado. Incluso se difundió en prime time televisivo un video del paciente en el momento en que era atendido por una enfermera. Durante la difusión de esas imágenes los periodistas no aclararon si las mismas habían sido cedidas por el paciente o si había dado su consentimiento para la publicación. Ante un caso de esta naturaleza se recomienda detallar de la mejor manera posible ante el público el origen de la información.

Vale mencionar que según la Ley 25.326, el tratamiento de información referida a la salud debe realizarse con especial cuidado, respetando la privacidad de las personas. Según el Artículo 2 de la norma, los datos de salud son considerados una categoría de datos sensibles y en consecuencia merecen una protección más rigurosa. Mientras que de acuerdo con el Artículo 7 ninguna persona puede ser obligada a proporcionar datos que se consideran sensibles. En tanto, el Artículo 5 de la ley exige que para la divulgación de los datos sensibles se requiere del consentimiento expreso e informado de la persona involucrada.

Por otro lado, el Código Civil y Comercial le dedica un capítulo a los derechos y actos personalísimos.²⁴ En el artículo 53 se refiere al derecho a la imagen y a la voz de las personas. La regla establece que se necesita el consentimiento de la persona para poder usar su imagen y su voz, pero existen tres excepciones: si se trata de una participación en actos públicos; si existe un interés científico, cultural o educacional prioritario, tomando las precauciones suficientes para evitar un daño innecesario; si se trata del ejercicio regular del derecho de informar sobre acontecimientos de interés general.

En tal sentido, la práctica periodística se enmarca en estas excepciones por lo que como regla general no es necesario obtener el consentimiento de la persona para publicar una foto o una imagen suya. De todas maneras, siempre es importante estar al tanto de la jurisprudencia más actualizada, ya que ella es la que nos orienta acerca de cómo se deben interpretar las normas generales al momento de ser aplicadas a cada caso particular.

Protección de niñas, niños y adolescentes

Si bien la Ley de Protección de Datos Personales no diferencia entre el tratamiento de los datos personales de mayores y de menores de edad, lo cierto es que la Convención sobre los Derechos del Niño en Argentina tiene rango constitucional y en este pacto internacional se especifica que ningún niño o niña puede ser objeto de injerencias arbitrarias o ilegales en su vida privada. Por lo tanto, se trata de un principio que se aplica para el tratamiento de datos personales de chicas y chicos en nuestro país.

En las coberturas periodísticas en las que estén involucradas chicas y/o chicos, los profesionales de la comunicación deben tomar todos los recaudos necesarios para abordar información referida a los menores de edad, sobre todo teniendo en cuenta el impacto que puede provocar en su vida cotidiana la difusión pública vinculada a sus personas. Si bien en nuestro país en los últimos años se ha tomado conciencia de qué es necesario preservar los rostros y los nombres de los menores, aún hay un largo camino por recorrer.

En ese contexto, la recomendación primordial para los periodistas profesionales y en formación es proteger los datos personales, la identidad y privacidad de las niñas, niños y adolescentes con el objetivo de no exponerlos a posibles vulneraciones de sus derechos.

Las coberturas periodísticas en oportunidades utilizan recursos de edición como el pixelado, el desenfocado o la cobertura del área de los ojos para evitar exponer la identidad de chicos y chicas. Sin embargo, a veces esos recursos no suelen ser del todo efectivos porque sí se difunde información vinculada con sus identidades como, por ejemplo, la calle en la que viven, los nombres de sus padres o la escuela a la que asisten. Se trata de indicios que podrían llevar a la identificación de las y los chicos.

A diferencia de lo que ocurre con una persona mayor, cuando se difunde información de menores de edad, la recomendación es solicitar a los padres y/o encargados el consentimiento explícito. El mismo debe ser brindado por escrito a padres y/o tutores del menor de edad. Se debe informar la finalidad para la cual se recogen los datos, quiénes tendrán acceso a esa información y explicitar cómo rectificar o revocar el acceso a los datos. Asimismo, cuando sea necesario brindar información en un caso de búsqueda de paradero las buenas prácticas periodísticas recomiendan publicar la foto del menor que fuera proporcionada por sus familiares para su difusión. Una vez hallada la persona dejar de difundir su imagen para evitar la exposición de la chica o el chico.

Al tratamiento de información sobre menores durante coberturas periodísticas también se suma otro aspecto no menor cuando hablamos de la protección de datos personales de las niñas, niños y adolescentes y está vinculado con sus derechos en entornos digitales.

De acuerdo con el informe “Chic@s Conectados”²⁵ que auspicia UNICEF, nueve de cada diez de las niñas, niños y adolescentes argentinos se conecta a internet a través del celular, utiliza las redes sociales para intercambiar mensajes con amigos y en un

80 por ciento de los casos, usa la red para hacer tareas escolares. En ese contexto, la mitad de los chicos y chicas entrevistados dijo “usar internet todo el tiempo”.

Lo cierto es que un gran porcentaje de esas niñas, niños y adolescentes no están al tanto de los posibles riesgos a los que están expuestos cuando comparten datos personales en entornos digitales y menos aún reconocen que esa información les pertenece y que tiene el derecho a exigir que no se difunda o se comparta con terceros.

Por eso resulta fundamental que los medios de comunicación retomen este tipo de problemáticas en su agenda de trabajo con el objetivo de brindar información certera sobre los derechos de los menores de edad respecto a la utilización de sus datos personales.

4. La privacidad y la protección de datos personales como interés público

Los periodistas y comunicadores pueden colaborar activamente en la defensa de la privacidad y la protección de datos personales promoviendo la difusión de los conflictos y tensiones que se desatan alrededor de estos derechos ya que se trata de temas de interés público y, por lo tanto, político.

También resulta necesario que los periodistas y comunicadores adopten buenas prácticas para asegurar la correcta protección del derecho a la privacidad y la protección de datos personales de las personas que se vean involucradas en hechos noticiables y coberturas periodísticas y así cumplir con su deber de informar de la mejor manera posible.

Como hemos desarrollado a lo largo de este trabajo, la privacidad y la protección de datos personales vienen ganando espacio en la agenda periodística, sólo se trata de contextualizar los hechos y hacerse las preguntas que cualquier periodista realiza ante los sucesos: qué, cuándo, dónde, quién, cómo y por qué.

El listado de temas que a las nociones vinculadas con la privacidad en entornos digitales es amplio y va desde el funcionamiento de los sistemas de reconocimiento facial por fuerzas de seguridad, el tratamiento de información recopiladas por aplicaciones -públicas y privadas-, campañas de desinformación online, la mediación algorítmica, la plataformización de la economía, regulaciones a las empresas tecnológicas, etc.

La mejor forma de visibilizar esta agenda de temas vinculados a la privacidad desde la práctica periodística es abordarlos con una

mirada crítica, poniendo el acento en la afectación de derechos asociados como la libertad de expresión, el acceso a la salud, al trabajo o la educación, entre otros.

Si bien el centro del debate global vinculado a la privacidad está dominado por la afectación de derechos en entornos digitales, lo cierto es que también se producen vulneraciones por fuera de ese ecosistema que obligan a los profesionales de la comunicación a realizar una mirada crítica sobre las prácticas periodísticas sin por eso afectar el derecho a informar sobre sucesos de interés público.

Resulta relevante que periodistas y comunicadores perciban el interés en resguardar información personal de protagonistas de las noticias cuando sea necesario, al tiempo que centren esfuerzos en abrir el debate público el derecho de las personas sobre su privacidad.

En definitiva, la construcción de una narrativa sólida sobre la privacidad y la protección de datos personales es una tarea en donde el periodismo tiene un rol central, abordando la agenda de temas vinculados con el acceso a derechos garantizados por la Constitución Nacional.

5. Notas

- 1 Declaración Universal de Derechos Humanos. Art. 12. Disponible en: <https://www.un.org/es/universal-declaration-human-rights/>.
Declaración Americana de los Derechos y Deberes del Hombre. Art. V. Disponible en: http://www.infoleg.gob.ar/?page_id=1000.
Convención Americana sobre Derechos Humanos (Pacto de San José). Art. 11. Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm.
Pacto Internacional de Derechos Civiles y Políticos. Artículo 17. Disponible en: <https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx>.
Convención sobre los Derechos del Niño. Artículo 16: <https://www.un.org/es/events/childrenday/pdf/derechos.pdf>.
- 2 Protección de los datos personales. Ley 25.326. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>
- 3 “¿Sirvieron de algo 50 años de bajadas de impuestos a los ricos?”
Disponible en: <https://www.bbc.com/mundo/noticias-55650204>
- 4 *El virus de la desigualdad*. Disponible en: <https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621149/bp-the-inequality-virus-summ-250121-es.pdf>
- 5 “Edward Snowden: the whistleblower behind the NSA surveillance revelations”. Disponible en: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.
- 6 “The Cambridge Analytica Files”. Disponible en: <https://www.theguardian.com/news/series/cambridge-analytica-files>.
- 7 “China’s social credit system was due by 2020 but is far from ready”.
Disponible en: <https://algorithmwatch.org/en/story/chinas-social-credit-system-overdue/>

- 8 “Libertades individuales vs. cámaras de vigilancia en América Latina”. Disponible en: <https://www.vice.com/es/article/gy4g99/libertades-individuales-vs-camaras-de-vigilancia-en-america-latina>
- 9 “81% of ‘suspects’ flagged by Met’s police facial recognition technology innocent, independent report says”. Disponible en: https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941?mc_cid=9b16974e83&mc_eid=f7ec87caff
- 10 “Seis días arrestado por un error del sistema de reconocimiento facial”. Disponible en: <https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien>
- 11 “San Francisco becomes the first US city to ban facial recognition by government agencies”. Disponible en: <https://www.theverge.com/2019/5/14/18623013/san-francisco-facial-recognition-ban-vote-city-agencies>
- 12 “Detenida por el parecido con una persona buscada”. Disponible en: <https://www.pagina12.com.ar/194339-detenida-por-el-parecido-con-una-persona-buscada>
- 13 “Spam filters are efficient and uncontroversial. Until you look at them”. Disponible en: <https://algorithmwatch.org/en/story/spam-filters-outlook-spamassassin/>
- 14 “Court Rules Deliveroo Used ‘Discriminatory’ Algorithm”. Disponible en: <https://www.vice.com/en/article/7k9e4e/court-rules-deliveroo-used-discriminatory-algorithm>
- 15 “Los ‘riders’ ganan el macrojuicio contra Deliveroo en Barcelona”. Disponible en: https://www.eldiario.es/catalunya/riders-ganan-macrojuicio-deliveroo-barcelona-jueza-sentencia-748-repartidores-son-falsos-autonomos_1_6745634.html

- 16 Helen Nissenbaum en Twitter: <https://twitter.com/HNissenbaum>
- 17 Cathy O'Neil en Twitter: <https://twitter.com/mathbabedotorg>
- 18 Natalia Zuazo en Twitter: <https://twitter.com/nataliazuazo>
- 19 Marta Peirano en Twitter: <https://twitter.com/minipetite>
- 20 Evgeny Morozov en Twitter: <https://twitter.com/evgenymorozov>
- 21 Eli Parisier en Twitter: <https://twitter.com/elipariser>
- 22 "Así fue la demanda de Menem a Noticias tras la revelación sobre su hijo Carlos Nair". Disponible en: <https://www.perfil.com/noticias/politica/caso-fontevecchia-damico-la-denuncia-de-menem-a-noticias-por-dos-tapas-sobre-su-hijo-carlos-nair.phtml>
- 23 "Balbín y una foto 'condenada' ". Disponible en: <https://www.eldia.com/nota/2012-2-11-balbin-y-una-foto-condenada>.
- 24 Código Civil y Comercial. Título I: Persona Humana. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/norma.htm#6>
- 25 *Kids online Argentina*. Disponible en: <https://www.unicef.org/argentina/media/1636/file/Kids-online.pdf>



adc.org.ar