Plataformas y riesgo informacional. El caso argentino en el periodo 2020-2022.

POR MAXIMILIANO JAVIER PAESANI Y MARÍA FLORENCIA ARES

Platforms and informational risk. The argentine case in the 2020-2022 period.

Maximiliano Javier Paesani. Profesor de la Universidad Nacional de Salta (UNSa), donde desarrolla actividades docentes en el área de Filosofía. Se ha desempeñado en asignaturas vinculadas con la Lógica, la Ética, la Metodología de las Ciencias y la Introducción a la Filosofía. Actualmente desarrolla su actividad docente en la Facultad Regional Multidisciplinar Tartagal de la UNSa. Correo-e: maxijpaesani@hotmail.com

María Florencia Ares. Licenciada en Sociología y docente de la Facultad Regional Multidisciplinar Tartagal de la Universidad Nacional de Salta (UNSa). Integra el equipo de investigación de la Unidad de Estudios Sociales y de Comunicación de la Sede Regional Tartagal (UNESCOM-SRT). Sus áreas de interés comprenden la sociología, los estudios sobre comunicación y cultura y el análisis de los mecanismos sociales. Correo-e: floren_flo@hotmail.com

Cómo citar: Paesani, M.J. y Ares, M.F. (2026). Plataformas y riesgo informacional. El caso argentino en el período 2020-2022. *Revista Argentina De Comunicación*, 14(17), 73-94.

CC BY NC SA

Fecha de Recepción: 19/08/2026 - **Fecha de aprobación:** 1/10/2026

Resumen

El propósito del presente trabajo es identificar casos que ilustren daños potenciales para individuos y poblaciones como resultado de la recolección, almacenamiento y utilización de datos personales por parte de entidades comerciales privadas o instituciones estatales. Nos centramos en las plataformas digitales y, en sentido amplio, en los sistemas de información que, como modelos de negocios y de gestión administrativa, requieren la estructuración de grandes bases de datos con información sensible. La fragilidad que de ello deriva se origina en la escasa protección que esos datos obtienen a largo plazo, ya sea por desidia o por el tipo de dinámicas que los circunscriben. Establecida la existencia de los riesgos en general, nos ocupamos del contexto nacional argentino durante el periodo 2020-2022 de la pandemia por COVID-19. A partir de un estudio exploratorio-descriptivo basado en fuentes secundarias, seleccionamos quince incidentes que, a nuestro juicio, permiten ilustrar el uso del concepto de riesgo informacional y las deficiencias que pueden observarse en las medidas de protección de los datos personales. Los resultados muestran un predominio de incidentes en organismos públicos y una presencia significativa de datos sensibles, en particular de salud. Repasamos algunas regulaciones vigentes en materia de protección de datos personales, sin entrar en discusiones jurídicas de carácter técnico. Por último, concluimos señalando la necesidad de desarrollar acciones precautorias a nivel individual, sin que ello exima a las instituciones de su responsabilidad en la protección de los datos que administran.

Palabras clave: ciberseguridad, datos personales, pandemia, plataformas, riesgo informacional.

Abstract

The purpose of this paper is to identify cases that illustrate potential harms to individuals and populations resulting from the collection, storage and use of personal data by private commercial entities or state institutions. We focus on digital platforms and, in a broader sense, on information systems that, as business and administrative management models, require the structuring of large databases containing sensitive information. The resulting fragility stems from the limited long-term protection these data receive, whether due to negligence or to the kind of dynamics that surround them. Having established the existence of these risks in general, we address the Argentine national context during the 2020-2022 period of the COVID-19 pandemic. Based on an exploratory and descriptive study of secondary sources, we select fifteen incidents that, in our view, illustrate the use of the concept of informational risk and the shortcomings that can be observed in personal data protection measures. The results show a predominance of incidents in public bodies and a significant presence of sensitive data, particularly health data. We review some current regulations on personal data protection, without entering into technical legal discussions. Finally, we conclude by pointing out the need to develop precautionary actions at the individual level, without releasing institutions from their responsibility to protect the data they manage.

Keywords: cybersecurity, informational risk, pandemic, personal data, platforms.

Introducción

El almacenamiento y procesamiento de datos personales estructurado en grandes plataformas digitales tiene ventajas obvias para los procesos administrativos y económicos. Los aspectos positivos de las posibilidades abiertas por la organización técnica de la información pueden, sin embargo, inducir a una consecuencial subestimación de riesgos e inconvenientes que vienen asociados a las innegables ventajas. La estructura estadística de tales riesgos (por ejemplo, su baja frecuencia) tiende a disminuir la conciencia pública e individual de su existencia. En tales casos, sostenemos, la ponderación impone considerar exposiciones por encima de la nuda probabilidad. Concretamente, las consecuencias son lo bastante graves como para impedir subestimar ciertos eventos sobre la base de su escasa presencia.

La creación de bases de datos con información personal sobre individuos y poblaciones permite la emergencia de tipos de acciones que pueden resultar perjudiciales en medidas variables para las personas involucradas. Utilizamos la categoría de "incidentes informáticos" que incluye: robos, secuestros, filtraciones y/o divulgación de información privada que exponen a ciberdelitos, cristalización de sujetos en categorías sociales o vulneración de derechos humanos.

Nos detenemos en algunos elementos ilustrativos enfocados en la casuística para Argentina, en el periodo de la pandemia por COVID-19, 2020-2022. Desarrollamos breves comentarios sobre cuestiones de regulación, sin entrar en la discusión de los aspectos jurídicos más técnicos. La intención es fundamentar una mirada escéptica sobre la prospectiva basada en el enfoque regulativo público.

El problema interesa a los estudios de comunicación en la medida en que las plataformas se han convertido en infraestructuras centrales de la mediación social contemporánea. La literatura sobre plataformización ha mostrado que la lógica de extracción y procesamiento de datos reorganiza tanto los intercambios comunicacionales como las relaciones entre ciudadanos, empresas y Estado (van Dijck et al., 2018), mientras que los estudios sobre vigilancia han caracterizado esa lógica como una nueva forma de acumulación basada en la conversión de la experiencia humana en datos de comportamiento (Zuboff, 2020). En ese marco, el objetivo del presente trabajo es identificar y describir incidentes de seguridad de la información ocurridos en Argentina entre 2020 y 2022 que permitan ilustrar el concepto de riesgo informacional, y discutir los alcances y límites de los mecanismos de protección vigentes.

Analizamos líneas generales de algunas propuestas para la protección de usuarios, considerando ciertos avances positivos. Pero consideramos que son insuficientes desde la perspectiva de la gestión personal de los riesgos.

Los modelos de negocios de plataformas basados en la publicidad y en la instrumentalización comercial de los usuarios, por ejemplo, no enfatizan lo suficiente en la seguridad de la información personal, que adquiere la forma de mercancía transable. Las ad-

ministraciones públicas, por otra parte, presentan deficiencias en la protección de los datos, y actúan sobre unos horizontes temporales que favorecen la irresponsabilidad a largo plazo. En concreto, las administraciones tienen plazos de corto y mediano alcance, mientras que, como explicaremos, las bases de datos tienden a la perennidad. El fracaso de las técnicas de anonimización, invalidadas en gran parte por el avance de las ciencias de la reidentificación, ejemplifica claramente las deficiencias en la protección de los datos personales a largo plazo.

Las falencias en la aplicación de la regulación y los incentivos perniciosos en los modelos de negocio más difundidos parecen requerir, principalmente, medidas defensivas al nivel de los ciudadanos y consumidores individuales.

Material y métodos

El presente artículo es resultado de una investigación de carácter exploratorio-descriptivo, basada en el estudio de casos a partir de datos secundarios. Los datos proceden de informes técnicos de organizaciones estatales, resoluciones de la Agencia de Acceso a la Información Pública (AAIP), documentos legales, periódicos en línea, artículos científicos y libros.

Los 15 casos presentados en la Tabla 1 corresponden a incidentes de seguridad de la información ocurridos en el periodo 2020-2022 en Argentina. La selección del periodo de análisis no es arbitraria: la pandemia por COVID-19 coincidió con un incremento de las denuncias por delitos informáticos, asociado al mayor uso de servicios y aplicaciones de internet (Secretaría de Innovación Tecnológica del Sector Público, 2022). El criterio de selección de los casos es la gravedad de los mismos, determinada por la cantidad de individuos afectados; cuando las fuentes no informan ese dato, la magnitud se consigna a partir del volumen de datos comprometidos o de la cobertura del sistema vulnerado. Además, se distingue el tipo de datos comprometidos (micro, meso o macrodatos) y los sistemas informáticos vulnerados. Se excluyen incidentes sobre los que no se tiene confirmación, ni información sobre la población y el tipo de datos afectados.

La definición de datos micro, meso y macro pertenece a Seltzer y Anderson (2008). Los datos micro son registros o archivos con identificaciones para cada individuo. Los datos meso son datos tabulados para áreas geográficas lo suficientemente pequeñas para que los resultados puedan utilizarse operacionalmente para identificar y actuar sobre un subgrupo poblacional específico. Los datos macro son tabulaciones referidas a grandes áreas geográficas. La diferencia entre datos meso y macro depende del tamaño de las unidades geográficas donde se recolectan los datos, de la distribución de la población objetivo en esas unidades, y de los usos operacionales previstos. En la Tabla 1, un incidente se clasifica como micro cuando compromete registros individuales identificables; se agrega la categoría meso cuando los datos filtrados permiten, además, identificar subgrupos poblacionales en áreas geográficas acotadas, y macro cuan-

do la base comprometida abarca potencialmente al conjunto de la población nacional, como en el caso del RENAPER.

¿Qué son las plataformas digitales y para qué sirven?

Las plataformas son sistemas de recursos técnicos y humanos, que permiten operativizar modelos de negocios y de gestión basados en la extracción, recolección, almacenamiento, análisis y uso de gigantescas cantidades de datos. "Son infraestructuras digitales que permiten que dos o más grupos interactúen. De esta manera se posicionan como intermediarias que reúnen a diferentes usuarios: clientes, anunciantes, proveedores de servicios, productores, distribuidores y objetos físicos" (Srnicek, 2021, p. 45). Permiten la mediación entre diferentes grupos. Son espacios en los cuales los usuarios desarrollan múltiples actividades, que son registradas, categorizadas, almacenadas y a veces publicadas (Srnicek, 2021).

Además, constituyen sistemas muy diversos entre sí, a veces difíciles de identificar como pertenecientes a una misma categoría. Así, por ejemplo, el régimen jurídico de propiedad económica y el tipo de producto-servicio que brindan, son características que pueden servir para establecer distinciones (Gillespie, 2017).

También se puede distinguir entre, por una parte, empresas que mueven productos físicos (sistemas materiales) por medio de servicios en línea, como Uber, Apple y el servicio de comercio electrónico de Amazon y, por otra parte, empresas que venden exclusivamente servicios en línea tal como Facebook, Twitter y Google. Estas últimas, puramente digitales, suelen violar impunemente e ignorar las regulaciones locales en mayor medida que las otras (Ohm, 2018). Las plataformas, además, poseen una característica particular que las diferencia de cualquier otro tipo de empresa: pueden operar en cualquier lugar del mundo en que tenga lugar la interacción digital (Srnicek, 2021).

Sus métodos de extracción de datos son múltiples: desde la mera observación de comportamientos en los medios digitales, a la solicitud de datos a través de encuestas o entrevistas, e incluso la extracción compulsiva. Sus registros abarcan variados aspectos de la vida de las personas. Registran tanto procesos productivos o factores climáticos como datos referidos a origen étnico, salud, educación, gustos, opiniones, ingresos, historial crediticio, localización geográfica, etc. Sin embargo, a pesar de su variedad, poseen características comunes. Gillespie (2017) señala dos: 1) todas almacenan y organizan contenidos producidos por los usuarios para su distribución y circulación pública, y 2) no producen ese contenido, pero toman decisiones sobre el mismo.

Cabe precisar que, en este trabajo, la noción de plataforma se emplea en un sentido amplio. Varios de los casos analizados no corresponden a plataformas de intermediación en sentido estricto, sino a sistemas de información de organismos públicos y de empresas (registros de identidad, bases de datos sanitarias, judiciales o de clientes).

Los incluimos porque comparten con las plataformas la lógica que aquí interesa: la recolección, el almacenamiento y el procesamiento centralizado de grandes volúmenes de datos personales, y la consiguiente exposición de sus titulares al riesgo informacional.

Potenciales daños asociados al uso de plataformas

El análisis de grandes bases de datos puede revelar características explotables de las personas. En general los objetivos son comerciales o administrativos. Pero también abren la posibilidad de usos explotativos de carácter más grave, como exposición a delitos o vulneraciones de la integridad personal y/o grupal de los usuarios.

William Seltzer y Margo Anderson (2008) han recopilado evidencia histórica de la utilización de bases de datos de individuos y poblaciones con propósitos diferentes a los que guiaron su creación. Los autores demuestran cómo datos poblacionales recolectados por agencias estadísticas y programas gubernamentales fueron utilizados para perseguir a individuos y subgrupos de población vulnerable. Este tipo de utilización de los sistemas de datos de población ha ocurrido tanto en países con regímenes totalitarios como democráticos y las consecuencias han sido desiguales para los diferentes subgrupos de población o individuos afectados: persecución, encierro y muerte, fueron algunos de los resultados más graves de tales acciones.

El modelo de negocio subyacente a algunas plataformas, por ejemplo, las denominadas redes sociales, depende de la disposición de los usuarios a compartir su información personal. En la actualidad el llamado *targeted marketing* o *behavioral targeting* es muy popular entre los anunciantes. Una empresa especializada en marketing digital describe la técnica y afirma que utiliza la información del usuario web para fortalecer las campañas publicitarias. La técnica consiste en recopilar datos de una variedad de fuentes sobre los comportamientos de compra y navegación en línea del cliente potencial. Por ejemplo, información de búsquedas en internet, historiales de compras, sitios web visitados con frecuencia y todo lo que se considere útil y accesible para crear un perfil de usuario lo más completo posible. Esta información ayuda a crear anuncios que se ajusten a los hábitos, intereses y deseos de ese usuario específico, y que luego se muestran en su navegador web. El objetivo es entregar mensajes publicitarios a los usuarios cuyos comportamientos han sido rastreados y que han mostrado el mayor interés en ellos (Lotame, 2018).

Puede resultar ilustrativo el caso de una famosa cadena de almacenes de Estados Unidos, cuyos analistas pueden identificar, según afirman, qué clientas se encuentran embarazadas, e incluso predecir sus fechas de parto, detectando cambios en los hábitos de compra (Ohm, 2010).

La actividad registrada en las plataformas constituye lo que se ha llamado "rastro digital": conjuntos de microdatos sobre las personas, que pueden contener información

sensible. Hal Abelson, Ken Ledeen y Harry Lewis (2008) señalan que muchos de los datos que las plataformas obtienen al registrar nuestros comportamientos y características implican intromisiones que vulneran la privacidad. Pueden ser el resultado inesperado de cosas que hacemos voluntaria y conscientemente. Otras veces, sin embargo, no sabemos que estamos creando "huellas o rastros digitales".

El término "riesgo informacional" hace referencia al daño potencial derivado de la desclasificación o divulgación de información personal. Los daños pueden ser económicos: perder un trabajo, no calificar para determinadas líneas de crédito, etc.; sociales: vergüenza, discriminación, etc.; psicológicos: depresión, etc. (Salganik, 2018); o incluso criminales: ser víctima de chantaje o extorsión, ser procesado por un delito, perder la libertad o incluso la muerte (Salganik, 2018; Seltzer y Anderson, 2008).

Una técnica protectiva es la anonimización: un conjunto de procedimientos de modificación de la información que dificultan la identificación de los sujetos, con el objetivo declarado de garantizar la privacidad. Es una técnica necesaria cuando quienes recolectan datos divulgan la información a otros grupos por diferentes motivos. Pero, a partir de los años 90, se demostró que el método es fácil de eludir y ya no garantiza la privacidad debido a la enorme capacidad técnica de las nuevas tecnologías que permite conectar nuestros "rastros digitales" dispersos por la red y llegar hasta nosotros. Los casos del buscador AOL y del Premio Netflix ilustran el fracaso de la anonimización y muestran las consecuencias no previstas para los individuos una vez que cierta información accede a dominio público (Ohm, 2010).

En el año 2006, en el marco de un programa de colaboración con la comunidad académica, investigadores de *America Online* (AOL) publicaron durante 10 días, en un sitio web, las búsquedas realizadas por 650.000 usuarios del buscador. Previo a su publicación, los datos fueron anonimizados: se borró toda información de carácter personal (como la dirección IP y el nombre de usuario) y se asignaron números únicos de identificación a fin de evitar que usuarios individuales pudieran ser identificados (Ohm, 2010). Poco tiempo después, dos periodistas de *The New York Times*, Michael Barbaro y Tom Zeller (2006), lograron identificar a una usuaria a partir de los registros publicados. Se trataba de una viuda de 62 años que vivía en una ciudad de Georgia, cuyos deseos, intereses y preocupaciones quedaron expuestos al público; entre sus búsquedas figuraban consultas sobre su salud, como "temblores en las manos", "boca seca" o "bipolar". Los registros de otros usuarios incluían búsquedas vinculadas con delitos y con situaciones personales y familiares de extrema sensibilidad (Bañales, 2006).

AOL pidió disculpas y eliminó los registros de búsquedas de su sitio. Sin embargo, al momento de retirar la publicación ya contaba con 806 descargas (Arrington, 2006). El caso de AOL terminó exponiendo cuánta información personal revelamos, a menudo sin querer o sin saber, al utilizar motores de búsqueda, y el riesgo al que nos exponemos cuando grandes empresas recopilan y almacenan esos datos (Barbaro y Zeller, 2006).

También en el año 2006, en el mes de octubre, Netflix publicó un conjunto de datos con las calificaciones de películas de 480.189 suscriptores, en el marco de un concurso que ofrecía un millón de dólares a quienes lograran crear un algoritmo de recomendación de películas. Los datos fueron anonimizados y solo se conservaron las calificaciones de películas y sus fechas (Narayanan y Shmatikov, 2008).

Arvind Narayanan y Vitaly Shmatikov (2008), en *Robust de-anonymization of large sparse datasets*, demostraron que es posible identificar de manera unívoca al 99% de los registros del conjunto de datos publicado conociendo 8 calificaciones de películas (de las cuales 2 pueden ser completamente erróneas) y sus fechas, con un margen de error de hasta 14 días; para el 68% de los registros, alcanzan 2 calificaciones y sus fechas, con un margen de error de 3 días. Además, realizaron una serie de experimentos que cruzaron información proveniente de registros públicos de Internet Movie Database (IMDb) con los registros anónimos publicados por Netflix, para obtener información confidencial sobre algunos suscriptores de IMDb presentes en la base de datos de Netflix. A partir de las calificaciones que un usuario realizó de forma pública y voluntaria en IMDb, los autores descubrieron todas las calificaciones privadas que ese usuario realizó en el sistema Netflix, con lo que es posible conjeturar acerca de su orientación política, sus opiniones religiosas y su orientación sexual. La conclusión es que la divulgación de datos de los suscriptores abre la posibilidad de extraer información no pública sobre ellos y los expone al riesgo de que esa información pueda ser utilizada, de alguna forma, en su contra.

Es común publicar información sobre nuestros gustos o aficiones, posiciones políticas, creencias religiosas, etc., con el objetivo, por ejemplo, de contribuir a causas sociales. Pero no siempre es posible controlar la difusión de nuestra información privada, o el uso que puede hacerse de ella cuando adquiere carácter público. ¿Cómo es posible evitar que esa información tenga un "mal uso"? ¿Cómo evitar que el derecho a expresarnos libremente implique que alguien pueda usar esa información en nuestra contra? La era digital plantea este tipo de cuestiones.

Cabe recordar el caso de una docente de la Universidad del Salvador (USAL) que en el año 2009 hizo pública su participación en la primera campaña colectiva de apostasía en Argentina y, al día siguiente, fue despedida de esa universidad, donde se desempeñaba desde hacía 10 años. El 31 de marzo se publicaron en un diario porteño sus declaraciones, en las que expresaba sus razones para desvincularse del catolicismo, adhiriendo a la campaña de apostasía colectiva realizada el día anterior en el Arzobispado de Buenos Aires. La carta de despido de la USAL está fechada el 1 de abril; en ella se le comunica que el motivo del despido son sus expresiones públicas sobre la apostasía y sus juicios negativos sobre la Iglesia católica. A pesar de sus reclamos, la docente no logró que sus datos fueran borrados del "Registro Digital de Sacramentos", donde figuraba como apóstata en anotaciones marginales del acta de bautismo y de otros documentos esenciales. Después de 11 años, en septiembre de 2020, la Dirección Nacional de Protección de Datos Personales intimó a la Iglesia católica a borrar toda la in-

formación referida a ella, y afirmó que la institución no está autorizada a llevar un registro de apóstatas. Si bien la ley habilita a la Iglesia católica, a las organizaciones religiosas y a las organizaciones políticas y sindicales a llevar un registro de sus miembros, prohíbe expresamente la formación de archivos, bancos de datos o registros que puedan revelar datos sensibles. Las convicciones religiosas constituyen datos sensibles y, por lo tanto, merecen una mayor protección que otras categorías de información (Carbajal, 2009, 2020). En septiembre de 2020, además, la Iglesia católica fue sancionada mediante la RESOL-2020-41-APN-AAIP por no inscribir su base de datos de carácter personal en el registro correspondiente (Agencia de Acceso a la Información Pública, 2020).

En general, se desconocen las maneras en que se pueden explotar los datos en perjuicio de los usuarios, dado que la aceleración tecnológica modifica constantemente el panorama de oportunidades e incentivos. La construcción de inmensas bases de datos, que se ha dado en llamar Big Data, agudiza la exposición en escala a consecuencias no deseadas derivadas de dichas prácticas. Las filtraciones de datos de individuos o poblaciones son cada vez mayores, a medida que se incrementa la cantidad de información recolectada.

Ante hechos como robo, filtración, y/o divulgación de datos debe tenerse en cuenta el tamaño de la plataforma, porque éste se relaciona con la capacidad de daño que pueden causar; una plataforma con 100 millones de usuarios es potencialmente más dañina que una con 1 millón de usuarios, solo por el hecho de que puede dañar a más personas (Ohm, 2018). Su capacidad y velocidad de extracción, recolección, almacenamiento, procesamiento y transmisión de datos, también son características a considerar cuando se trata de evaluar el daño potencial.

La recolección y almacenamiento de datos en la era digital supone una escala completamente nueva, en la que el poder de las empresas y los gobiernos para observar y experimentar con personas, incluso sin su conocimiento, es cada vez mayor. Se ha utilizado la analogía con el Panóptico de Bentham para ilustrar la asimetría de conocimiento entre ver y ser visto (Foucault, 1975; Salganik, 2018). Las empresas y los gobiernos con sus plataformas ocuparían la torre de vigilancia desde la cual observan, registran y regulan conductas. Los vigilados no pueden mantener su privacidad, o ni siquiera saben que son observados.

La pérdida de confianza en prestadores de servicios e instituciones nos conduce a reflexionar acerca de lo imprevisible de las consecuencias cuando estos fallan en proteger los datos de sus usuarios. David Le Breton (2021) sostiene que la noción de confianza es necesaria para vivir sin temor y nos permite relacionarnos con los otros. Por ejemplo, cuando conducimos un vehículo confiamos que los otros conductores, también, respetarán las reglas de tránsito, esto es, se detendrán en los semáforos, no conducirán en contramano, etc. Toda pérdida de confianza respecto de esto provoca una

intensa sensación de vulnerabilidad. Nos preguntamos entonces: quienes recogen, almacenan y organizan nuestros datos ¿en qué medida pueden protegerlos?

La protección de datos personales en Argentina

Nadie está protegido de todos los imponderables que pueden surgir producto de la vida misma. Los seguros y el Estado tratan de brindar a los individuos cierta protección, de tipo financiera o a través de legislaciones que protejan su estatus social y material (Le Breton, 2021). El riesgo derivado del uso de plataformas tecnológicas y sus posibles consecuencias no deseadas, principalmente aquellas que afectan al control de nuestra información en línea, ha suscitado la emergencia de una serie de instrumentos legales, tales como leyes e instituciones destinadas a prevenir y actuar cuando se vulneran derechos humanos como la privacidad, que constituye un derecho fundamental consagrado en numerosos tratados de derechos humanos, y que resulta central en la protección de la dignidad humana.

Las constantes innovaciones de la era digital han provocado cambios en el derecho a la privacidad, que ha evolucionado hasta abarcar las obligaciones del Estado relacionadas con la protección de datos personales (Asociación por los Derechos Civiles y Privacy International, 2017). Actualmente, la protección de datos personales en Argentina es regulada por la Ley Nº 25.326 que sigue estándares internacionales y se aplica al tratamiento de datos personales por organismos públicos y privados. En el año 2000, en nuestro país, conjuntamente con la sanción de la Ley 25.326, se creó la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente entonces del Ministerio de Justicia y Derechos Humanos que, en tanto órgano de aplicación y control de la Ley 25.326, tenía la competencia para notificar a las plataformas y demás intermediarios en línea el bloqueo a contenidos que sean incompatibles con esa Ley. Desde 2017, la autoridad de control de la Ley 25.326 es la Agencia de Acceso a la Información Pública (AAIP), en cuyo ámbito funciona la DNPDP (Decreto 746/2017). Corresponde a la AAIP realizar todas las acciones necesarias para el cumplimiento de los objetivos y disposiciones de la ley; además, posee la facultad para atender denuncias y reclamos en relación con el tratamiento de datos personales.

A partir de la sanción de la Ley 25.326, Argentina quedó alineada con el marco de protección de la Unión Europea (UE). El 30 de junio del año 2003 la UE le otorgó estatus de país con protección adecuada. Ello facilita el flujo de información y simplifica el procesamiento de datos de residentes europeos a aquellas empresas radicadas en el país (Decisión 2003/490/CE, 2003). En el año 2018 comenzó a aplicarse en la UE el Reglamento General de Protección de Datos (RGPD o GDPR, por sus siglas en inglés). Desde ese momento, Argentina empezó un proceso de actualización del régimen de protección de datos personales, a fin de cumplir los estándares que esa norma establece, teniendo en cuenta las nuevas condiciones tecnológicas y los riesgos que con ellas aparecen (Minuto, 2021).

La pandemia por COVID-19 puso en evidencia que las infraestructuras tecnológicas de información y comunicación estaban expuestas a graves incidentes. Como respuesta, en el periodo 2020-2022, se han establecido una serie de Resoluciones y Disposiciones referidas a la Seguridad de la Información y a la Protección de los Datos personales: se aprobó el "Modelo Referencial de Política de Seguridad de la Información" (Disposición DNCIB 1/2022), se creó el Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad (Disposición DNCIB 1/2021), y se establecieron el "Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional" (Disposición DNCIB 7/2021), la Guía Introductoria a la Seguridad para el Desarrollo de Aplicaciones Web (Disposición DNCIB 8/2021), los Requisitos mínimos de Seguridad de la Información para Organismos públicos (Decisión Administrativa 641/2021), el Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras (Disposición DNCIB 6/2021), y la AAIP sometió a consulta pública un anteproyecto de reforma de la Ley 25.326 de Protección de Datos Personales que, entre otras cosas, propone incluir los datos genéticos y los biométricos como datos sensibles; incorpora el concepto de extraterritorialidad para los casos en que los responsables de la recolección y del tratamiento de datos no se encuentren en el país; establece el principio de minimización de los datos personales, que implica no pedir más datos personales que los necesarios para los fines declarados; crea la obligación de notificar a la autoridad de control y a los titulares de los datos en casos de incidentes de seguridad, como hackeos; aumenta el monto económico de las sanciones, teniendo en cuenta el tipo de dato, riesgo y posición económica del infractor, etc. (ERREIUS, 2022b). A la fecha de redacción de este artículo, la reforma no ha tenido tratamiento parlamentario ni dictamen de comisión.

Resultados: incidentes informáticos y selección de casos (2020-2022)

Si bien en el pasado nuestras actividades también dejaban indicios, registros o "huellas", en la forma de registros telefónicos, gastos en tarjetas, pagos de cuentas, censos, etc., en la era digital —como afirman Abelson et al. (2008)— hay algo nuevo: la capacidad y la potencia informática para correlacionar, unir puntos, y crear una imagen nítida y detallada a partir de fragmentos dispersos. Una imagen de nosotros donde nuestros secretos, opiniones, acciones pasadas, gustos, están al descubierto. El presente trabajo busca resaltar posibles consecuencias negativas de los avances tecnológicos, y sus encarnaciones en modelos específicos de negocio o gestión, para aspectos de la integridad personal como ser la privacidad. La referencia a casos concretos de robos de datos y/o filtraciones puede ayudarnos a tomar conciencia de los peligros que implica que nuestra información personal se encuentre en manos de extraños.

A continuación, en primer lugar, presentamos los resultados de los informes publicados por la Dirección Nacional de Ciberseguridad sobre los incidentes informáticos re-

gistrados en los años 2020, 2021 y 2022, por el Centro Nacional de Respuesta ante Emergencias Informáticas (CERT.ar), que realiza tareas vinculadas a ciberataques que puedan afectar los sistemas y redes del Sector Público Nacional. En segundo lugar, avanzamos en elementos de casuística local relativos a robo y/o filtraciones de datos de individuos o poblaciones, con posibles implicaciones en términos de privacidad.

Se define un *incidente de seguridad* de la información o incidente informático como:

> acceso o intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información. Puede ser un evento que produzca un impedimento en la operación normal de un dispositivo, redes, sistemas o recursos informáticos. También puede ser una política de violación de seguridad de la información de una organización. (Dirección Nacional de Ciberseguridad [DNCIB], 2023, p. 1)

Durante el año 2020 se registraron 226 incidentes informáticos; en 2021 la cifra ascendió a 591 y en 2022 se reportaron 335, es decir, un 43,3% menos que el año anterior. Se observa, también, una migración hacia las plataformas digitales por parte de organismos estatales, industrias y usuarios particulares. Esta tendencia se mantiene desde el año 2020. Los organismos públicos registraron una mayor cantidad de ataques informáticos en el año 2022. Para las entidades privadas y los usuarios particulares las cifras disminuyeron respecto a años anteriores.

Un informe de la Secretaría de Innovación Tecnológica del Sector Público (2022) sostiene que durante los dos primeros años de la pandemia del COVID-19, en Argentina, se produjo un incremento de denuncias sobre diferentes modalidades delictivas en Internet. El incremento en el número de casos puede deberse a un mayor uso de las Tecnologías de la Información y las Comunicaciones, de servicios y aplicaciones de Internet, surgidos a partir de la implementación del teletrabajo, la educación a distancia y el pago de servicios, generado por el aumento del comercio electrónico.

El año 2021 se caracterizó por un alza considerable en la tasa de delitos informáticos. En cambio, en el 2022, si bien hubo menos delitos, se registra un aumento de la cantidad de denuncias sobre diferentes modalidades delictivas en Internet, lo que indica una mayor complejidad y sofisticación en las técnicas para cometer delitos (DNCIB, 2023). Asimismo, se advierte sobre "la aparición de asociaciones ilícitas y de bandas con cierto grado de organización, que toman al cibercrimen como emprendimiento delictivo" (Secretaría de Innovación Tecnológica del Sector Público, 2022, p. 2).

Los sectores que más ataques informáticos sufrieron, durante el 2021 y 2022, fueron el Estado y las Finanzas. Asimismo, los ataques más dañinos registrados fueron realizados por ransomware: un programa malicioso que encripta archivos de un dispositivo o sistema y afectaron principalmente a organizaciones públicas y privadas. Esta tendencia se originó en el año 2020 y continuó en los años siguientes. Los criterios del nivel de severidad se determinan a partir del tipo de incidente y la criticidad del recurso afectado. El nivel de impacto se valora según el daño potencial y/o real adverso causado sobre las infraestructuras tecnológicas, los sistemas de información y la informa-

ción que gestionan. Según el impacto se consideran 4 niveles de severidad: bajo, medio, alto y crítico (DNCIB, 2022). No todos los incidentes de seguridad son iguales. No es lo mismo perder los datos de una base de datos de empleados de una pequeña empresa, que perder los datos de una base de datos de todos los ciudadanos de un país.

Durante el 2021, 467 de los incidentes reportados fueron de severidad alta (79,02%), 69 de severidad media (11,68%), 39 de severidad baja (6,60%) y 16 de severidad crítica (2,71%). En el año 2022, 305 de los incidentes reportados (91,04%) fueron de severidad alta, 18 de severidad media (5,37%), 11 de severidad crítica (3,28%) y 1 de severidad baja (0,30%). En el 2022 se redujo la cantidad de incidentes registrados, pero, hubo un incremento en los incidentes considerados críticos como, por ejemplo, los dirigidos a los Ministerios. También subió la cantidad de incidentes de severidad alta y descendieron los de severidad media y baja. El tipo de incidentes más reportado en el sector estatal fue el de "Modificación no autorizada de la información": en el 2021 representó el 33,62% (79 casos) del total de 235 incidentes registrados en el sector estatal, mientras que en el 2022 alcanzó el 54,9% (39 casos) de un total de 71 (DNCIB, 2022, 2023). Este tipo de incidente, se ubica en la categoría "Compromiso de la Información" que fue, en el 2021 y 2022, la segunda categoría con mayor cantidad total de incidentes registrados: 101 casos y 63 casos, respectivamente. Se refiere a ataques de ransomware. Generalmente, quienes capturan la información solicitan un rescate para liberarla y no publicarla. Es una modalidad de ataque dirigida a organizaciones, y posee un gran potencial de daño para las infraestructuras tecnológicas, los sistemas de información y la información gestionada (DNCIB, 2022, 2023), además de someter a las instituciones a acciones de extorsión implica, también, riesgos adicionales para los individuos, cuyos datos fueron sustraídos y pueden ser vendidos en la dark web o ser utilizados para la comisión de otros ataques.

La Tabla 1 presenta una serie de "Incidentes de seguridad de la información" ocurridos en Argentina durante el periodo 2020-2022. Para cada caso se registra: Incidente informático y Plataformas involucradas; Cantidad de datos comprometidos y/o población afectada; Sistemas de información involucrados; Tipo de datos vulnerados; Fecha del Incidente y Fuente. Los criterios de selección de cada item han sido aclarados en el apartado "Material y métodos".

Entre los años 2020-2022 fue hackeado un gran número de entidades públicas y privadas. La casuística presentada incluye solo aquellos incidentes cuya ocurrencia ha sido confirmada (sea por fuentes oficiales o por medios de comunicación) y que involucran datos personales y/o datos sensibles de una gran cantidad de individuos y/o poblaciones.

Tabla 1. Selección de casos de robo, secuestro, filtración y/o divulgación de datos personales y/o sensibles de individuos, grupos o poblaciones de Argentina, en el periodo 2020-2022

Incidente informático y plataformas involucradas	Cantidad de datos comprometidos y/o población afectada	Sistemas de información involucrados	Tipo de datos vulnerados	Fecha del incidente	Fuente
Filtración de datos sensibles de la Dirección Nacional de Migraciones	1,8 GB de datos de personas que ingresaron y egresaron al país durante 2015 y 2016	Base de datos de control de ingreso y egreso al país: SICAM (Sistema Integrado de Captura Migratoria)	Micro Meso	Agosto de 2020	Torres Gómez (2020)
Filtración de datos personales de la Empresa Camino de las Sierras	20 GB de datos involucrados correspondientes a 54 mil clientes registrados de la Empresa Camino de las Sierras	Base de datos personales de clientes de la empresa Camino de las Sierras S. A.	Micro	Noviembre de 2020	El Doce (2020)
Filtración de datos personales de clientes de sucursales de Easy, Jumbo, Vea y Disco	Clientes de Easy, Jumbo, Vea y Disco (Cencosud cuenta con 8 millones de clientes en Argentina)	Base de datos de clientes del grupo Cencosud S. A.	Micro	Noviembre de 2020	Agencia de Acceso a la Información Pública (2021a)
Filtración de datos personales del Ministerio de Salud de la provincia de San Juan	115.281 personas residentes en San Juan registradas en "Andes Salud".	Sistema Sanitario "Andes Salud"	Micro	Julio de 2020	Agencia de Acceso a la Información Pública (2021b)
Filtración de datos personales y sensibles del RENAPER	60000 registros confirmados. Es posible que se trate de los datos de toda la población argentina	Sistema de Identidad Digital (SDI). Base de datos de RENAPER	Micro Meso Macro	Octubre de 2021	Marquez (2021) Truncado (2021)
"Aníbal Leaks". Filtración de datos de afiliados de la Obra Social de las Fuerzas Armadas (IOSFA)	1.193.316 militares argentinos y empleados de diversas agencias de defensa nacional	Base de datos de IOSFA	Micro	Septiembre de 2021	Reddit (2021)
Robo y filtración de datos personales sensibles de trabajadores del Senado de la Nación Argentina	Trabajadores del Senado de la Nación (5000 trabajadores aprox.)[1]	Base de datos de trabajadores del senado.	Micro	Enero de 2022	D'Imperio (2022)
Filtración de datos personales de Jueces, funcionarios y empleados de la Suprema Corte de Justicia de la Provincia de Buenos Aires	15 mil registros personales de jueces, funcionarios y empleados de la SCJ de la Provincia de Buenos Aires.	Sistema de la Mesa de Entradas Virtual (MEV)	Micro	Julio de 2022	Diario Judicial (2022) Brodersen (2022)
Filtración de usuarios y contraseñas de 256 sitios de Argentina	Usuarios de 256 sitios argentinos	256 sitios argentinos (AFIP, Aplicación Mi Argentina, etc.)	Micro Meso	Marzo de 2022	El Cronista (2022)
Acceso no autorizado al código fuente y base de datos de Mercado Libre y Mercado Pago	300 mil usuarios de Mercado Libre y Mercado Pago	Base de datos de Mercado Libre y Mercado Pago	Micro	Marzo de 2022	Página12 (2022)
Filtración de datos personales y sensibles de OSDE (Organización de Servicios Directos Empresarios)	140 GB de información interna comprometida	Sistemas informáticos de OSDE	Micro	Junio de 2022	Harán (2022)
Filtración de datos personales y sensibles de salud del Hospital Pediátrico Garrahan	5.5GB de bases de datos (12 millones de registros con información de pacientes y tratamientos)	Bases de datos del Hospital Garrahan	Micro Meso	Julio de 2022	Foletti (2022)
Hackeo y filtración de datos personales y sensibles del Poder Judicial de Santa Cruz	Ciudadanos cuyos datos se encuentren en el Poder Judicial de la Provincia de Santa Cruz	Computadora de resguardo (back up) de información que almacena las claves de acceso internos del Poder Judicial	Micro	Septiembre de 2022	TiempoSur (2022)
Filtración de datos personales de clientes de Aerolíneas Argentinas	65 mil correos de clientes de Aerolíneas Argentinas	Base de datos de clientes de Aerolíneas Argentinas	Micro	Octubre de 2022	Urgente24 (2022)

Incidente informático y plataformas involucradas	Cantidad de datos comprometidos y/o población afectada	Sistemas de información involucrados	Tipo de datos vulnerados	Fecha del incidente	Fuente
Hackeo de WhatsApp	2,3 millones de números de teléfono de usuarios de Argentina	Plataforma WhatsApp	Micro	Noviembre de 2022	Alippe (2022); TN (2022)

Fuente: elaboración propia.

Análisis de los casos seleccionados

La lectura de la Tabla 1 permite advertir algunas regularidades. En primer lugar, predominan los incidentes que afectaron a organismos del sector público: ocho de los quince casos corresponden a instituciones estatales nacionales o provinciales (Dirección Nacional de Migraciones, Ministerio de Salud de San Juan, RENAPER, IOSFA, Senado de la Nación, Suprema Corte de Justicia de la Provincia de Buenos Aires, Hospital Garrahan y Poder Judicial de Santa Cruz), a los que se suma una empresa de propiedad estatal (Aerolíneas Argentinas). Los restantes involucran a empresas privadas (Camino de las Sierras, Cencosud, Mercado Libre, OSDE y WhatsApp) y a un conjunto heterogéneo de 256 sitios públicos y privados. Esta distribución es consistente con lo señalado por los informes del CERT.ar, que ubican al Estado entre los sectores más atacados durante 2021 y 2022 (DNCIB, 2022, 2023).

En segundo lugar, se destaca la presencia de datos sensibles. Tres de los casos (Ministerio de Salud de San Juan, OSDE y Hospital Garrahan) comprometieron información sanitaria de pacientes o afiliados, categoría que la Ley 25.326 protege de manera especial, y la filtración del RENAPER afectó a la base sobre la que se sostiene la identificación de toda la población. En todos los casos se comprometieron microdatos, es decir, registros que permiten identificar a cada individuo; en cuatro de ellos, además, los datos permitían individualizar subgrupos poblacionales (datos meso) y, en el caso del RENAPER, la base afectada abarcaba potencialmente al conjunto de la población (datos macro).

En tercer lugar, la distribución temporal muestra una concentración de casos en 2022 (nueve, frente a cuatro en 2020 y dos en 2021). Este dato no contradice la reducción del total de incidentes registrada por el CERT.ar para ese año, sino que se corresponde con el aumento de los incidentes de severidad alta y crítica señalado en sus informes: menos ataques, pero de mayor alcance. Por otra parte, solo en dos de los casos relevados (Cencosud y Ministerio de Salud de San Juan) la fuente disponible es una resolución de la AAIP; en los demás, la información proviene principalmente de medios periodísticos, lo que sugiere una escasa visibilidad pública de las respuestas institucionales ante este tipo de incidentes.

Por último, cabe señalar que buena parte de los datos comprometidos en el sector público (documentos de identidad, registros migratorios, historias clínicas) fue entregada

por los ciudadanos de manera obligatoria o como condición para acceder a servicios esenciales. En estos casos, el margen de acción individual para prevenir el riesgo es muy limitado, lo que refuerza la responsabilidad de las instituciones que administran esas bases de datos.

Conclusiones

El sistema de registro e intercambio de datos, necesario para modelos de negocios y de gestión administrativa característicos del mundo contemporáneo, revela potenciales de perennidad y accesibilidad crecientes. Más personas tienen más acceso a información asociada (de manera correcta o no) a otras personas, y la localización de piezas de información explotables se hace más fácil al encontrarse organizada en bases de datos.

El fenómeno contiene un primer componente de índole puramente material y técnico. Se requieren centros masivos de almacenamiento de datos, como los que sostienen los sistemas de computación gratuita de uso común. Otro componente técnico crucial es la conectividad, que permite acceder y distribuir el contenido, o sea, copiar información de forma redundante. La distribución de una pieza de información puede imposibilitar prácticamente su eliminación u ocultamiento posterior. En la web, la no accesibilidad temporaria de la información no equivale a su eliminación. La distribución amplia permite que un contenido permanezca almacenado en alguna memoria de la que puede retornar a publicidad. Muchos de los mecanismos que utiliza internet para el seguimiento de los usuarios son difíciles de detectar y resistentes al bloqueo y a la eliminación.

Nos interesa enfocarnos en factores de orden social que tienen a los componentes técnicos mencionados como condiciones de posibilidad. Es claro que tales medios técnicos también dependen de sistemas sociales, pero se quiere destacar su condición de meros recursos que pueden insertarse en contextos históricos concretos con resultados variables.

Si bien los modelos de negocios extractivos de datos (como los proveedores de servicios de computación sin abono pago, que obtienen sus dividendos capturando la atención de los usuarios y subastando aspectos de su interfaz al publicista que mejor oferte) suelen invertir recursos considerables en seguridad informática, esa inversión no neutraliza los riesgos que derivan de su propia lógica de funcionamiento. La alta velocidad de circulación de contenidos y la amplia distribución por múltiples equipos, potencia la accesibilidad y perennidad de la información. El impacto en la privacidad, y otras desventajas del modelo de red social son ya de conocimiento masivo, y se han expuesto algunos ejemplos. Pero el fenómeno es más amplio. La recolección, registro,

1 Población estimada en base a las listas de personal permanente, interino y contratado del Senado de la Nación Argentina. Disponible en https://www.senado.gob.ar/recursos-humanos/agente/temporales

almacenamiento y procesamiento de datos son hechos sociales que verificamos hasta en transacciones cotidianas. Parecen configurar, en muchos casos, conjuntos de sistemas plenamente funcionales en el caso de consumidores atentos y cumplimiento adecuado de las regulaciones. Pero existen puntos de fragilidad que generan incentivos para el tráfico de datos con fines explotativos. Los incentivos generados no sólo son de tipo económico. La información puede explotarse de modos tan variados como la propia imaginación humana. Verificamos la existencia de casos de ataques a entidades sociales de gran envergadura como empresas, organizaciones e instituciones del sector público y privado, cuyas consecuencias, en algunos casos, aún se desconocen. Y la proliferación de medios de interacción que presuponen tráfico de datos no ha parado de crecer, al menos en variedad, como lo atestigua la multiplicación de medios de pago electrónico. En cuanto a los modelos de gestión administrativa, es difícil argumentar contra la necesidad de adquirir información para orientar políticas públicas razonables. En el cuerpo del trabajo constan casos de uso de datos oficiales que han significado incrementos en la exposición a daños potenciales o efectivos. La legislación es clara, precisa y, a nuestro juicio, razonable; el problema radica menos en la norma que en su aplicación y en las capacidades institucionales para garantizarla. En la Ley 25.326, el artículo 9, "Seguridad de los datos", establece:

> 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad. (Ley 25.326, 2000, art. 9)

Por supuesto, no es la intención del presente trabajo emitir juicio técnico jurídico alguno relativo a la legislación sobre las cuestiones aquí tratadas. Pero debería llamarse la atención sobre los ritmos relativos a la administración y a la innovación tecnológica, con las brechas que necesariamente aparecen. A priori puede deslizarse la suspicacia de que no necesariamente dependencias estatales contarán con la infraestructura, recursos humanos y de capital, necesarios para hacer frente a ataques suficientemente motivados y equipados.

Hay incentivos externos para explotar datos generados para otros fines. Las ofertas en sitios Web sugieren un mercado bien desarrollado para el tráfico de datos, que puede producir retornos muy altos en escala. Cabe esperar un correlativo aumento de la eficacia en los ataques, parejo a los incentivos.

Ciertos incentivos mercantiles y lastres que ralentizan la gestión pública, sin mencionar connivencias y venalidades, se alinean, en no pocos casos, de maneras que exponen a usuarios y ciudadanos. Los cambios tecnológicos suelen ir más rápido que la legislación, por lo que, quizás, no solamente el refuerzo de supervisiones o prohibicio-

nes regulatorias sino, también, la concientización y educación de los usuarios pueden producir alternativas en defensa de la privacidad. No obstante, como muestran los casos relevados, buena parte de los datos comprometidos fue entregada obligatoriamente al Estado, por lo que la concientización individual no puede sustituir la responsabilidad de las instituciones que los administran. Para ello es necesario que el conocimiento de los peligros y amenazas asociados al uso de esas tecnologías de la información se propague con la misma velocidad que sus usuarios. Pero es difícil clamar melancólicamente sobre privacidad y riesgos cuando multitudes abultan con entusiasmo deportivo la base de datos de la ruina, y colaboran en el ajuste de la retícula táctica más detallada de la historia, lo que convierte a cada cuerpo en un blanco virtual.

Referencias

Abelson, H., Ledeen, K. y Lewis, H. (2008). *Blown to bits: Your life, liberty, and happiness after the digital explosion*. Addison-Wesley. https://www.niemanlab.org/pdfs/blowntobits.pdf

Agencia de Acceso a la Información Pública. (2020). *RESOL-2020-41-APN-AAIP*.

Agencia de Acceso a la Información Pública. (2021a). *RESOL-2021-146-APN-DNPDP#AAIP*. https://www.argentina.gob.ar/sites/default/files/rs-2021-146-apn-dnpdpaaip_censurado.pdf

Agencia de Acceso a la Información Pública. (2021b). *RESOL-2021-64-APN-DNPDP#AAIP*. https://www.argentina.gob.ar/sites/default/files/2021/05/rs-2021-45161366-apn-dnpdpaaip_ministerio_de_salud_san_juan.pdf

Alippe, E. (2022, 25 de noviembre). Masivo hackeo de WhatsApp pone en alerta al mundo: en Argentina habría más de 2 millones de usuarios damnificados. *Vía País*. https://viapais.com.ar/tecnologia/masivo-hackeo-de-whatsapp-pone-en-alerta-al-mundo-en-argentina-habria-mas-de-2-millones-de-usuarios-damnificados/

Arrington, M. (2006, 6 de agosto). AOL proudly releases massive amounts of private data. *TechCrunch*. https://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/

Asociación por los Derechos Civiles y Privacy International. (2017). *El derecho a la privacidad en Argentina. Informe de las partes interesadas. Examen Periódico Universal, 26.º período de sesiones – Argentina*. https://adc.org.ar/wp-content/uploads/2019/06/026-el-derecho-a-la-privacidad-en-argentina-03-2017.pdf

Bañales, J. A. (2006, 10 de agosto). La pública intimidad de los usuarios de AOL. *El Mundo*. https://www.elmundo.es/navegante/2006/8/10/tecnologia/1155202140.html

Barbaro, M. y Zeller, T. (2006, 9 de agosto). A face is exposed for AOL searcher no. 4417749. *The New York Times*. https://www.nytimes.com/2006/08/09/technology/09aol.html

Brodersen, J. (2022, 21 de julio). Ciberdelincuentes subieron datos sensibles de la Suprema Corte bonaerense y los venden online. *Clarín*. https://www.clarin.com/tecnologia/ciberdelincuentes-subieron-datos-sensibles-suprema-corte-bonaerense-venden-online_0_Lmqlo6cy9T.html

Carbajal, M. (2009, 14 de abril). Docente despedida por apóstata. *Página/12*. https://www.pagina12.com.ar/diario/sociedad/3-123204-2009-04-14.html

Carbajal, M. (2020, 30 de septiembre). Orden inédita de habeas data para una persona que apostató. *Página/12*. https://www.pagina12.com.ar/diario/sociedad/3-123204-2009-04-14.html

Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina. (2003). *Diario Oficial de la Unión Europea*, L 168. https://www.informatica-juridica.com/anexos/decision-2003-490-ce-de-la-comision-de-30-de-junio-de-2003-con-arreglo-a-la-directiva-95-46-ce-del-parlamento-europeo-y-del-consejo-sobre-la-adecuacion-de-la-proteccion-de-los-datos-personales-en-arge/

Decisión Administrativa 641/2021. Requisitos mínimos de Seguridad de la Información para Organismos públicos. 25 de julio de 2021. Jefatura de Gabinete de Ministros. https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345

Decreto 746/2017. (2017). *Boletín Oficial de la República Argentina*.

Diario Judicial. (2022, 22 de julio). *Cuidado con los datos de los jueces*. https://www.diariojudicial.com/news-92632-cuidado-con-los-datos-de-los-jueces

D'Imperio, J. (2022, 25 de enero). Ciberataque en el Senado: extrajeron datos personales y los funcionarios siguen sin sistema. *Perfil*. https://www.perfil.com/noticias/actualidad/ciberataque-senado-extrajeron-datos-personales-funcionarios-siguen-sin-sistema.phtml

Dirección Nacional de Ciberseguridad. (2022). *Incidentes informáticos. Informe anual sobre incidentes de seguridad informática registrados en el 2021 por el CERT.ar*. https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f__0.pdf

Dirección Nacional de Ciberseguridad. (2023). *Incidentes informáticos. Informe anual sobre incidentes de seguridad informática registrados en el 2022 por el CERT.ar*. https://www.argentina.gob.ar/sites/default/files/2023/02/informe_cert_2022.docx.pdf

Disposición DNCIB 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos. 19 de enero de 2021. Dirección Nacional de Ciberseguridad. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2021-347311

Disposición DNCIB 1/2022. Aprueba el "Modelo Referencial de Política de Seguridad de la Información". 14 de febrero de 2022. Dirección Nacional de Ciberseguridad. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2022-360957

Disposición DNCIB 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras. 11 de noviembre de 2021. Jefatura de Gabinete de Ministros. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-6-2021-348661

Disposición DNCIB 7/2021. Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional. 12 de agosto de 2021. Dirección Nacional de Ciberseguridad. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-7-2021-353181

Disposición DNCIB 8/2021. Guía Introductoria a la Seguridad para el Desarrollo de Aplicaciones Web. 10 de noviembre de 2021. Jefatura de Gabinete de Ministros. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-8-2021-356582

El Cronista. (2022, 2 de marzo). *Se filtraron miles de usuarios y contraseñas de sitios argentinos: desde AFIP hasta Mi Argentina*. https://www.cronista.com/infotechnology/actualidad/se-

filtraron-miles-de-usuarios-y-contrasenas-de-sitios-argentinos-desde-afip-hasta-mi-argentina-hasta/

El Doce. (2020, 30 de octubre). *Denuncian masiva filtración de datos: Jorge Cuadrado y otras personalidades, en la lista*. https://eldoce.tv/sociedad/denuncian-masiva-filtracion-datos-jorge-cuadrado-otras-personalidades-lista-peaje-caminos-sierras_105175

ERREIUS. (2022b, 12 de septiembre). *Principales puntos del proyecto de reforma de la ley de datos personales*. https://www.erreius.com/opinion/14/civil-persona-y-patrimonio/Nota/844/principales-puntos-del-proyecto-de-reforma-de-la-ley-de-datos-personales

Foletti, N. (2022, 13 de julio). Ciberseguridad: ¿cuál es la gravedad de las filtraciones sufridas por el Hospital Garrahan? *iProUP*. https://www.iproup.com/economia-digital/32826-ciberseguridad-hubo-filtraciones-en-el-hospital-garrahan

Foucault, M. (1975). *Surveiller et punir: naissance de la prison*. Gallimard.

Gillespie, T. (2017). Governance of and by platforms [Preprint]. En J. Burgess, T. Poell y A. Marwick (Eds.), *The SAGE handbook of social media*. SAGE. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/Gillespie-Regulation-ofby-Platforms-PREPRINT.pdf

Harán, J. M. (2022, 12 de agosto). Ransomware LockBit publica información de pacientes y afiliados a obra social OSDE. *WeLiveSecurity*. https://www.welivesecurity.com/la-es/2022/08/12/ransomware-lockbit-publica-informacion-pacientes-afiliados-obra-social-osde/

Le Breton, D. (2021). *Sociología del riesgo* (J. I. Gorrias, Trad.). Prometeo.

Ley 25.326 de 2000. Protección de los Datos Personales. 4 de octubre de 2000. https://www.argentina.gob.ar/normativa/nacional/ley-25326-2000-64790

Lotame. (2018). *What is behavioral targeting?* https://www.lotame.com/what-is-behavioral-targeting/

Marquez, J. (2021, 13 de octubre). El Registro Nacional de las Personas de Argentina sufre una filtración de datos de DNI. *Hipertextual*. https://hipertextual.com/2021/10/filtracion-datos-renaper-argentina

Minuto, M. E. (2021, 27 de abril). El futuro llegó hace rato. La imperiosa necesidad de actualizar la Ley de Protección de Datos Personales de Argentina. *Abogados.com.ar*. https://abogados.com.ar/el-futuro-llego-hace-rato-la-imperiosa-necesidad-de-actualizar-la-ley-de-proteccion-de-datos-personales-de-argentina/28139

Narayanan, A. y Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. En *2008 IEEE Symposium on Security and Privacy* (pp. 111-125). IEEE. https://doi.org/10.1109/SP.2008.33

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, *57*(6), 1701-1777. https://www.uclalawreview.org/pdf/57-6-3.pdf

Ohm, P. (2018). Regulating at scale. *Georgetown Law Technology Review*, *2*(2), 546-556. https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Ohm-pp-546-56.pdf

Página12. (2022, 8 de marzo). *Hackean datos Mercado Libre y Mercado Pago y hay preocupación por la filtración de datos de 300 mil usuarios*. https://www.pagina12.com.ar/406594-hackean-datos-mercado-libre-y-mercado-pago-y-hay-preocupacio

Reddit. (2021, 30 de septiembre). *Filtran datos privados de un millón de efectivos de Seguridad y bautizan al golpe "AnibalLeaks"* [Publicación en r/argentina]. https://www.reddit.com/r/argentina/comments/pypjzp/filtran_datos_privados_de_un_mill%C3%B3n_de_efectivos/

Salganik, M. J. (2018). *Bit by bit: Social research in the digital age*. Princeton University Press.

Secretaría de Innovación Tecnológica del Sector Público. (2022). *Delitos informáticos en Argentina: modalidades detectadas durante la pandemia del Covid-19. Recomendaciones preventivas para los ciudadanos*. https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf

Seltzer, W. y Anderson, M. (2008). Using population data systems to target vulnerable population subgroups and individuals: Issues and incidents. En J. Asher, D. Banks y F. J. Scheuren (Eds.), *Statistical methods for human rights* (pp. 273-328). Springer. http://ndl.ethernet.edu.et/bitstream/123456789/8256/1/50.pdf

Srnicek, N. (2021). *Capitalismo de plataformas* (A. Giacometti, Trad.). Caja Negra.

TiempoSur. (2022, 29 de septiembre). *Hackearon el Poder Judicial de Santa Cruz*. https://www.tiemposur.com.ar/info-general/hackearon-el-poder-judicial-de-santa-cruz

TN. (2022, 25 de noviembre). *Alerta mundial por un masivo hackeo de WhatsApp: hay más de 2 millones de cuentas de Argentina comprometidas*. https://tn.com.ar/tecno/aplicaciones/2022/11/25/alerta-mundial-por-un-masivo-hackeo-de-whatsapp-hay-mas-de-2-millones-de-cuentas-de-argentina-comprometidas/

Torres Gómez, R. (2020, 10 de septiembre). Datos robados sobre migrantes en Argentina son publicados en la deep web. *CriptoNoticias*. https://www.criptonoticias.com/seguridad-bitcoin/datos-robados-migrantes-argentina-son-publicados-deep-web/

Truncado, E. (2021, 23 de octubre). Filtración del Renaper: difunden datos sensibles de 60.000 argentinos y piden cerca de 17 mil dólares por todos los DNI. *Titulares.ar*. https://titulares.ar/filtracion-del-renaper-difunden-datos-sensibles-de-60-000-argentinos-y-piden-cerca-de-17-mil-dolares-por-todos-los-dni-titulares-de-tecnologia/

van Dijck, J., Poell, T. y de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.

Zuboff, S. (2020). *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder* (A. Santos Mosquera, Trad.). Paidós.