GUÍA

para el resguardo de los datos personales en el desarrollo e implementación de Plataformas de Datos Abiertos por parte de los Órganos de la Administración del Estado

Junio
2020

consejo para la Transparencia

Esta guía ha sido elaborada en el marco del Compromiso N°10 del Cuarto Plan de Acción de Gobierno Abierto de Chile 2018 – 2020, denominado "Política de Datos Abiertos y Protección de Datos Personales".

En el desarrollo de este compromiso, el Consejo para la Transparencia organizó, entre los meses de septiembre y diciembre de 2019, paneles de conversación con diversos actores relevantes, tanto desde la perspectiva del acceso a la información pública como de la protección de datos personales, incluyendo órganos y servicios públicos, la academia y organizaciones de la sociedad civil. Estos conversatorios tuvieron por objeto identificar, desde la perspectiva de los actores convocados, las problemáticas, incidencias o riesgos para los datos personales que pueden surgir a partir de los procesos de disponibilización de datos abiertos, junto con determinar las salvaguardas, mecanismos y/o herramientas que se debiesen utilizar en las plataformas de datos abiertos, en orden a garantizar la seguridad y proteger adecuadamente las bases de datos personales administradas por organismos públicos.

Agradecemos los valiosos comentarios y aportes entregados en estos conversatorios por representantes del Ministerio Secretaría General de la Presidencia; Ministerio de Desarrollo Social y Familia; Ministerio de Ciencia, Tecnología, Conocimiento e Innovación; Dirección de Compras Públicas; Servicio de Registro Civil e identificación; Dirección de Presupuestos; Laboratorio de Gobierno; Municipalidad de Puente Alto; Fundación Derechos Digitales; Fundación Datos Protegidos; y, Fundación Abriendo Datos. Asimismo, agradecemos las observaciones y planteamientos formulados por académicos del Instituto Milenio Fundamento de los Datos; Instituto de Data Science de la Facultad de Ingeniería de la Universidad del Desarrollo; Centro de Regulación y Consumo de la Universidad Autónoma; Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile; y, Facultad de Derecho de la Pontificia Universidad Católica de Chile.

consejo para la Transparencia

Contenido

I. Introducción

Nos encontramos insertos en la data-driven society, concepto que hace referencia a un mundo donde la toma de decisiones se basa en el análisis e interpretación de datos. En esta nueva realidad, los datos son considerados intrínsecamente valiosos, permitiendo fortalecer las capacidades de los sujetos y organizaciones que están en condiciones de trabajar con ellos, junto con mejorar la transparencia y rendición de cuentas (accountability) de autoridades, empresas y particulares, tanto respecto a la legitimidad de sus actuaciones, como a la medición de su desempeño en relación a ciertos criterios establecidos[1].

La información del sector público, en vista a su volumen, variedad y carácter centralizado, constituye un recurso de enorme relevancia, especialmente cuando se disponibiliza en formatos libres y reutilizables, bajo la modalidad de datos abiertos. Los datos abiertos del Estado son un medio importante para mejorar el acceso a la información por parte de los ciudadanos y la sociedad civil, promoviendo el crecimiento económico, la investigación científica y la responsabilidad política y empresarial. En este contexto, muchos gobiernos y organismos públicos en el mundo están poniendo a disposición del público general un número cada vez mayor de bases de datos, a través de portales nacionales, regionales, locales o temáticos, sobre la base de compromisos políticos en favor del gobierno abierto y los datos abiertos[2].

Una gran cantidad de los datos almacenados y procesados por el sector público revisten el carácter de datos personales, cuya publicación puede generar un riesgo para la privacidad[3]. Debemos tener presente que los nuevos entornos digitales donde se comunican, almacenan e intercambian los datos han transformado muchas de las formas en que concebimos la privacidad y el acceso a la información en poder de organismos públicos. Por otra parte, en la era de los "gigantes tecnológicos", los gobiernos siguen siendo los principales recopiladores de información sobre sus ciudadanos[4]. El telón de fondo de este nuevo entorno son las tecnologías de análisis de big data, que permiten la continua recopilación y uso instantáneo de grandes cantidades de datos, con propósitos que abarcan desde la elaboración perfiles, targeting, proyecciones, predicciones y evaluaciones de diversa índole, hasta la generación de insumos que faciliten el desarrollo de investigaciones científicas[5].

En este contexto, a nivel internacional, es posible apreciar una creciente preocupación por el debido resguardo de los derechos a la privacidad y a la protección de los datos personales en la implementación, desarrollo y ejecución de sistemas o plataformas que tienen por objeto facilitar el acceso y reutilización de información pública, en formato de datos abiertos. **Uno de los principales desafíos en esta materia es lograr que los principios de acceso a la información pública y protección de datos personales sean compatibilizados. Esto, implica promover la utilidad de los datos, garantizando al mismo tiempo el adecuado cumplimiento por parte de los responsables de las bases de datos del deber de respetar los derechos que la ley reconoce a sus titulares.** Así, se hace necesario contemplar técnicas y herramientas que armonicen la cultura de la transparencia con los principios y obligaciones del derecho a la protección datos personales, permitiendo la publicación y disponibilización segura

[1] Simperl, O'Hara & Gomer, 2016: 4.

[2] Janssen, 2012.

[3] Simperl, O'Hara & Gomer, 2016: 3.

[4] Jaatinen, 2016: 2.

[5] Conroy & Scassa, 2015: 175.

de datos abiertos al público general.

En el tratamiento masivo de datos resulta necesario adoptar medidas que aseguren la confidencialidad de aquella información que reviste el carácter de secreta o reservada. Para ello, se requiere que el sector público utilice modelos y herramientas que permitan identificar previamente los riesgos inherentes a la privacidad y protección de datos personales de un proyecto de datos abiertos en particular, empleando estándares de seguridad técnica y organizativa apropiados.

En definitiva, en el diseño, implementación, desarrollo y operación de soluciones tecnológicas tendientes a la publicación de información del sector público deben considerarse como un pilar fundamental la estricta observancia de los principios, derechos y obligaciones propios de la protección de datos personales, contribuyendo a que los beneficios aparejados al uso de big data, no impliquen una afectación o impacto negativo en los derechos fundamentales de los individuos.

Lo anterior, sobre todo si consideramos que, a partir del año 2018, **el derecho a la protección de los datos personales es reconocido como derecho fundamental en nuestra Constitución Política de la República**, consagrado en el artículo 19 N°4 de la Carta Fundamental.

II. Objetivos

El objetivo de estas guías es presentar algunas directrices a los organismos de la Administración del Estado que desarrollen sistemas o plataformas digitales que permitan al público general acceder, usar y reutilizar la información o datos públicos que generen o administren, en formato de datos abiertos, garantizando que en todas las etapas de sus procesos de disponibilización de datos se dé estricta observancia al estatuto que garantiza los derechos fundamentales a la protección de la vida privada y a la protección de los datos personales.

Para la elaboración de este documento se llevó a cabo un análisis del concepto, características relevantes y principales beneficios de los datos abiertos, junto con una revisión de los marcos regulatorios pertinentes, tanto a nivel nacional como en derecho comparado. Asimismo, se analizó el estatuto de protección a los datos de carácter personal, con especial énfasis en los principios y normas aplicables a los tratamientos de datos efectuados por los organismos públicos. Sobre la base de este marco teórico, se efectuó un diagnóstico de los eventuales riesgos a la adecuada protección de los datos personales que pueden verificarse a consecuencia de los procesos de disponibilización de datos abiertos. El referido análisis se encuentra contenido en el **Informe Técnico de estas guías**.

Las directrices que se presentan a continuación dan cuenta de un enfoque eminentemente proactivo y preventivo, y se elaboraron sobre la base de los principios de privacidad por defecto y por diseño, así como en la necesidad de emplear técnicas y herramientas que permitan la debida anonimización de los datos personales que puedan formar parte de las bases o bancos de datos que se pretende disponibilizar como datos abiertos, evitando cualquier vulneración respecto de los derechos que la Constitución y la Ley N°19.628, sobre Protección de la Vida Privada (LPVP), reconocen a los titulares de datos personales.

III. 11 Guías para el resguardo de los datos personales en el desarrollo e implementación de Plataformas de Datos Abiertos por los Órganos de la Administración del Estado

1. Aplicación de los principios de proporcionalidad y minimización.
2. Elaboración de inventarios o mapas de datos, según taxonomía de datos.
3. Auditorías periódicas de los datos almacenados y sus operaciones de tratamiento.
4. Promover la formación continua.
5. Considerar el "ciclo de vida" de los datos.
6. Desarrollar planes para la implementación de iniciativas de datos abiertos.
7. Realizar evaluaciones de impacto de privacidad y operaciones de análisis de riesgos.
8. Gestionar las brechas de privacidad y protección de datos personales detectadas.
9. Enfoque sistémico para abordar los riesgos a la privacidad y la protección de datos personales.
10. La seguridad informática como elemento principal.
11. Transparencia en las iniciativas de datos abiertos.

1. Aplicación de los principios de proporcionalidad y minimización.

Se sugiere observar de forma estricta los principios de proporcionalidad y minimización, especialmente al momento de recopilar datos personales.

La protección de datos personales constituye un pilar esencial e indispensable de cualquier proceso que implique el tratamiento de bases de datos, como un componente esencial e indispensable. Esto implica para los organismos públicos, la necesidad de proporcionar a los titulares de datos personales **el más alto nivel de protección de sus datos, por diseño y por defecto, lo que debiese hacerse extensivo a todos procesos, protocolos y sistemas de procesamiento de datos que desarrollen o implementen.**

Una importante medida de protección de la privacidad consiste en poner en relieve al interior de los organismos públicos, a todos los niveles, la importancia de limitar la recopilación de información de carácter personal a aquella que resulta **estrictamente necesaria para el cumplimiento de un determinado objetivo o finalidad**[6], y que, **una vez cumplida éste, se proceda a la cancelación o eliminación de los datos**. Así, cobran relevancia los principios de limitación de propósito, proporcionalidad y minimización de datos[7]. La limitación de la finalidad es un principio clave de la protección de los datos, que exige que los datos personales que se han recogido para un fin específico no se utilicen para otro fin incompatible.

Los riesgos para la privacidad y la protección de datos personales se crean, en primer lugar, en el momento en que se procede a recabar los datos: no se puede volver a identificar a los titulares de los datos a menos que se hayan recogido y almacenado datos sobre ellos. **Además, cuantos más datos se reúnan, mayor será la probabilidad de reidentificación, con los consiguientes efectos perniciosos.** Esto es así no sólo en lo que respecta al número de características medidas, sino también al número de registros recopilados. Tan pronto como los datos son recopilados, éstos se ven afectados por los riesgos de acceso no autorizado, uso indebido o filtración, a través de múltiples medios. Por consiguiente, **los responsables del tratamiento deben suponer que cualquier dato que recojan es susceptible de vulnerabilidades, debiendo garantizar cuidadosamente (antes de recopilar información de carácter personal) que los beneficios de la recolección superen los riesgos**[8].

Muchas de la amenazas a la adecuada protección de los datos personales surgen debido a la excesiva recopilación de características personales o registros que no son esenciales para el cumplimiento de las competencias y funciones del responsable del tratamiento. En vista a ello, **los organismos públicos deberían seguir pautas de minimización de datos**, limitando la recopilación de información personal a aquella que sea directamente pertinente y necesaria para lograr un propósito específico.

2. Elaboración de inventarios o mapas de datos, según taxonomía de datos.

Se sugiere la elaboración de inventarios o mapas de datos, clasificando las bases de datos de las cuales el organismo público es responsable, definiendo para ello una taxonomía de datos.

6 Scassa, 2018: 9.

7 GT29, 2013: 7

8 Green et al., 2017: 33.

Con el fin de realizar un adecuado seguimiento de los riesgos para la privacidad y la protección de datos personales en todas las bases de datos almacenadas y administradas por un determinado organismo público, se requiere saber en forma previa qué datos posee la institución y qué riesgos implica su tratamiento. Esto releva la **importancia que las instituciones públicas en general, realicen un catastro de todos los datos que poseen, categorizándolos**[9]. A partir de dicho levantamiento, puede establecerse la existencia de bases de datos que no podrían ser disponibilizadas de forma desagregada en formatos abiertos, en vista al estatuto jurídico que les resulta aplicable.

Asimismo, este proceso de clasificación debe incluir una análisis que permita detallar la situación en que se encuentra cada base de datos, en términos de: responsables y actores implicados: antigüedad y frecuencia de actualización; localización de los datos; formatos y medios de acceso; calidad y fiabilidad; y, medidas de seguridad aplicadas[10].

Los inventarios de datos y los esquemas de clasificación de la privacidad son formas eficaces para determinar los riesgos a la adecuada protección de los datos personales, permitiendo establecer, por ejemplo, la existencia de bases de datos redundantes[11], lo que puede suponer problemas de inconsistencia de información y de seguridad[12].

Por regla general, los organismos públicos mantienen numerosas bases de datos -a menudo distribuidos entre departamentos o áreas funcionales diferentes– de diversa índole. **Sin un conocimiento exhaustivo de las bases de datos disponibles, los organismos pueden tomar decisiones de gestión de datos deficientes o duplicar sus esfuerzos de recolección y procesamiento de información.** Además, los conjuntos de datos desconocidos e insuficientemente supervisados plantean diversas amenazas: no resulta posible mitigar riesgos que nadie sabe que existen. Los datos personales que no se supervisan activamente no podrán ser debidamente resguardados, aumentando la probabilidad que esta clase de información sea publicada como datos abiertos. Adicionalmente, la vertiginosa evolución de los mecanismos de análisis de big data es especialmente preocupante, ya que significa un constante incremento en los riesgos que puedan afectar a un conjunto de datos.

Los inventarios de datos facilitan la tarea de evaluar los riesgos a la privacidad y a la protección de los datos personales dentro de cada conjunto o banco de datos. Un posible enfoque es el desarrollo de esquemas de clasificación que ponderen los riesgos que conlleva cada conjunto de datos en categorías simples, por ejemplo, riesgo alto, medio y bajo. Tal sistema, podría proporcionar una visión general de los riesgos a la privacidad y a la protección de los datos personales de cada base de datos, ayudando a los organismos a dirigir sus recursos a mitigar los riesgos más graves e identificar los conjuntos de datos que son buenos candidatos para ser publicados como datos abiertos[13]. Por consiguiente, se pone énfasis en la importancia que cada institución desarrolle mapas de riesgos de vulneración de datos personales, en orden a facilitar su control. A este respecto, se debe tener presente que ciertos datos, considerados de forma aislada, pueden ser calificados como de bajo riesgo, pero al combinarlos con otros pueden dar indicios de

9 Para ello, resulta recomendable realizar entrevistas con todos aquellos actores que participen en la gestión de información dentro de la organización, personal informático y responsables funcionales de datos (Consejería de Fomento y Medio Ambiente de la Junta de Castilla y León, 2019: 20).

10 Ibid. 20.

11 Green et al., 2017: 36. El concepto de redundancia de datos dice relación con el almacenamiento de la misma información en diferentes bancos de datos, en distintos lugares, debido principalmente a la existencia de descoordinaciones en las actividades de recopilación, almacenamiento y cancelación de datos.

12 Nos referimos a la redundancia no controlada.

13 Ibid. 36 ff.

los hábitos conductuales de ciertos individuos o permitir perfilamientos.

Por otra parte, el balance entre privacidad/protección de datos personales y los intereses públicos que motivan la disponibilización de datos abiertos, puede tener un resultado diferente según el tipo de información de que se trate. Para ayudar a equilibrar los intereses involucrados, puede distinguirse entre cuatro categorías de datos, con niveles dispares de riesgo para la privacidad y la protección de datos personales: a) datos personales brutos; b) datos seudonimizados; c) datos anonimizados; y, d) datos no personales[14].

Los **datos personales brutos** son aquellos datos, relativos a un individuo determinado o determinable, respecto de los cuales no se ha intentado mitigar los riesgos de reidentificación. Entre los ejemplos de datos personales brutos se incluyen los nombres, número de cédula de identidad y las direcciones de correo electrónico personales. **Las iniciativas de datos abiertos no debiesen incluir la publicación de esta clase de datos, a menos que exista una base legal expresa que ordene o autorice su disponibilización al público general.**

Los **datos seudonimizados**, por su parte, constituyen una categoría de dato personal, que, no obstante revestir mayores niveles de seguridad que los datos personales brutos, al no incluir los datos denominativos de un sujeto, reduciendo la vinculabilidad de un conjunto de datos con la identidad original del interesado, se encuentran igualmente sometidos a las reglas contenidas en la LPVP.

El hecho de que los datos personales puedan **anonimizarse**, mediante la aplicación de técnicas que permiten lograr una desidentificación irreversible[15], parece una forma adecuada de lograr un equilibrio entre los intereses de la privacidad y los intereses de los datos abiertos. Por ejemplo, las estadísticas pueden divulgarse a menudo como datos abiertos, siempre que sean anónimos y agregados[16], pudiendo ser revelados con seguridad y sin restricciones de reutilización[17].

Finalmente, los **datos no personales** se encuentran fuera del ámbito de aplicación de la LPVP, de manera tal que, generalmente, puede ser disponibilizados como datos abiertos[18]. Ahora bien, en algunos casos, bases que en principio no contienen datos personales, pueden, luego de un análisis más profundo, tener, a lo menos, información que reviste la calidad de dato mixto[19].

Sobre esta base, los organismos deben decidir, caso a caso, cuándo y bajo qué condiciones puede divulgarse un conjunto de datos, lo que permite la diferenciación que es necesaria para equilibrar los intereses involucrados[20].

14 Zuiderveen Borgesius et al. 2015: 2114.

15 GT29, 2014: 7. Respecto a la irreversibilidad de la desidentificación, se debe tener presente la razonabilidad de los medios usados como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es "razonablemente" imposible, teniendo presente el contexto y las circunstancias particulares de cada caso.

16 Cuanto más agregados y no vinculables sean los datos anonimizados, más segura será su publicación (ICO, 2012: 36).

17 Zuiderveen Borgesius et al. 2015: 2118.

18 Sin embargo, a veces puede haber argumentos no relacionados con la privacidad o la protección de datos personales en contra de la divulgación de datos no personales. Por ejemplo, es posible que alguna información revista el carácter de reservada o confidencial debido a la seguridad del Estado (ibid. 2120).

19 Así, por ejemplo, a veces es difícil separar la información concerniente a una persona jurídica respecto de información sobre personales naturales. Por otra parte, incluso los datos supuestamente no personales pueden proporcionar información sobre un individuo (Ibid. 2121).

20 Ibid. 2125.

3. Auditorías periódicas de los datos almacenados y sus operaciones de tratamiento.

Se sugiere llevar a cabo auditorías periódicas de los datos almacenados y sus operaciones de tratamiento, para asegurar el cumplimiento de estándares adecuados de protección de datos personales.

La evaluación periódica de los enfoques, procedimientos y protocolos aplicables en materia de privacidad y protección de datos personales ayudará a caracterizar y mitigar cualquier riesgo no previsto.

El rápido desarrollo de las herramientas de recopilación y análisis de big data implica una dificultad para determinar a priori todas las vulnerabilidades que pueden afectar a un determinado conjunto de datos, o los riesgos que plantea una iniciativa de apertura de información del sector público. Estos cambios desafían constantemente las definiciones y concepciones acerca de la privacidad, así como sobre los datos que pueden revelarse o liberarse sin afectar los derechos de sus titulares.

Tales cambios pueden provenir de diversas fuentes, por ejemplo, del surgimiento de técnicas de reidentificación más efectivas, aumentando la posibilidad de efectuar inferencias, lo que hace prácticamente insostenibles los enfoques de mitigación anteriores; la disponibilización de nuevos conjuntos de datos (en la misma plataforma de datos abiertos y en otros lugares) que aumentan las posibilidades de reidentificación, mediante el efecto de mosaico[21] (es decir, la vinculación de la información entre conjuntos de datos); la rotación de personal especializado; o los cambios en las estructuras internas que pueden disminuir la capacidad institucional de seguridad informática o la capacidad de gestionar eficazmente la privacidad de los datos.

Por consiguiente, **los organismos públicos debiesen someter sus bases de datos, así como los procesos y protocolos de gestión de dichos bancos, a auditorías periódicas, en orden a garantizar que sus enfoques de protección de datos alcancen niveles adecuados, junto con documentar suficientemente los resultados de esas auditorías, elaborando los respectivos reportes, manteniendo la trazabilidad de las mismas.**

Esto requiere evaluar el desempeño pasado del programa en la protección de la privacidad y los datos personales, así como cualquier cambio que haya ocurrido en el marco institucional de gestión de datos. Estas auditorías ayudarán a los organismos públicos, además, a evaluar el desempeño de su programa de datos abiertos, identificando cualquier modificación o mejora que sea requerida[22].

4. Promover la formación continua.

Se sugiere aumentar la conciencia interna y la atención a los riesgos a la privacidad y a la protección de los datos personales, a través de la formación continua de quienes tengan a su cargo o estén involucrados en operaciones de tratamiento de datos personales.

Resulta fundamental institucionalizar la conciencia respecto del valor intrínseco y la función de la privacidad y la protección de los datos personales en la gestión de cualquier base de datos. De esta forma, surge la necesidad de desarrollar programas que contemplen la capacitación de los funcionarios del organismo responsable del tratamiento, para asegurar que las políticas y prioridades en materia de privacidad se entiendan de manera amplia y con suficiente profun-

21 Green et al., 2017: 20.

22 Ibid. 55.

didad. En este sentido, se debe promover dentro de la organización la existencia de una cultura de la protección de datos personales, a todos los niveles, y con respaldo de los estamentos directivos que permita un enfoque descendente.

La responsabilidad de gestionar la privacidad en los datos se extiende a todas las áreas funcionales, direcciones, departamento y unidades del organismo público, de ahí que **generar equipos y procesos conscientes de la privacidad y la protección de datos personales resulta crucial para manejar satisfactoriamente los diversos riesgos que pueden derivarse de los procesos de apertura de información del sector público.**

La gestión eficaz de la privacidad y la protección de datos personales requiere un centro de decisión en esta materia de carácter multidisciplinario, que abarque colectivamente al organismo y sea capaz de considerar estos elementos en cada decisión relativa a los datos que se procesan[23].

Además, debido a la diversidad de encargados de cada base de datos que puede existir al interior de la organización, estos deben trabajar de forma coordinada, y bajo los mismos protocolos generales. Los organismos públicos deben desarrollar sistemas y procesos integrales, junto con una capacitación adaptada a cada función, para gestionar la privacidad.

En este contexto, resulta **clave la formación adecuada del personal encargado de la gestión y funcionamiento de los portales de datos abiertos**, constituyendo una medida primordial para evitar que se vulneren datos personales cuando se publica información en poder de organismos públicos. Para ello, se deben determinar las capacidades existentes, estableciendo pautas de evaluación, para luego establecer con precisión las necesidades de generación de capacidades.

5. Considerar el "ciclo de vida" de los datos.

En los procesos de apertura de información se debe tener presente todo el "ciclo de vida" de los datos.

La apertura responsable de datos al público implica un proceso mucho más complejo que su simple carga[24]. Así, **las cuestiones vinculadas a la privacidad y a la protección de datos personales deben considerarse en cada etapa del ciclo de vida de los datos, y no sólo al momento de su publicación como datos abiertos.** Los riesgos para la privacidad y la debida protección de los datos personales pueden surgir y verificarse a lo largo de todo el proceso de disponibilización de una base de datos, lo que incluye su recopilación, mantenimiento, agregación, preparación, liberación y eliminación[25].

A este respecto, se debe tener presente que el ciclo de vida de los datos abiertos comprende las siguientes fases[26]:

a. **Recolección o creación de datos.**

b. **Procesamiento de los datos.**

c. **Agregación o combinación de distintas bases o conjuntos de datos.**

d. **Preparación de los datos.** Los datos necesitan un procesamiento especial antes

23 Ibid. 51.

24 Ibid. 32.

25 Ibid. 5.

26 Elaborado a partir de los elementos expuestos en el documento "Open Data Goldbook for Data Managers and Data Holders", elaborado por el European Data Portal.

de su publicación, para mejorar su calidad. A menudo esto implica "limpiar" los datos, eliminar errores, detectar inconsistencias o actualizarlos. Asimismo, la etapa de preparación resulta imprescindible para reducir los riesgos de una eventual afectación de los derechos de los titulares de datos personales, pudiendo incluir el empleo de técnicas adecuadas de anonimización, que aseguren que no se publicarán datos que puedan ser asociados a personas determinadas o determinables[27]. En la preparación de los datos deben tenerse presente las finalidades que se persiguen con su publicación, considerando no sólo los objetivos teóricos que subyacen en la decisión de apertura, sino que también es necesario identificar y evaluar los usos más probables que tendrá esta información una vez disponibilizada[28].

e. **Publicación y disponibilización del conjunto de datos.**

f. **Acceso, reutilización y redistribuición de los datos.**

g. **Monitoreo de los datos abiertos.** Después de la publicación, el organismo debiese monitorear el uso de los datos abiertos, teniendo presente el contexto dentro del cual son disponibilizados. Esto debe hacerse de forma activa, involucrando a los interesados en el programa de divulgación de datos abiertos, para llevar a cabo un análisis informado[29], teniendo en cuenta los riesgos adicionales que se identifiquen. Se recomienda que los administradores de datos abiertos consulten constantemente con expertos en materia de privacidad y protección de datos personales, así como con posibles consumidores/usuarios de datos abiertos[30].

h. **Gestión de riesgos y respuesta a incidentes.** Los responsables deben establecer protocolos de respuesta para gestionar y mitigar las consecuencias de vulnerabilidad en materia de protección de datos personales, en caso de que surjan incidentes tras la publicación de una base de datos abiertos. Ello podría incluir la modificación, o incluso el retiro, del conjunto de datos publicado, notificando a los terceros que estén utilizando esos datos (cuando sea posible). Asimismo, debiese contemplarse mecanismos de notificación a las personas que, a raíz de estos riesgos o incidentes, puedan verse afectadas en sus derechos.

i. **Cancelación de los datos.** La última etapa del ciclo de vida de los datos es la eliminación de los mismos. Esto implica retirar los datos de las plataformas de datos abiertas. Pueden existir diversas razones para proceder a cancelar estos datos, las que muchas veces son consecuencia de procesos de evaluación posteriores a su disponibilización, por ejemplo, las probabilidades de hacer inferencias sobre sujetos identificables o,

27 La preparación de los conjuntos de datos que se han de divulgar es uno de los retos más comunes a los que se enfrentan las iniciativas de datos abiertos, ya que no siempre está claro si los datos plantean riesgos para la privacidad y, en caso afirmativo, cómo gestionar esos riesgos (Green et al., 2017: 40).

28 Por ejemplo, cuanto más relevantes sean los datos para aspectos claves de la participación democrática, más fuertes serán los argumentos para su divulgación como datos abiertos. Por tanto, al decidir si se liberan los datos personales, la transparencia política tendría más peso que los intereses puramente comerciales de los reutilizadores (Zuiderveen Borgesius et al. 2015: 2127).

29 GT29, 2013: 7.

30 Wood et al., 2016, 11.

más grave aún, que el conjunto de datos permita la reidentificación de personas.

6. Desarrollar planes para la implementación de iniciativas de datos abiertos.

Se sugiere desarrollar planes para la implementación de iniciativas de datos abiertos, que presten igual atención tanto a los objetivos o resultados propuestos, como a los procesos mismos de apertura de datos.

Los planes integrales para la implementación de iniciativas o plataformas de datos abiertos, deben contemplar, al menos, las siguientes etapas secuenciales[31]:

a. Levantar mapas de información o inventarios de bases de datos que serán objeto de apertura, analizando la situación en la que se encuentra cada una de ellas.

b. Determinar el marco legal y normativo aplicable a las bases de datos en cuestión, junto con analizar las normas técnicas y guías que documenten los procedimientos a partir de los cuales éstas serán manejadas.

c. Establecer el marco organizativo para gestionar la iniciativa, fijando tareas, procesos internos y centros de responsabilidad.

d. Modelar y representar la plataforma, teniendo presente el potencial valor y utilidad del catálogo de datos que será abierto.

e. Determinar el ecosistema tecnológico que será utilizado.

f. Establecer un plan de difusión, sensibilización y participación durante la reutilización de los datos.

g. Mantener una estrategia de datos abiertos, lo que incluye el soporte de la plataforma (que permita corregir eventuales problemas), junto con su monitorización y revisión.

Al desarrollar estos planes, **los organismos encargados de disponibilizar datos abiertos no deben centrarse únicamente en el eventual impacto positivo de una iniciativa de apertura de información, sino que también en la implementación de medidas eficaces y controles que reduzca al mínimo una posible afectación del derecho a la protección de datos personales y a la privacidad**[32]. De este modo, se sugiere desarrollar estructuras y procesos operativos suficientemente estandarizados y reflexivos, que codifiquen la adecuada gestión de la privacidad y la protección de datos personales en las iniciativas de disponibilización de datos abiertos.

Se debe tener presente que en el área de la seguridad de la información se han elaborado normas basadas en procesos, que hacen hincapié en mejores prácticas para gestionar y minimizar los riesgos de incumplimiento, y evaluar los esfuerzos en base a su adhesión a estos procesos más que en relación a resultados particulares[33].

En definitiva, se deben **diseñar procesos coherentes de gestión de datos para evaluar continuamente los riesgos y beneficios de la apertura de datos.** A fin de asegurar el cumplimiento continuo de estos procesos

31 Consejería de Fomento y Medio Ambiente de la Junta de Castilla y León, 2019: 19 ff.

32 Green et al., 2017: 32.

33 Ibid. 49.

dentro del ecosistema de privacidad y protección de datos personales -que evoluciona rápidamente-, los organismos públicos debiesen examinar periódicamente sus prácticas en materia de apertura de datos, evaluando riesgos y beneficios[34].

Finalmente, se recomienda incorporar a los usuarios de datos abiertos en la toma de decisiones respecto a contenidos y formatos de publicación, a partir de su experiencia de usabilidad, generando canales que permitan recibir retroalimentación (por ejemplo, sobre problemas en la interoperabilidad de la información que se publica, lo que puede afectar su reutilización). De este modo, podría mejorarse la disponibilidad de los datos, rediseñando las plataformas en base a la demanda y recomendaciones de los usuarios. Asimismo, el mantenimiento de mecanismos continuos de diálogo con las partes interesadas puede ayudar al responsable del tratamiento a identificar no sólo si los datos son adecuados para los fines propuestos, sino que también para detectar posibles usos indebidos o amenazas emergentes, como filtraciones de datos personales o, respecto de aquellos datos que han sido sometidos a algún proceso de anonimización, eventuales riesgos de desanonimización.

7. Realizar evaluaciones de impacto de privacidad y operaciones de análisis de riesgos.

Se sugiere realizar evaluaciones de impacto de privacidad y operaciones de análisis de riesgos, que informen el diseño e implementación de programas de datos abiertos.

La apertura responsable de datos requiere un análisis exhaustivo de los riesgos para la privacidad que conlleva, considerando cuidadosamente el impacto potencial en los interesados[35]. De esta forma, en los procesos de disponibilización de datos abiertos se deben identificar los riesgos inherentes involucrados, así como los controles de privacidad y seguridad adecuados para mitigar estos riesgos. Sólo será posible analizar y elegir los mejores métodos y técnicas de mitigación de riesgos una vez realizada la evaluación de las repercusiones que el proceso de apertura de datos tendrá en materia de privacidad y protección de datos personales[36].

La evaluación de los impactos en la privacidad y la protección de datos personales a lo largo de la vida de un conjunto de datos, y no sólo en el momento de su publicación, es ahora una práctica óptima en materia de datos abiertos[37], insertándose dentro de un enfoque proactivo y no reactivo; preventivo más que correctivo. Así, **estas evaluaciones deben realizarse siempre antes de disponibilizar, en formatos abiertos y reutilizables, cualquier información del sector público que pudiese contener datos personales, y aun cuando la base en cuestión aparentemente no incluya datos personales. De lo contrario, el responsable del tratamiento podría no identificar los conjuntos de datos que incluyen indirectamente información de carácter personal.**

A este respecto, se debe adoptar un enfoque basado en las cualidades y atributos de los datos que se gestionan, lo que permite identificar de mejor forma eventuales vulnerabilidades, las fuentes de los riesgos (que pueden ser multifactoriales) y las medidas para abordarlos, gestionarlos y mitigarlos. Luego, será posible asignar a cada amenaza un valor de probabilidad

34 Ibid. 5.

35 GT29, 2013: 6 ff.

36 Jaatinen, 2016: 5.

37 Scassa, 2018: 7.

de ocurrir, y un valor de impacto probable si llegase a ocurrir[38].

Los organismos deben identificar nuevos riesgos y evaluar regularmente los riesgos residuales, teniendo presente elementos contextuales relevantes (por ejemplo, naturaleza de los datos originales, los mecanismos de control que se hayan implementado, el tamaño de la muestra o la entrega prevista de los datos a terceros), valorando si los controles para la identificación de riesgos son eficaces, y procediendo a su modificación si fuera necesario[39].

8. Gestionar las brechas de privacidad y protección de datos personales detectadas.

Se sugiere gestionar y mitigar oportunamente las brechas de privacidad y protección de datos personales detectadas, empleando herramientas técnicas adecuadas.

A partir de las evaluaciones de impacto de privacidad y de análisis de riesgos, se podrán establecer medidas de gestión y mitigación apropiadas, tales como la eliminación de los campos que contengan datos personales o de los registros que resultan particularmente complejos de filtrar (ya sea por los tipos de datos que presentan o por sus características propias, que hacen más fácilmente identificables a los titulares de datos); **o, el empleo de mecanismos de anonimización, sean de aleatorización o de generalización.**

Entre las técnicas de anonimización, puede destacarse:

a. La agregación de datos, esto es, resumir los datos de un grupo o población y publicar un informe de esas estadísticas, sin divulgar datos personales brutos.

b. La adición de ruido a los datos (también conocido como "perturbación aleatoria), ajustando los datos con aleatoriedad para compensar su información original, de manera tal que el nivel de protección de la privacidad aumenta a medida que se añade más ruido a un conjunto de datos.

c. La permutación de datos, esto es, intercambiar los valores contenidos en el conjunto de datos, trasladándolos de un registro a otro, para que algunos de ellos puedan vincularse artificialmente a distintos interesados.

d. La creación de identificadores anónimos, reemplazando los atributos con códigos generados aleatoriamente y que no tienen ninguna conexión subyacente con el atributo que reemplazan.

e. El empleo de técnicas de privacidad diferencial, entendida como un estándar de seguridad que proporciona una garantía demostrable de privacidad contra una amplia gama de posibles ataques[40].

f. La adopción de técnicas de k-anonimización[41].

38 Green et al., 2017: 12.

39 GT29, 2014: 27.

40 Estos modelos, mediante fórmulas matemáticas, permiten recopilar y compartir información agregada, manteniendo la privacidad de los titulares de dichos datos. Estas herramientas disminuirían la probabilidad de identificar personas en el análisis de los datos, sin modificar los resultados generales del análisis. No obstante lo anterior, se trataría de una herramienta tecnológicamente muy costosa.

41 Ibid. 26 ff.

Adicionalmente, es importante **establecer protocolos de anonimización**, que permitan decidir sobre el nivel de analítica que se podrá llevar a cabo respecto de la base de datos que se disponibiliza. Así, los responsables del tratamiento de los datos deben centrar su atención en los medios concretos que serían necesarios para revertir la técnica de anonimización empleada, teniendo presente los costos y a los conocimientos asociados al uso de dichos medios, evaluando la probabilidad de su uso. Aquí, cobra relevancia el concepto de "esfuerzo razonable de reidentificación", el que depende del estado de la técnica y de su evolución en el corto-mediano plazo (el riesgo de reidentificación puede aumentar con el tiempo, según el grado de desarrollo de las tecnologías de la información y la comunicación)[42]. A dicho respecto, pueden establecerse **tres criterios que permiten asegurar que un conjunto de datos se encuentra efectivamente anonimizado:**

- **Individualización:** no debe ser posible aislar a un individuo en el conjunto de datos.

- **Correlación:** no debe ser posible vincular conjuntos separados de datos relativos a un mismo individuo.

- **Inferencia:** no debe ser posible inferir, casi con certeza, nueva información sobre un individuo[43].

Un mecanismo que se puede utilizar para evaluar la efectividad de las medidas o herramientas de mitigación de los riesgos de privacidad que han sido implementadas consiste en llevar a cabo, antes de compartir o publicar la información en cuestión, ejercicios internos de reconstrucción de datos, denominados "evaluaciones de riesgos de reidentificación", detectando oportunamente la persistencia de ciertas vulnerabilidades que incidan en la adecuada protección de aquella información que revista la calidad de dato personal, considerando factores como otros datos disponibles y que podrían vincularse con el conjunto de datos que se disponibiliza; la probabilidad de que se intente una reidentificación; y, la probabilidad de que la reidentificación, si se intenta, tenga éxito, considerando la eficacia de las técnicas de anonimización propuestas[44].

Dentro de este enfoque, cobran relevancia las "pruebas de penetración", desarrolladas en el contexto de la seguridad de la información para probar la solidez de los sistemas informáticos, tratando explícitamente de encontrar y explotar eventuales riesgos. Al realizar internamente pruebas de penetración, los administradores de sistemas de seguridad de los datos pueden identificar y remediar, en tiempo y forma, cualquier problema subyacente en algún programa informático. De este modo, es posible que los responsables del tratamiento empleen una aproximación similar en los procesos de disponibilización de datos abiertos, a través de sus departamentos o unidades especializadas internas, o en asociación con la academia u organizaciones de la sociedad civil del área tecnológica, llevando a cabo pruebas de reidentificación de los individuos a quienes conciernen un determinado conjunto de datos.

En caso que luego de la apertura y disponibilización de un conjunto de datos se materialice el riesgo de reidentificación de los mismos, el organismo responsable de la respectiva base debe tener la capacidad de apagar su alimentación, eliminándolos del sitio web de datos abiertos[45].

42 GT29, 2014: 9 ff.

43 CNIL, 2020.

44 GT29, 2013: 14.

45 GT29, 2013: 18.

Finalmente, cuando no sea posible anonimizar los datos, debiese optarse por entregar información estadística agregada, en formato de tablas o gráficos.

9. Enfoque sistémico para abordar los riesgos a la privacidad y la protección de datos personales.

El enfoque para abordar los riesgos a la privacidad y a la protección de datos personales debe ser sistémico y no descansar únicamente en intervenciones individuales.

En términos generales, los organismos públicos deben concebir sus sistemas de procesamiento de datos personales como sistemas funcionales eficaces y eficientes tanto respecto de su propósito principal (el cumplimiento de su mandato legal), como respecto del derecho constitucional a la protección de datos personales, los que deben coexistir balanceadamente, estableciendo enfoques sistémicos para el adecuado manejo de bases de datos personales.

La gestión efectiva de la privacidad y la protección de los datos personales es esencial para maximizar los beneficios de los datos abiertos. Por consiguiente, se pone en relieve -más allá de las iniciativas de datos abiertos- la importancia de **generar modelo integrales y comprehensivos para la administración responsable de la información por parte de los organismos públicos, entendido como un aspecto relevante de su marco operacional**. Como contrapartida, se deben evitar modelos de gobernanza de datos fragmentados, donde no existen centros de decisión (a nivel directivo) o procesos unificados de gestión y control.

Entre los principales elementos de estos enfoques holísticos, se destacan la adopción de procesos de categorización y estructuración de bases de datos, con la generación de taxonomías de datos; la operativización, en todas las áreas que trabajen con datos, de los principios de privacidad por diseño y por defecto; la realización de evaluaciones de riesgos de privacidad suficientemente documentados; la incorporación de medidas de seguridad adecuadas, estableciendo protocolos, permisos y perfiles de acceso, junto con la aplicación de funciones de enmascaramiento de datos (incorporando procedimientos que permitan su trazabilidad); y, la implementación de procesos seguros de comunicación o transmisión de datos, aplicando herramientas de encriptación.

Al implementar estos enfoques, se deben tener especialmente presente las peculiaridades de la institución en cuestión y de las operaciones de tratamiento de datos que realiza. Así, por ejemplo, las organizaciones que anonimizan los datos personales requieren una estructura de gobierno eficaz y comprehensiva, que abarque aspectos como la responsabilidad de autorizar y supervisar el proceso de anonimización; la formación continua del personal; el desarrollo de procedimientos para identificar casos en los que la anonimización puede ser problemática o difícil de lograr en la práctica; la gestión de conocimientos sobre cualquier nueva orientación que permita aclarar el marco técnico y jurídico que rodea a la anonimización; y, la revisión de las consecuencias de los programas de anonimización, particularmente a través del análisis de cualquier retroalimentación que se reciba sobre ello[46].

46 ICO, 2012: 39 ff.

10. La seguridad informática como elemento principal.

La seguridad informática debe estar en el centro del desarrollo de las iniciativas de datos abiertos.

Los organismos públicos deben proteger el ciclo completo del procesamiento de datos personales, desde su diseño, implementación y operación, adoptando las medidas necesarias para garantizar la seguridad de la información (lo que comprende su integridad, confidencialidad y disponibilidad), tales como el uso de cifrado en todo momento, la anonimización temprana, la definición de roles de acceso a datos, la destrucción segura de datos y el establecimiento de mecanismos para implementar el ejercicio de derechos de los titulares y el control de los datos por sus titulares.

Como extensión de lo anterior, los portales o plataformas digitales de datos abiertos deben abordar suficientemente aspectos vinculados a las capas básicas de seguridad que debiesen estar presentes en dichos sistemas, empleando herramientas y configuraciones tecnológicas que prevengan eventuales vulneraciones al derecho a la protección de datos personales.

Así, **se recomienda implementar, desde el diseño de las plataformas de datos abiertos, medidas de seguridad técnicas y organizativas que permitan resguardar suficientemente los datos personales, lo que comprende medidas tecnológicas, protocolos, ámbitos normativos, seguridad física y técnica, entre otros.**

De igual manera, se debe tener presente la importancia de emplear tecnologías de encriptación de datos en el procesamiento y comunicación de datos personales, especialmente entre organismos públicos.

11. Transparencia en las iniciativas de datos abiertos.

Los organismos públicos deben ser transparentes y responsables respecto a todas las prácticas relacionadas con sus iniciativas de datos abiertos.

En términos generales, los organismos públicos deben ser suficientemente transparentes respecto a sus sistemas de procesamiento de datos personales, informando a los titulares sobre la recolección, procesamiento, eventual comunicación y purga de datos, a través de políticas legibles de protección de datos personales y mecanismos de notificación a titulares.

Para promover los objetivos vinculados con la efectiva rendición de cuentas en materia de datos abiertos, los organismos públicos deber ser transparente sobre esta clase de decisiones[47], compartiendo, entre otros elementos, los modelos, sistemas y metodologías empleadas, junto con las herramientas de gestión de riesgos. Estos objetivos deben estar presentes en todas las etapas del programa de datos abiertos, siendo necesario documentar cuidadosamente estas prácticas, asegurándose que todas las descripciones sean accesibles para los no expertos[48]. Si bien nos encontramos frente a temáticas difíciles de explicar a la ciudadanía, se afirma la importancia de realizar procesos de pedagogía social y difundir entre el público general la existencia de plataformas de datos abiertos, así como también de sus objetivos y características relevantes.

Así, **los organismos deben ser abiertos y transparentes en cuanto a los datos abiertos que procesan y publican**, informando, por ejemplo, sobre cómo se han anonimizado los datos (si es que lo han hecho) u otras medidas de seguridad que se han aplicado para

47 Green et al., 2017: 6.

48 Ibid. 83.

resguardar la privacidad y la protección de los datos personales, junto con informar con claridad su calidad de entidad administradora y responsable de los datos disponibilizados.

De igual manera, resulta relevante **explicar al público por qué se están cancelando ciertos datos**, dejando claro, por ejemplo, que se están eliminando para proteger la privacidad, en lugar de subvertir la transparencia, y aclarar el calendario aplicable a los procesos de cancelación[49].

49 Ibid. 47.

IV. Documentos consultados

Agencia Española de Protección de Datos – AEPD (2019a): “Guía de Privacidad desde el Diseño”. Disponible [en línea]: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Agencia Española de Protección de Datos – AEPD (2019b): “Nota Técnica: La K-Anonimidad como medida de la privacidad”. Disponible [en línea]: https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf

Cavoukian, Ann (2011): “Privacy by Design. The 7 Foundational Principles”. Disponible [en línea]: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Comité Europeo de Protección de Datos – CEPD (2019): “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”. Disponible [en línea]: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

Commission Nationale de l’Informatique et des Libertés - CNIL (2020): “L’anonymisation de données personnelles”. Disponible [en línea]: https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

Conroy, Amy & Scassa, Teresa (2015): “Promoting transparency while protecting privacy in open government in Canada”, en Alberta Law Review, Vol 53, N°1, pp. 175-206.

Consejería de Fomento y Medio Ambiente de la Junta de Castilla y León (2019). “Open Data. Publicación y reutilización de Datos Abiertos como iniciativa de Gobierno Abierto en la Administración”. Disponible [en línea]: https://datos.gob.es/es/documentacion/open-data-publicacion-y-reutilizacion-de-datos-abiertos-como-iniciativa-de-gobierno

Digital Science (2019): “The State of Open Data 2019. A selection of analyses and articles about open data, curated by Figshare”. Disponible [en línea]: https://digitalscience.figshare.com/articles/The_State_of_Open_Data_Report_2019/9980783#:~:text=A%20formal%20account%20of%20an,any%20other%20type%20of%20information.&text=The%20State%20of%20Open%20Data%202019%20report%20is%20the%20fourth,articles%20from%20global%20industry%20experts.

Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.

Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público.

Directiva 2019/1024/UE del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público.

European Data Portal (2018): "Open Data Goldbook for Data Managers and Data Holders. Practical guide-book for organisations wanting to publish Open Data". Disponible [en línea]: https://www.europeandataportal.eu/sites/default/files/european_data_portal_-_open_data_goldbook.pdf

G8 Open Data Charter. Disponible [en línea]: https://www.gov.uk/government/publications/open-data-charter/g8-open-data-charter-and-technical-annex

Green, Ben et al. (2017): "Open Data Privacy", Research Publication N° 2017-1, The Berkman Klein Center for Internet & Society Research Publication Series.

Grupo de Trabajo del Artículo 29 - GT29 (2013): "Opinion 06/2013 on Open Data and PSI Re-use".

Grupo de Trabajo del Artículo 29 - GT29 (2014): "Dictamen 05/2014 sobre técnicas de anonimización".

Halonen, Antti (2012): "Being Open about Data: Analysis of the UK Open Data Policies and Applicability of Open Data", The Finnish Institute in London. Disponible [en línea]; http://www.fininst.uk/wp-content/uploads/2017/09/being-open-about-data.pdf

Information Commissioner's Office - ICO (2012): "Anonymisation: managing data protection risk". Disponible [en línea]: https://ico.org.uk/media/1061/anonymisation-code.pdf

Information Commissioner's Office – ICO (2019): "Guide to the General Data Protection Regulation (GDPR)". Disponible [en línea]: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Instructivo Presidencial N° 005 de 2012, que imparte instrucciones sobre Gobierno Abierto.

Janssen, Katleen (2012). "Open Government Data and the Right to Information: Opportunities and Obstacles", en The Journal of Community Informatics, 8(2).

Jaatinen, Tanja (2016): "The relationship between open data initiatives, privacy, and government transparency: a love triangle?", en International Data Privacy Law, Volume 6, Issue 1, February 2016, pp. 28–38.

Open Data Charter (2015). Principios carta internacional de datos abiertos. Disponible [en línea]: https://opendatacharter.net/principles-es/

Pagallo, Ugo & Eleonora Bassi (2013): "Open Data Protection: Challenges, Perspectives, and Tools for the Reuse of PSI", en Digital Enlightenment Yearbook 2013, editado por Mireille Hildebrand, Kieron O'Hara y Michael Waidner, IOS Press, Amsterdam, pp. 179-189.

Scassa, Teresa (2018): “Public draft: Open Data & Privacy”, en The State of Open Data, editado por Tim Davies, Stephen Walker, Mor Rubinstein y Fernando Perini.

Simperl, Elena, O’Hara, Kieron & Gomer, Richard (2016): “Analytical Report 3: Open Data and Privacy”, European Data Portal.

Unidad de Modernización y Gobierno Digital, Ministerio Secretaría General de la Presidencia (2013). “Norma Técnica para Publicación de Datos Abiertos en Chile”.

Viollier, Pablo (2017): “El Estado de la Protección de Datos Personales en Chile”, Derechos Digitales. Disponible [en línea]: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

Wiebe, Andreas & Dietrich Nils (2017): “Open Data Protection. Study on legal barriers to open data sharing – Data Protection and PSI”, Universitätsverlag Göttingen.

Wood, Alexandra, O’Brien, David & Gasser, Urs (2016): “Privacy and Open Data Research Briefing”, Networked Policy Series, Berkman Klein Center Research Publication No. 2016-16.