

PRIVACIDAD DESDE EL DISEÑO EN EL REGISTRO UNICO DE BENEFICIARIOS FINALES

Augusto Ho.¹

Sumario. -1.- Introducción. 2.- Privacidad desde el Diseño. 3.- Registro de Beneficiarios Finales. 3.1.- Datos sobre Beneficiarios Finales. 4.- Conclusiones. Bibliografía.

Palabras Clave: Privacidad desde el diseño. Beneficiario final. Personas jurídicas. Personas naturales. Datos personales. Panamá.

Abstract: El presente artículo aborda la necesidad de compatibilizar la legislación aprobada en la República de Panamá en relación con la creación del Registro Único de beneficiarios finales con la Ley N° 81 de protección de datos personales que entrará en vigencia en marzo de 2021.

Se analizan los principios de la privacidad desde el diseño en el entendido que la reglamentación de la Ley N° 129, de 2020, debería considerarlos en tanto implicará un mecanismo de adecuada ponderación en la necesidad de resguardar el equilibrio imprescindible entre la protección de la información personal, manifestación de la dignidad humana y la transparencia del sistema financiero, manifestación imprescindible de los principios republicanos.

1.- Introducción

A inicios de este año 2020 se promulgó en la República de Panamá, la Ley N° 129, de 17 de marzo de 2020, G.O. 28985-C, por la que se “crea el Sistema Privado y Único de

¹ Licenciado en Derecho y Ciencias Políticas por la Universidad de Panamá. Maestría en Derecho Comercial y Maestría en Derecho Civil, ambas por la Universidad Latinoamericana de Ciencia y Tecnología de Panamá. Catedrático de Informática Jurídica y Derecho Informático desde 1993. Director del Instituto de Derecho y Tecnologías de la Universidad Santa María la Antigua (USMA). Socio Director de Prudensdata, empresa dedicada a prestar servicios de gobierno de la información con especial foco en protección de datos personales. Presidente electo de LACRALO, unidad regional para América Latina y el Caribe de ICANN.

Registro de Beneficiarios Finales de Personas Jurídicas”.

Los beneficiarios finales” (BF), también denominados “beneficiarios efectivos” o “titulares o propietarios reales”, o en inglés “*ultimate beneficial owners (UBO)*” o simplemente “*beneficial owners (BO)*” ha venido cobrando importancia a nivel internacional debido a su rol central para la transparencia e integridad del sector financiero.

La noción de beneficiario final tiene su origen en el **trust** anglosajón, en que coexisten “dos derechos de propiedad sobre el mismo bien: la propiedad legal de los bienes en fiducia (que recae sobre el fiduciario) y la propiedad efectiva o final (que recae sobre los beneficiarios).

La motivación que subyace la aprobación de esta norma es la existencia de múltiples compromisos internacionales asumidos por la República de Panamá y que, por tanto, más temprano que tarde harían imperativo iniciar el cumplimiento.

La Ley textualmente indica que su objeto es establecer el marco regulatorio para la creación del sistema privado y único de registro de beneficiarios finales en la República.

Su finalidad está sindicada por la necesidad de facilitar el acceso sobre beneficiarios finales de personas jurídicas recabados por los abogados o firmas de abogados que presten servicios de agentes residentes a efectos de asistir a la autoridad competente en la prevención de delitos de blanqueo de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, de acuerdo con las disposiciones normativas vigentes en la República.

La Ley pretende elevar el nivel de transparencia de las personas jurídicas de diferente índole, permitiendo conocer quién o quiénes son las personas naturales que realmente son beneficiarias de éstas.

Tiempo atrás, el gremio de abogados efectuó variados e interesantes cuestionamientos, particularmente, porque se iniciaría un nuevo período en el que las figuras del anonimato, protección de patrimonios e inversiones discretas cambiaban su sentido y funcionalidad. Ahora bien, algunos profesionales también cuestionaron la robustez del sistema desde los diferentes puntos de vista: técnico, protección y privacidad de los datos solicitados o lo adecuado de su utilización.

Por lo anterior, ya aprobada la norma jurídica corresponde reglamentarla y desarrollar algunos aspectos en ella contemplados en concordancia con la Ley N° 81, de 2019 sobre protección de datos personales, la que entrará a regir en el próximo mes de marzo de 2021.

Este análisis, en consecuencia, toma en consideración ambas normas jurídicas (La Ley N° 129 y la Ley N° 81) y pretendiendo explicitar la necesidad de aplicar a la reglamentación de la primera, los principios fundacionales de la Privacidad desde el Diseño (PbD por sus siglas en inglés).

2.- Privacidad desde el diseño

La Privacidad desde el Diseño “promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización”². De ahí que, desde antes que se recolecte información y durante todo su ciclo de vida, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con la finalidad de evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad e incluso, tratamientos indebidos de datos personales. Incluso un paso más indicaría la necesidad de que la ética desde el diseño y por defecto también sean incluidas, de forma tal de irradiar los procesos de exportación de datos, verificándose en consecuencia, su condición de parte del ADN de cualquier aspecto relacionado con las diferentes actividades que impliquen tratamiento de información personal.

El concepto de protección de datos desde el diseño no es necesariamente nuevo; existe desde hace más de 20 años y mayormente es utilizada la terminología de “*privacy by design*”.

Fue desarrollado por Ann Cavoukian, Comisionada de Protección de Datos de Ontario, en la década de los años 90 y fue presentado en la trigésima primera (31ª) Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 bajo el título “*Privacy by Design: The Definitive Workshop*” siendo posteriormente

² Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: <http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf> (último acceso: 27/12/2020).

aceptado internacionalmente en la trigésima segunda (32ª) Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, celebrada en Jerusalén en el año 2010, con la aprobación de la “Resolución sobre la Privacidad por Diseño”.

Básicamente en esta resolución se reconocía la importancia de incorporar los principios de privacidad dentro de los procesos de diseño, operación y gestión de los sistemas de la organización para alcanzar un marco de protección integral en lo que a protección de datos personales se refiere.

Gracias al acelerado avance de las tecnologías de la información, y tomando en cuenta que cada vez las personas son más propensas a entregar sus datos tanto a las empresas como a las diferentes entidades públicas, aparece como imprescindible considerar que la protección de datos y la privacidad están unidas en todo el ciclo de vida de la información que se vincula con las tecnologías.

Siendo así, es, por tanto, fundamental la consideración de este ciclo de vida desde el momento mismo de la concepción del sistema, considerando a la privacidad en su diseño hasta su definitiva utilización por el público general.

Tradicionalmente la práctica en el diseño de un nuevo producto o servicio consistía en lanzarlo al mercado y posteriormente analizar las diversas situaciones jurídicas que se pudieren presentar, una vez en funcionamiento.

Sin embargo, este nuevo concepto indica que se debe abordar la cuestión técnica y tener en cuenta no solamente las disposiciones normativas sino los principios de privacidad y protección de la información personal, desde el momento mismo del diseño de la *app* o *software*, y no así a posteriori de su incursión en el mercado.

La privacidad nace en el diseño, antes que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida completo de los datos. Considérese además que, la privacidad por defecto implica que solo son objeto de tratamiento aquellos datos personales que sean necesarios para cada una de las finalidades específicas del tratamiento. Y esta debe adicionarse a la privacidad desde el diseño.

Por lo tanto, debe considerarse que su idea base radica en garantizar la privacidad del usuario desde el diseño tecnológico del producto o servicio en forma consistente con la arquitectura del sistema de información y con el modelo de negocios.

Esta corriente considera que el respeto por la privacidad de los usuarios o clientes de productos o servicios tecnológicos, no puede ni debe resignarse únicamente al cumplimiento de los marcos regulatorios, sean jurídicos o técnicos, sino que la garantía del derecho debe convertirse en el modo de actuación predeterminado de toda organización que se dedique a desarrollos tecnológicos, formando parte de sus procesos y residiendo en la génesis de los productos o servicios. Pretende, por tanto, un compromiso social-empresarial que eleve los estándares a los máximos niveles.

Con el advenimiento de la nueva normatividad europea en materia de protección de datos y privacidad, representada por el Reglamento General Europeo de Protección de Datos (GDPR) la Privacidad desde el Diseño y por Defecto quedaron definitivamente consagradas en términos normativos.

El art. 25 del RGPD le ha conferido la categoría de requisito legal, a la práctica de considerar la privacidad desde las primeras etapas del diseño de productos y servicios

La PbD considera la privacidad y los principios de protección de datos desde la concepción de cualquier tipo de tratamiento.

Establecido lo anterior, es interesante la consideración de los Principios fundacionales de la PbD, a saber:

1. **Proactivo, no reactivo; preventivo, no correctivo.** Una adecuada política de PbD se caracteriza por la adopción de medidas proactivas que se anticipan a las amenazas, identificando las debilidades de los sistemas con el objetivo de neutralizar o minimizar riesgos en vez de aplicar medidas correctivas para resolver los incidentes de seguridad una vez sucedidos. Es decir, la PbD huye de la “política de subsanar” anticipándose a los eventos que afecten a la privacidad antes que sucedan. Por lo tanto, la privacidad por diseño se anticipa a los riesgos, tiene un carácter preventivo. Se trata de actuar antes y no después de acaecidos los sucesos.
2. **La privacidad como configuración predeterminada.** La PbD pretende proporcionar al usuario el máximo nivel de privacidad y, en particular, que los datos personales

estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio. La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. Esto implica que cualquier sistema ha de estar configurado de forma que, por defecto, no se comparta la información del usuario salvo que éste realice una acción o cambie su configuración. La privacidad por defecto otorga un mayor control sobre la información propia, ya que el usuario está protegido, aunque no realice ninguna acción. Más aún, en caso de decidir compartir la información, este principio sugiere implementar una serie de buenas prácticas para asegurar la información del usuario.

- 3. Privacidad incorporada en la fase de diseño.** La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo ya preexistente.

El concepto de PbD se presenta integrado en el diseño y en la arquitectura de los sistemas de tecnologías de información y prácticas de negocios.

Implica considerar la protección de datos personales como un componente esencial del sistema que forma su núcleo funcional y no está agregado, superpuesto o añadido.

La protección de la privacidad ha de estar integrada en el sistema desde el momento en que se diseña, sin que ello disminuya su plena funcionalidad. No se trata de una opción que se añade a posteriori, sino que lo compone integralmente.

- 4. Funcionalidad total: pensamiento “todos ganan”.** Tradicionalmente se ha entendido que se gana privacidad a costa de perder otras funcionalidades, presentando dicotomías como privacidad vs usabilidad, privacidad vs funcionalidad, privacidad vs beneficio empresarial, incluso privacidad vs seguridad. Esta aproximación es artificial y el objetivo ha de ser encontrar el balance óptimo en una búsqueda tipo “ganar-ganar”, con una mentalidad abierta a nuevas soluciones para conseguir sistemas plenamente funcionales, eficaces y eficientes también a nivel de privacidad.

Esta funcionalidad plena, en consecuencia, significa que tanto seguridad como privacidad no han de ser características excluyentes, sino que ambas han de estar

garantizadas e integradas en cualquier sistema. Se trata de evitar falsas dicotomías y probar que la seguridad y privacidad son complementarias y no opuestas.

5. **Protección del dato durante todo el ciclo de vida.** La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida completo de los datos. La seguridad de la información impone confidencialidad, integridad, disponibilidad y resiliencia de los sistemas que cubre. La protección de la información se ha de configurar desde el momento en que se recaban los datos, y debe durar todo su ciclo de vida hasta su destrucción, garantizando también que se eliminen de forma segura y confidencial, respetando los períodos de retención establecidos.

6. **Visibilidad y transparencia:** Garantizar la privacidad es poder demostrarla, verificando que el tratamiento es acorde con la información entregada.

Esto significa que la entidad que trate los datos ha de estar sujeta a los términos y condiciones informados desde un principio, los que no podrán modificarse sin el previo consentimiento del afectado. También podrá estar sujeto a una verificación independiente.

7. **Respeto por la privacidad de los usuarios:** mantener un enfoque centrado en el usuario siendo que el fin último debe ser garantizar los derechos y libertades de las personas cuyos datos son objeto de tratamiento. Este debe ser garantizar los derechos y libertades de los usuarios cuyos datos son objeto de tratamiento, por lo que cualquier medida adoptada debe ir encaminada a garantizar su privacidad. Ello supone diseñar procesos, aplicaciones, productos y servicios “con el usuario en mente”, anticipándose a sus necesidades.

La idea de la PbD es mantener el sistema centrado en el usuario. Tanto los arquitectos, como los operadores, tienen la responsabilidad de proveer fuertes esquemas de privacidad por defecto, que recaben el consentimiento y fortalezcan las soluciones que son amigables para el usuario.

Pensando en las entidades que disponen de grandes y complejos sistemas informáticos creados sin considerar la privacidad por diseño, ha surgido un nuevo principio denominado:

8. **Rethink, Redesign and Revive** (repensar, rediseñar y revivir):

- *Rethink* (repensar): consiste en que las organizaciones revisen sus estrategias de mitigación de riesgos, procesos y sistemas, considerando opciones que otorguen una mayor protección a la privacidad. Por ejemplo, revisando períodos de retención de datos y controles de acceso a los datos.
- *Redesign* (rediseñar): consiste en implementar mejoras en el funcionamiento de los sistemas respetando la privacidad del usuario. Por ejemplo, valorar la disminución en el tipo de datos recabados.
- *Reviving* (revivir): consiste en revivir el sistema en base a un nuevo enfoque más protector de la privacidad.

El interés de las personas siempre ha de estar presente en el diseño y configuración de sistemas y aplicaciones, por ejemplo, mediante fuertes medidas de seguridad (encriptación, verificación en dos pasos, entre otras), información completa y comprensible, opciones “*user-friendly*”.

3.- Registro de Beneficiarios Finales

Beneficiarios finales deben entenderse aquellas personas, esto es, personas físicas o naturales, que verdaderamente controlan o se benefician económicamente de un vehículo jurídico, como una sociedad mercantil, un fideicomiso, una fundación, etc. El GAFI³ los conceptualiza como las personas naturales que “finalmente” —en caso de que la titularidad/control se ejerza mediante una cadena de titularidad o a través de otros medios— posee o controla a un cliente y/o la persona natural en cuyo nombre se realiza una transacción. Incluye también a las personas que ejercen el control efectivo final sobre una persona jurídica u otra estructura jurídica.

El beneficiario final es la persona que efectivamente controla o se beneficia de un vehículo jurídico. Este control o beneficio económico puede ejercerse de diversas formas que las regulaciones jurídicas nacionales determinan de acuerdo a su idiosincrasia particular y ordenamiento jurídico interno.

³ Grupo de Acción Financiera Internacional.

En términos generales y a los efectos de clarificar conceptualmente la referencia, los beneficiarios finales son aquellas personas naturales que, de manera directa o indirecta, controlan un activo o pueden beneficiarse efectivamente de él.

Es menester dejar establecido que ni en el caso de las Sociedades Anónimas ni en las Fundaciones de Interés Privado (entre las personas jurídicas más utilizadas en Panamá) se excluye la posibilidad de que la Junta Directiva esté conformada a su vez por otra(s) persona(s) jurídica(s).

Ahora bien, la condición de miembro Dignatario no implica participación accionaria ni beneficiaria, vale la pena señalar que en todo caso no se consideran beneficiarios finales; siempre recaerá sobre una persona natural, por ende, en esos casos lo correcto sería considerar beneficiario final a aquellos que controlan las personas jurídicas que conforman la Directiva de otra persona jurídica.

Por regla general, los beneficiarios finales serán personas naturales que participan, directa o indirectamente, en el capital o los derechos de voto en una sociedad, es decir, quienes representan el máximo nivel de poder, no siendo controlados por otras personas. Sin embargo, llegado el caso, directores, gerentes, o incluso terceros, podrían considerarse beneficiarios finales si se estima que ejercen un control efectivo sobre una sociedad, en el sentido de que pueden incidir de manera determinante en sus decisiones. Esto último toda vez que esas decisiones pueden implicar particularmente la disposición de los bienes o beneficios de la respectiva persona jurídica.

Determinar quién tiene la calidad de beneficiario final en una sociedad puede ser complejo y depende en gran medida del tipo y forma que adopta la estructura jurídica de la que se trata.

Una determinación que merece destaque es que la identificación del beneficiario final es independiente de la nacionalidad que ostenta. Es decir, un vehículo jurídico debería identificar a sus beneficiarios finales, independientemente de su nacionalidad y lugar de residencia.

Las disposiciones normativas de los diferentes países establezcan criterios particulares en sus definiciones sobre quiénes deben ser considerados beneficiarios finales. Además, y de acuerdo con lo establecido en la Recomendación N° 24 del GAFI, ***“los países deben asegurar que exista información adecuada, precisa y oportuna sobre el beneficiario***

final y el control de las personas jurídicas, que las autoridades competentes puedan obtener o a la que puedan tener acceso oportunamente. En particular, los países que tengan personas jurídicas que puedan emitir acciones al portador o certificados de acciones al portador, o que permitan accionistas nominales o directores nominales, deben tomar medidas eficaces para asegurar que estas no sean utilizadas indebidamente para el lavado de activos o el financiamiento del terrorismo. Los países deben considerar medidas para facilitar el acceso a la información sobre el beneficiario final y el control por las instituciones financieras”.

De ahí la importancia que la República de Panamá haya promulgado su propia legislación en la materia, de forma tal de clarificar el sistema, establecer criterios y responsabilidades en este particular ámbito de la actividad financiera y mercantil.

Tanto el Grupo de Acción Financiera Internacional como el Foro Global exigen que la información sobre los beneficiarios finales sea exacta y verifique niveles de actualización permanente permitiendo confirmar los listados de estas personas mínimamente una vez al año.

Se trata de información que debe estar disponible y ser de manejo habilitado a las autoridades, siendo imperativo, - de acuerdo a los requerimientos de las señaladas instituciones -, que los diferentes países cuenten con mecanismos de verificación de cumplimiento de las obligaciones que se impusieren, así como la determinación de sanciones en caso de incumplimientos.

Imperativo es considerar qué datos son de imprescindible manejo a la hora de la construcción de un registro de las características que dispone la Ley N° 129. Y en consecuencia, la utilización de mecanismos de privacidad desde el diseño para su concreción.

3.1.- Datos sobre Beneficiarios Finales

Los datos de los beneficiarios finales que deben registrarse deben implicar una identificación fiel, exacta de la persona impidiendo que sea confundida con otra persona. Se presenta entonces, como imprescindible la consideración del principio de calidad de los datos también conocido como principio de veracidad, en materia de protección de datos personales.

Los datos imprescindibles requeridos en la generalidad de las legislaciones son:

- Nombre completo

- Fecha de nacimiento
- Nacionalidad
- País de residencia
- Fecha desde que la persona es beneficiaria final.

A lo anterior, en Panamá se agrega:

- Dirección laboral
- Teléfono personal
- Documento de identidad
- Número de pasaporte
- País de nacimiento
- Género
- Estado Civil
- Profesión
- Forma en la que se ejerce el control sobre el vehículo jurídico

Todos los datos señalados, son datos de carácter personal que identifican y/o hacen identificable a las personas, en el caso, beneficiarios finales.

Si se observan los datos requeridos con detenimiento, éstos remiten a diferentes categorías de datos que requieren mayor o menor protección. Es factible identificar datos que no requieren consentimiento informado, hasta datos sensibles. De ahí que las consideraciones de las obligaciones impuestas por la Ley de protección de datos personales son de imprescindible consideración.

Es importante tener presente, que las obligaciones de transparencia y el imperativo requerimiento de obtención de transparencia en el sistema financiero, de manera alguna es óbice para que un derecho fundamental sea vulnerado.

Es por esta razón, que se entiende imprescindible realizar una construcción de contexto que incluya los imprescindibles requerimientos de la Ley N° 129, de 2020, en coadyuvancia con la Ley N° 81 de 2019.

4.- Conclusiones

Panamá verifica una gran oportunidad normativa en esta materia, en tanto, como se indicó, es imperativo contextualizar la aplicación de ambas disposiciones normativas para garantizar

tanto los derechos asociados a la República, en tanto, obligaciones y necesidades de transparencia, cuanto aquéllos asociados en forma directa con la dignidad de las personas, esto es, los referidos a la protección de datos personales.

Así es que vale la pena recalcar que lo recomendable será que en la reglamentación – que se espera se promulgue prontamente – para la Ley N° 129 se consideren los señalados principios fundacionales de la privacidad por diseño. Su inclusión sería un interesante avance al momento de diseñar el Sistema Privado y Único de Registro de Beneficiarios, ya no desde el punto de vista estrictamente jurídico, sino técnico y tecnológico.

Brindaría la credibilidad y privacidad oportunas a un sistema contentivo de información personal, que requiere de protección y cuya necesidad de especial protección como garante para la transparencia del sistema financiero, la transforma en un elemento clave.

No puede perderse de vista que, en todo caso, contendrá información general de los clientes corporativos, de abogados y agentes residentes. Esta sería la mejor manera, en principio, de asegurar la integridad, confidencialidad, trazabilidad y seguridad informática y de la información en relación con los datos de necesario tratamiento.

Por otra parte, y en su calidad de medida de responsabilidad proactiva, no cabe discusión en relación con lo recomendable de su inclusión dada la cercanía de la entrada en vigencia de la Ley N° 81, de 2019.

Es el momento propicio para seguir estos principios ya que brindarían a la comunidad jurídica en general y a su clientela, los elementos para confiar y colaborar en la conformación del contenido del citado registro. Con esto se concretaría evitar la necesidad del rediseño permanente de los sistemas para adaptarlos al imperativo de este derecho fundamental a la protección de datos personales. De esta forma, en consecuencia, se reducirán los costes, ya que no es recomendable estar siempre solucionando errores después de que ya se ha diseñado o implementado el servicio o plataforma en la entidad.

Por otra parte, es importante a tener en cuenta que las medidas de seguridad física y lógicas que se adopten deberán ser proporcionales y adecuadas en función de la sensibilidad de los datos que se requiera coleccionar y tratar.

Finalmente, cabe mencionar que, si bien es cierto que los principios de privacidad desde el diseño no son vinculantes en Panamá, toda vez que ni la Ley de protección de datos

personales ni la Ley de Registro Único de beneficiarios finales mencionan su aplicación, también lo es, que ya se han adoptado en otras latitudes con buenos resultados e incluso es parte de la disposición normativa internacional más relevante a nivel mundial en materia de protección de datos personales. Disposición normativa esta última, que, sumada a los Estándares Iberoamericanos en materia de Protección de Datos Personales, adoptados por la Red Iberoamericana de Protección de Datos, se consideran como los estándares de protección más importantes a nivel mundial.

En su calidad de principios, además, informan todo el andamiaje normativo nacional, en su calidad de elementos centrales del funcionamiento del sistema jurídico. De ahí que se entiende aconsejable su consideración a la hora de avanzar en la construcción de la imprescindible reglamentación.

Bibliografía

- BID. Regulación sobre beneficiarios finales en América Latina y el Caribe. Disponible en: <https://publications.iadb.org/publications/spanish/document/Regulaci%C3%B3n-sobre-beneficiarios-finales-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf>
- Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: <http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf> (último acceso: 27/12/2020).
- Cavoukia, Ann. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Disponible en: <http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf> (último acceso: 27/12/2020).
- Cavoukia, Ann. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Disponible en: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (último acceso: 27/12/2020).

Filipelli, Inés y otro. Entre la solidaridad y el Cumplimiento. Prevención del Lavado de Activos y Financiamiento del Terrorismo en Organizaciones sin fines de lucro. Disponible en: <http://brumcosta.com/2020/04/20/entre-la-solidaridad-y-el-cumplimiento-prevencion-del-lavado-de-activos-y-financiamiento-del-terrorismo-en-organizaciones-sin-fines-de-lucro/> (último acceso: 27/12/2020).

- Ley N° 129, de 17 de marzo de 2020.
- OCDE – GAFI. Estándares Internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación. Recomendaciones del GAFI. Disponible en: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf> (último acceso: 27/12/2020).