Privacy by Design: de la abstracción jurídica a la práctica ingenieril

Flavia Baladán, Gustavo Betarte, Alejando Blanco, Cecilia Montaña, Bárbara Muracciole, Beatriz Rodríguez

***Abstract*— Privacy is a fundamental right recognized by the most important legal instruments for the protection and guarantee of human rights. Privacy by Design, a concept developed in the 1990s by Ann Cavoukian, constitutes both a conceptual and practical development for the defense of that right. We discuss the different views that exist on this discipline from a legal and engineering perspective and put forward the understanding and preliminary conclusions that have been obtained as the result of a research work carried out by a team of doctors in law, security and data scientists and computer engineers. It was of particular interest of this team to incorporate into the research hypotheses the characteristics of the legal normative framework of Latin America and in particular the one of Uruguay.**

***Index Terms*—** *fundamental right, privacy by design, data protection, legal framework, privacy engineering.*

I. Introducciön

La privacidad es un derecho fundamental reconocido por los instrumentos jurídicos más importantes de protección y garantía de los derechos humanos. Cuando hablamos de derechos fundamentales, referimos a *"aquellos derechos subjetivos esenciales o básicos, inherentes a los seres humanos por su sola calidad de tales, sin distinción ni discriminación alguna en función de factores tales como la nacionalidad, el sexo, origen racial o étnico, credo o religión ... por su alto valor ético, todos estos derechos están reconocidos y protegidos por los Tratados Internacionales y las Cartas Constitucionales de los Estados democráticos, destacando no solo la formulación de los mismos sino, además, las garantías y fórmulas apropiadas para hacer valer su respeto y vigencia.*"[1]

A nivel internacional cabe mencionar la Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948, que en su artículo 12 dispone "*[n]adie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*". Similar texto ha sido recogido por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1966.En los ámbitos regionales, la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) en su artículo 11 establece "*[t]oda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*". En sentido conteste, el Convenio Europeo de Derechos Humanos dispone en su artículo 8 "*[t]oda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"*. De igual forma se pronuncia la Carta de los Derechos Fundamentales de la Unión Europea y el Tratado de Lisboa.

Uno de los desarrollos conceptuales y prácticos para la defensa de este derecho lo constituye la denominada Privacidad por Diseño (en adelante e indistintamente PbD por sus siglas en inglés), que refiere a un concepto elaborado en la década de los 90' por Ann Cavoukian [2], en ese entonces comisionada de información y privacidad de Ontario (Canadá). Este concepto surge como respuesta al entonces incipiente y creciente uso de las Tecnologías de la Información y Comunicaciones (TICs) y el tratamiento masivo de datos, así como a la necesidad de dar cumplimiento al marco regulatorio y normativo de protección de datos personales. La PbD tiene como objetivo que los requerimientos de privacidad se consideren durante todo el ciclo de vida de los sistemas, de forma que ésta se convierta en un modo predeterminado de construcción. En definitiva lo que se busca es no resignar la privacidad al cumplimiento de normas técnicas y jurídicas. Cuando nos referimos a "sistemas" no solo estamos hablando de sistemas informáticos o de información,

Flavia Baladán es asesor letrado de la URCDP y AGESIC, Profesor Adscripto aspirante de Informática Jurídica y Ayudante de Derecho Informático de la Facultad de Derecho de la Universidad de la República, Uruguay (flavia.baladan@agesic.gub.uy).

Gustavo Betarte es Profesor Titular del Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República, Uruguay (e-mail gustun@fing.edu.uy) y responsable del CSIRT Tilsor (e-mail: gbetarte@tilsor.com.uy).

Alejandro Blanco es Profesor Adjunto del Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República, Uruguay (e-mail ablanco@fing.edu.uy) .

María Cecilia Montaña es asesor letrado de AGESIC (cecilia.montana@agesic.gub.uy).

Bárbara Muracciole es asesor letrado de la URCDP y AGESIC, Profesor Adscripto aspirante de Informática Jurídica y Ayudante de Derecho Informático de la Facultad de Derecho de la Universidad de la República, Uruguay (barbara.muracciole@agesic.gub.uy).

Beatriz Rodríguez es asesor letrado de la URCDP y AGESIC, Profesor Adscripto aspirante de Informática Jurídica y Ayudante de Derecho Informático de la Facultad de Derecho de la Universidad de la República, Uruguay (beatriz.rodriguez@agesic.gub.uy).

sino también a los procesos de negocio y gobernanza de la organización, las tecnologías de comunicación involucrada y el ecosistema completo de los sistemas de información.

En el año 2016 en el marco del centro de I+D *Information and Communications Technologies for Verticals* (*ICT4V,http://www.ict4v.org*) se creó un equipo de trabajo multidisciplinario integrado por ingenieros y abogados pertenecientes a la Facultad de Ingeniería de la Universidad de la República, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), la Unidad Reguladora y de Control de Datos Personales (URCDP) y TILSOR S.A.[1]. El primer y principal objetivo de este equipo es estudiar y profundizar el estado del arte de la disciplina de *Privacy by Design*, particularmente a nivel latinoamericano y desde una doble perspectiva técnica y jurídica, a fin de identificar los desafíos nacionales en la materia y las perspectivas de progreso, mediante el estudio de la doctrina científica destacada en la materia. Sus avances y conclusiones preliminares justifican la redacción de este documento.

La estructura del resto de este artículo es la siguiente. La sección II está dedicada a introducir en forma breve la motivación de este trabajo. En la sección III se describe el contexto normativo internacional, regional y nacional. En la sección IV se exponen los principios fundacionales de la PbD. En la sección V se discuten las diferentes visiones que existen sobre esta disciplina, desde el mundo jurídico y técnico-ingenieril, en particular, y se posiciona el entendimiento que tienen los autores al respecto. La sección VI describe algunos resultados preliminares que se desprenden del avance que el equipo de trabajo ha realizado. Finalmente, la sección VII describe trabajo futuro.

II. Motivación

Toda investigación debe ser considerada a partir del contexto circundante que la forja, en este sentido, no podemos soslayar al abordar Privacy by Design, el impacto de la Sociedad de la Información en los derechos humanos, particularmente en la privacidad y la protección de datos personales.

"*La humanidad vive la revolución más grande y acelerada que haya experimentado en su historia. El uso y continuo desarrollo de las tecnologías de la información y comunicación -TIC- han cambiado y seguirán afectando nuestra forma de vida en todos los ámbitos: la cultura, la política, el arte, la economía y, en general, todas las formas en que los seres humanos nos relacionamos. Estamos transitando, pues, por lo que se ha denominado la "sociedad de la información", la cual está definida por la importancia que tienen las nuevas formas de comunicación, así como el uso –en todos sus aspectos– y la propiedad de la información*." [3]

Ahora bien, estos fenómenos transformadores que, sin duda, presentan grandes oportunidades, también entrañan peligros para los derechos humanos. Si bien aludimos a todos los derechos civiles, políticos, económicos, sociales y culturales, en cuanto *"constituyen valores universalmente exigibles, elaborados y desarrollados como parte esencial de una conciencia univesal en un momento o período histórico determinado*" [4], la referencia tecnológica posiciona en el ojo de la tormenta a la intimidad, la privacidad y la protección de datos.

Desarrollos tales como Big Data, Internet de las cosas (IoT), wearables, aplicaciones (apps), sistemas de localización, drones, realidad aumentada, inteligencia artificial, entre otros, provocan la aparente pérdida de la privacidad de los usuarios de desarrollos tecnológicos, creando una sensación de desprotección y fomentando la idea que el consentimiento agoniza y que la privacidad debe resignarse en pos de la utilización de las mencionadas herramientas.

En este escenario y partiendo siempre de la concepción de la persona como centro, la privacidad, en cuanto derecho fundamental, debe garantizarse -más que nunca- sin mediar actuación alguna de los usuarios finales de desarrollos tecnológicos, en concordancia con los textos legales tuitivos. A partir de esta realidad surge la dificultad de implementar y armonizar las exigencias legales y reglamentarias, por lo que resulta necesaria su revisión.

III. Contexto Normativo

Desde la ciencia jurídica, la Privacidad por Diseño nació como una buena práctica pero con el devenir del tiempo ha sido recogida en instrumentos de reconocida importancia en lo que a protección de datos se refiere, mostrando una clara evolución en la materia.

Un primer paso está marcado por la Resolución sobre PbD emanada de la 32ª Conferencia Internacional de Protección de Datos, celebrada en Israel en el año 2010. Este documento recoge en forma expresa los principios fundacionales de la PbD y exhorta a las autoridades nacionales a que fomenten su adopción. Asimismo, invita a su promoción de la forma más amplia posible mediante la distribución de materiales, su inserción en la educación, y la incorporación de los principios en la formulación de las políticas públicas y la legislación en cada una de sus jurisdicciones. Por último, la resolución fomenta en forma proactiva la investigación en la materia y su inclusión en las agendas que la abordan.

Posteriormente, el 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al

[1] FING - UDELAR. La Facultad de Ingeniería de la Universidad de la República aporta el conocimiento académico de su Grupo de Seguridad Informática.

AGESIC – URCDP. La Unidad Reguladora y de Control de Datos Personales es el órgano competente para estudiar, regular y controlar la Privacidad desde el Diseño, por lo que su opinión experta es determinante en todo proyecto que aborde el tema.

TILSOR S.A. Es una empresa uruguaya que se distingue por su especialización en la entrega de servicios de misión crítica y de seguridad informática. Es del interés de Tilsor promover, comprender e impulsar el paradigma de Privacidad desde el Diseño.

tratamiento de datos personales y a la libre circulación de estos datos, cuyo artículo 25 regula en forma expresa la protección de datos desde el diseño y por defecto. De esta forma, por primera vez desde su nacimiento la Privacidad por Diseño se transforma de una práctica en una obligación legal de aplicación directa a todos los países de la Unión Europea.

Sobre el contenido, es de destacar que esta norma establece que se debe tener en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, el ámbito, el contexto, y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas para aplicar la privacidad desde el diseño. En su mérito, el responsable del tratamiento debe utilizar medidas técnicas y organizativas apropiadas como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, así como la minimización de datos, e integrar las garantías necesarias en el tratamiento.

La conformidad con el Reglamento puede ser demostrada por el responsable mediante la adopción de políticas internas y medidas que cumplan con los principios de protección de datos desde el diseño y por defecto. Agrega el citado artículo 25 que "*Dichas medidas podrían consistir en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad".*

Además, el citado Reglamento establece que los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.La aprobación del Reglamento General de Protección de Datos impacta el sistema normativo uruguayo en la materia, especialmente en los aspectos relativos a la adecuación para la transferencia internacional de datos y al ámbito de aplicación territorial.

Respecto de la adecuación y transferencia internacional de datos, en virtud que nuestro país deberá ordenar sus procesos y normas internas para mantener la decisión de la Comisión Europea que le confiere estatus de país confiable para importar y exportar datos personales. [5]

Relacionado con la vocación extraterritorial, en tanto el Reglamento habrá de aplicarse a responsables y encargados de tratamiento aún no establecidos en la Unión Europea, cuando las actividades de bienes o servicios se realicen a interesados situados en la Unión o se dirija al control de su comportamiento. "*Por ello que una empresa uruguaya (...) que ofrezca bienes o servicios a individuos en la UE o que controle su comportamiento, deberá cumplir con el nuevo Reglamento de Protección de Datos. Y esto no solo implica cumplir con las obligaciones y respetar los derechos de los individuos, sino también designar un representante en la UE, salvo que la actividad de tratamiento de datos personales sea ocasional*". [6]

A. Situación regional

América Latina, por su parte, se ha caracterizado por regular la protección de datos personales pero no la privacidad desde el diseño. En su mérito, podemos clasificar a los Estados latinoamericanos en cuatro categorías:

i. sin ley de protección de datos (Bolivia y Paraguay),
ii. con ley de protección de datos pero sin regulación expresa de la PbD (Argentina, Colombia, Costa Rica, México, Nicaragua, Perú, y Uruguay),
iii. con ley de protección de datos en proceso de reforma (Argentina y Chile) y
iv. con proyecto de ley (Ecuador, Brasil, Honduras y Panamá).

Hasta el momento, sólo Colombia ha incorporado a texto expreso mediante el Decreto N° 1413, de 25 de agosto de 2017, la privacidad desde el diseño y por defecto, así como las medidas para garantizar su efectiva aplicación.

No obstante no será el único país en hacerlo, ya que el artículo 38 de la reforma legal Argentina de protección de datos prevé similar agregado, disponiendo que el responsable del tratamiento aplicará las medidas tecnológicas y organizativas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos. También las aplicará con miras a garantizar que, por defecto, solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada uno de sus fines.

B. Situación nacional

En Uruguay el derecho a la protección de datos personales se encuentra regulado por la Ley Nº 18.331, de 11 de agosto de 2008, cuyas disposiciones no incluyen la Privacidad por Diseño a texto expreso.

Sumariamente podemos decir que su artículo primero reconoce que el derecho a la protección de datos personales "*es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República"*, extendiendo su ámbito de aplicación subjetivo a las personas jurídicas, en cuanto corresponda, extremo discutible debido a que, justamente, referimos a derechos humanos.

Relacionado con los principios, en su artículo 5 la referida ley dispone que la actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales:

- Legalidad (artículo 6)
- Veracidad (artículo 7)
- Finalidad (artículo 8)
- Previo consentimiento informado (artículo 9)
- Seguridad de los datos (artículo 10)
- Reserva (artículo 11)
- Responsabilidad (artículo 12)

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

Se consagra el consentimiento expreso como regla para la generalidad de los casos, y expreso y escrito para la categoría de datos sensibles (aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual).

Destacan categorías de datos especialmente protegidos, dentro de los cuales se encuentran los datos sensibles, datos relativos a la salud, a las telecomunicaciones, a las bases de datos con fines de publicidad y de la actividad comercial o crediticia.

Además de los principios rectores, la ley establece que el titular de los datos tendrá derecho de:

- Información (artículo 13)
- Acceso (artículo 14)
- Rectificación (artículo 15)
- Actualización (artículo 15)
- Inclusión (artículo 15)
- Supresión (artículo 15)
- Impugnación a las valoraciones personales derivadas de tratamientos automatizados y con efectos jurídicos (artículo 16)

Esta ley crea un órgano de control con autonomía técnica y competencias expresas e implícitas, suficientes para velar por el cumplimiento de la ley, lo que incluye potestades sancionatorias administrativas. Por último, interesa resaltar la instauración de un régimen jurisdiccional de protección de este derecho, mediante la acción de Habeas Data consistente en un proceso sumario y efectivo.

IV. Principios Fundacionales de Privacy by Design

Si bien las regulaciones de protección de datos personales especifican requerimientos de privacidad en lo relativo al manejo de los datos personales, desde un punto de vista ingenieril ofrecen muy pocos detalles de su significado. La falta de precisión se torna una dificultad a la hora de hacer el pasaje de los requerimientos de privacidad a partir de marcos regulatorios legales, éticos o sociales a requerimientos de diseño e implementación de los sistemas que manipulan esos datos. Cavoukian en su propuesta sintetiza estos requerimientos en 7 principios fundacionales [2]:

- Proactivo, no reactivo; tomemos acciones preventivas y no de recuperación.

  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.

- Privacidad por defecto

  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 asegurarla.

- Privacidad integrada en el diseño

  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.

- *Positive-sum, not zero*

  Se trata de evitar falsa dicotomías y probar que la privacidad es complementaria y no opuesta a otros requisitos o funcionalidades.

- Protección durante todo el ciclo de vida

  La protección de la información se ha de configurar desde el momento en que se recaban los datos, y debe durar durante todo su ciclo de vida hasta su destrucción, garantizando también que se eliminen de forma segura y confidencial, respetando los periodos de retención establecidos.

- Visibilidad y transparencia (*Keep it Open, trust but verify*)

  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.

- Respeto por la privacidad del usuario

  La idea de la PdD es mantener el sistema centrado en el usuario. Los diseñadores del sistema 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.

En el año 2011, pensando en las entidades que disponen de grandes y complejos sistemas informáticos creados sin considerar la Privacidad por Diseño, Cavoukian desarrolla la idea de Privacy by ReDesign (Pb^RD) [7] que consiste en:

- *Rethink, Redesign and Revive* (repensar, rediseñar y restablecer):
  - *Rethink* (repensar): revisar estrategias de mitigación de riesgos, procesos y sistemas, considerando opciones que otorguen una mayor protección a la privacidad. Por ejemplo, revisando periodos de retención de datos y controles de acceso.
  - *Redesign* (rediseñar): implementar mejoras en el funcionamiento de los sistemas

respetando la privacidad del usuario. Por ejemplo, valorar la disminución en el tipo de datos recabados.

- *Revive* (restablecer): restablecer el sistema en base a un nuevo enfoque más protector de la privacidad.

Los 7 (siete) principios fundacionales de PbD han servido como punto de partida para su adopción en ámbitos gubernamentales y corporativos. Sin embargo, han sido fuertemente criticados debido a que el concepto de PbD permanece vago y tampoco aporta información sobre cómo llevarlos a la práctica en el desarrollo de sistemas informáticos (las prácticas ingenieriles). Algunos de los principios usan el término de PbD para explicarse a sí mismos (p.e. privacidad integrada en el diseño) generando definiciones recursivas circulares (Privacidad por Diseño significa aplicar Privacidad por Diseño). Por otro lado, resulta realmente difícil llevar a la práctica o traducir estos 7 (siete) principios de PbD a estrategias o metodologías de diseño, análisis o desarrollo (el proceso de construcción) de los sistemas informáticos.

A. De los principios jurídicos a los requerimientos técnicos

En [8] en lugar de partir de los principios de PbD propuestos por Cavoukian, se realiza un análisis de los requerimientos de privacidad tomando como insumo marcos legales y regulatorios de protección de datos personales y privacidad. En este trabajo se tomó como punto de partida el marco regulatorio Europeo, las guías de la OECD (Organization of Economic Co-Operation and Development) y las especificaciones técnicas ISO 29100 (Privacy Framework). A partir de este análisis los autores derivan 8 (ocho) requerimientos de privacidad que tienen como objetivo satisfacer las exigencias legales. Estos son luego tomados como insumo para derivar las estrategias de diseño de privacidad que den soporte a la construcción de sistemas de TI que contemplen los requerimientos de privacidad en etapas tempranas del desarrollo (diseño y análisis). Los requerimientos derivados en [8] para cumplir el marco legal y regulatorio de protección de datos personales y privacidad analizados, son los siguientes:

- Limitación de propósito
- Minimización de los datos
- Calidad de los datos
- Transparencia (*Openness* en términos de la OECD)
- *Data Subject Rights* (en términos de consentimiento, derecho de acceso, eliminar y rectificar datos personales)
- Derecho al olvido
- Protección (seguridad) adecuada
- Portabilidad de los datos
- Notificación de los casos de violación de acceso a datos personales.
- Auditoría y (quizás) asegurar el cumplimiento (*compliance*).

Una conclusión importante a destacar del análisis de requerimientos de privacidad a partir del marco regulatorio realizado en [8] es que no todo requerimiento legal o regulatorio puede satisfacerse diseñando el sistema de TI en una forma específica. Dicho de otra forma, no todos los requerimientos legales van a tener un impacto en el diseño de un sistema de TI. A modo de ejemplo podemos considerar el requerimiento de "Procesamiento Legitimo", ya que una especificación precisa de este concepto jurídico y su correspondiente implementación técnica entendemos sería de difícil concreción.

Por otra parte, en [9] se presenta una taxonomía para clasificar problemas de privacidad. En este trabajo el autor identifica 4 grupos básicos de actividades que afectan la privacidad:

- recolección (y almacenamiento) de datos,
- procesamiento de información,
- diseminación de la información (transferencia) e
- invasión

Si consideramos entonces un sistema de TI como un sistema de almacenamiento y procesamiento de información, en general este cuenta con un sistema de base de datos. Más aun, la legislación de datos personales se redactó teniendo en "mente" este modelo.

En resumen, a partir de los requerimientos derivados del marco regulatorio y legal de protección de datos personales y privacidad, los 4 (cuatro) grupos básicos de actividades que afectan la privacidad y el modelo subyacente de los sistemas de información se pueden derivar 8 (ocho) estrategias de diseño de privacidad: MINIMIZE, SEPARATE, AGGREGATE, HIDE, INFORM, CONTROL, ENFORCE y DEMONSTRATE. Estas estrategias a su vez se pueden agrupar en dos clases: *data-oriented* y *process-oriented*.

B. Hacia la construcción de sistemas PbD

Como bien sabemos la seguridad, así como la privacidad son propiedades fundamentales de los sistemas que están fuertemente influenciadas por el proceso de diseño y construcción. No son propiedades que se puedan hacer cumplir (*enforce*) como un agregado al sistema luego de desarrollado sino que debe considerarse desde las etapas más tempranas y durante todo su ciclo de vida.

Figura I: PbD en el ciclo de vidad de desarrollo de sistemas

Como se ilustra en la Figura I las estrategias de diseño deberían asistir las etapas de desarrollo conceptual y análisis del ciclo de vida de software (SDLC por sus siglas en inglés), los *Privacy Design Patterns* la etapa de diseño y las *Privacy Enhanced technologies* (PETs) deberían ser utilizadas durante la implementación. Ahora bien, se necesita poder contar con estrategias de diseño de privacidad y una metodología para su aplicación en las etapas iniciales del SDLC. Este es uno de los principales desafíos a la hora de poner en práctica los principios de PbD.

En las últimas décadas se han propuesto y definido un amplio abanico de técnicas y tecnologías de *Privacy Design Patterns* y PETs, como ser *Zero-knowlege Proofs, Private Information Retrival (PIR),* anonimización*, Attributed Based Credentials (ABC), Differential Privacy* entre otros. Sin embargo PbD debe primero considerarse a nivel del diseño, concepción o de la arquitectura del sistema de software que se está diseñando. Desde el punto de vista ingenieril esto es un desafío sobre el cual actualmente se está investigando.

V. Perspectivas Técnicas y Jurídicas

Existen visiones diferentes y complementarias del concepto de Privacidad por Diseño. Como se señala en [10], puede entenderse que es un concepto multifacético. Por un lado, en documentos legales se describe usualmente en términos muy generales. Por otro, los computistas e ingenieros informáticos a menudo lo equiparan con el uso de estrategias, *Privacy Design Patterns* o *PET*s. Sin embargo, entendemos que la Privacidad por Diseño no es ni una recopilación de meros principios generales ni puede solo reducirse al uso de estrategias o mecanismos, es un proceso que involucra variados componentes tecnológicos y organizacionales que son usados para implementar principios de privacidad y protección de datos. Estos suelen ser derivados de requerimiento legales, a pesar de que a menudo son insuficientemente especificados. La construcción de sistemas de información que garanticen requerimientos de privacidad no es posible si esos requisitos no son integrados desde el inicio en las actividades típicas de ingeniería de sistemas. Dado que la mayoría de los requisitos de privacidad se basan en mecanismos básicos de ingeniería de seguridad, por ejemplo, mecanismos para garantizar la confidencialidad, integridad o disponibilidad, las actividades de ingeniería de seguridad como el análisis de riesgos y amenazas también deben acompañar el proceso. Existe poca experiencia en el diseño de sistemas con la privacidad en mente, la que adicionalmente es en general inaccesible para los diseñadores de políticas que discuten los principios de Privacidad por Diseño.

Una de las estrategias que ha sido recurrentemente utilizada para el diseño de sistemas informáticos que preserven la privacidad es la aplicación de técnicas de minimización. Por minimización de datos se entiende la no recolección de datos innecesarios para implementar en forma adecuada las funcionalidades del sistema, limitando así el posible impacto de privacidad que tenga en este. Ahora bien, por minimización de datos, no solo nos referimos a los datos recolectados sino también a la exposición de estos fuera del dominio de confianza del titular de los datos (o usuario del sistema). Se debe ampliar el concepto y hacer referencia a las distintas estrategias de diseño que restrinjan el flujo de datos bajo el dominio o control del usuario evitando así dominios controlados por terceros.

En [12] se identifica como estrategia primaria de diseño de privacidad la minimización del riesgo y la necesidad de confianza (*need for trust*). Por “riesgo”, se entiende limitar siempre que sea posible la probabilidad y el impacto de un evento que provoque la perdida de privacidad. Por “necesidad de confianza”, se hace referencia a limitar cuando sea posible la dependencia a que otras entidades se comporten como es esperado con respecto al manejo de datos sensibles. Por otro lado, con “minimizar la necesidad de confianza” se refiere a una falta de confianza "emocional" en otras entidades. Este concepto está en realidad relacionado con que las entidades logren la funcionalidad del sistema, sin que la misma esté condicionada a la recolección y procesamiento de grandes volúmenes de datos sensibles que puedan llevarnos a la pérdida de privacidad. En la mayoría de los casos, el concepto de minimización de riesgos es equivalente a minimizar el riesgo que se materialicen fugas de datos personales. La estrategia de minimización en realidad está expresando una familia de estrategias derivadas, como ser:

- Minimización de recolección, limitando siempre que sea posible la cantidad de datos que son recolectados (capturados) y almacenados por el sistema.
- Minimización de disclosure, restringir el flujo de información a aquellas partes (componentes) o entidades al que los datos están relacionados.
- Minimización de inferencias (linkability), que se pueda hacer vinculando datos del sistema,
- Minimización de retención, de los datos en el sistema.

Persiste de todas formas la pregunta de cómo aplicar estas estrategias de diseño en el proceso de construcción de sistemas informáticos. En los trabajos [13] y [12] se analiza este punto y

se propone una metodología basada en una serie de actividades a seguir en la etapa de diseño del sistema. Otros trabajos [14, 15] llegan a proponer un modelo formal como marco para desarrollar esta actividad.

En otra línea de investigación, se encuentran propuestas fundadas en una taxonomía para una mejor gobernanza de los datos personales [16]. Este trabajo propone un modelo pre definido que ayude a las empresas a clasificar su información para un mejor control del flujo de datos personales.

Lo cierto es que esta es un área incipiente de investigación y en evolución con pocas metodologías para su aplicación en proyectos de desarrollo, las que cabe destacar requieren un alto nivel de *expertise* para su puesta en práctica, así como una regulación legal expresa que permita su efectivo desarrollo. Actualmente el equipo de trabajo está investigando las metodologías y técnicas propuestas para validarlas en casos prácticos. Si bien es cierto que la regulación de la privacidad y la protección de datos personales otorgan un marco conceptual para la aplicación de la Privacidad por Diseño, no puede sostenerse que sea suficiente para exigir su efectiva implementación, y mucho menos la forma de hacerlo. Una constatación irrefutable al relevar el contexto normativo y repasar la evolución histórica de este concepto, resulta que debe ser regulado a texto expreso para que su implementación se torne uniforme, de lo contrario, persistirá simplemente como buena práctica.

En el caso de Uruguay, la ley Nº 18.331 sigue el anterior modelo europeo de protección de datos personales, tomando como fuente de inspiración la Directiva 95/46/CE, así como la Ley Orgánica 15/999 española en la materia, que no preveían su regulación en particular, debido a que se trataba de una teoría incipiente de escaso desarrollo. Se considera necesario que próximas reformas legislativas incorporen la Privacidad por Diseño en el ordenamiento jurídico interno.

VI. AVANCES

Dentro de los aspectos que han sido estudiados por el equipo de trabajo, uno de los primeros consensos al que se arribó fue la necesidad de trabajar en la armonización del vocabulario técnico-ingenieril y jurídico, desde que se constató en reiteradas ocasiones las diferentes acepciones de un mismo término desde ambos ámbitos. Este problema sucede con mucha frecuencia a la hora de la implementación de soluciones técnicas derivadas de requerimientos legales. En este sentido, se considera necesario trabajar en forma conjunta para definir el alcance de los conceptos utilizados en el marco de la PbD, con la finalidad de homogeneizar su interpretación.

Un resultado preliminar obtenido lo constituye el desarrollo, a partir del resumen de los 10 requerimientos de privacidad presentados en [8] y derivados del marco jurídico europeo, las guías de la OECD y la ISO 29100, del cotejo de estos requerimientos con los principios de la Ley Nº 18.331 a los efectos de verificar su cumplimiento. La Tabla 1 presenta una descripción muy resumida del resultado del estudio comparativo realizado.

Requerimientos de Privacidad [8]	**Principios y derechos Ley Nº 18.331**
Limitación de propósito	Principio de legalidad (art.6) Principio de Finalidad (art. 8) Derecho a la información (art. 13)
Minimización de los datos	Principio de Veracidad (art.7) Principio de Finalidad (art.8)
Calidad de los datos	Principio de Veracidad (art.7)
Transparencia (*Openness* en términos de la OECD)	Derecho a la Información (art. 13)
Data Subject Rights (en términos de consentimiento, derecho de acceso, eliminar y rectificar datos personales)	Principio del Previo Consentimiento (art. 9) Derecho de Acceso (art. 14) Derecho de rectificación, actualización, inclusión o supresión (art. 15) Derecho de impugnación de las valoraciones personales (art. 16)
Derecho al olvido	Principio de Veracidad (art. 7) Principio de Finalidad (art.8) Derecho de supresión (art. 15)
Protección (seguridad) adecuada	Principio de Seguridad (art. 10)
Portabilidad de los datos	Derecho de Acceso (art. 14)
Notificar los casos de violación de acceso a datos personales.	Derecho de Información (art. 13) Principio de Seguridad (art. 10) Principio de Responsabilidad (art. 12)
Auditoría y (quizás) asegurar el cumplimiento (*compliance*).	Principio de Legalidad (art. 6) Derecho de Acceso (art. 14) Derecho de rectificación, actualización, inclusión o supresión (art. 15) Derecho de impugnación de las valoraciones personales (art. 16) Principio de Seguridad (art. 10) Principio de Responsabilidad (art. 12)

Tabla 1: Cotejo de requerimientos de PbD y derechos de ley

La referida tabla fue elaborada en base a los requisitos jurídicos contenidos en la Ley N° 18.331, según el razonamiento que se describe a continuación.

Se considera que el requerimiento limitación de propósito, cumple con el principio de legalidad que establece que la formación de bases no puede tener finalidades violatorias de derechos humanos o ser contrarios a las leyes o a la moral pública. Además, cumple con el principio de finalidad que indica que los datos sean utilizados para el propósito para el cual fueron recolectados, y con el principio de información que obliga a notificar al titular del tratamiento previsto al momento de colecta de sus datos.

La minimización respeta los principios de veracidad y finalidad en tanto los datos que se vayan a tratar no serán excesivos en relación con la finalidad para la cual se hubieren obtenido.

La calidad de datos como requerimiento cumple con el principio de veracidad en tanto los datos deben ser ciertos, adecuados, ecuánimes, no excesivos, exactos y actualizados.

La transparencia contempla en todo el derecho a la información frente a la recolección de datos debido a que es necesario informar previamente a los titulares en forma expresa, precisa e inequívoca la finalidad para la cual van a ser tratados, la existencia de la base de datos, la identidad y domicilio del responsable, el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, las consecuencias de proporcionar los datos o de la negativo a hacerlo o de su inexactitud, la posibilidad del titular de ejercer los derechos de acceso, rectificación o supresión de los datos.

Los data subject rights se conceptualizan en términos de consentimiento, derechos de acceso, eliminación y rectificación de datos personales. Desde el punto de vista jurídico este requerimiento prevé la observancia del principio de previo consentimiento informado entendido éste como una manifestación libre, previa, expresa e informada que deberá documentarse. Además, refiere al cumplimiento del ejercicio de los derechos por parte del titular de acceder a toda la información que se halle en bases de datos públicas o privadas, a rectificarla, a actualizarla y suprimirla en los casos de perjuicio a los derechos e intereses legítimos de terceros, notorio error o contravención legal, o solicitar la inclusión si correspondiere. Cuando se trate de bases de datos con fines de publicidad el titular puede solicitar en cualquier momento el retiro o bloqueo de sus datos personales. Asimismo, se considera que queda comprendido el derecho a la impugnación de valoraciones personales cuando el titular es sometido a una valoración de su comportamiento cuyo único fundamento sea un tratamiento que ofrezca una definición de sus características o personalidad.

Otro requerimiento es el derecho al olvido. En este aspecto desde una perspectiva jurídica este requerimiento contempla los principios de veracidad y finalidad así como el derecho de supresión. Esto es, los datos deben ser veraces, exactos y estar actualizados, ser utilizados para la finalidad para la cual fueron recabados teniendo el titular del dato el derecho a solicitar su eliminación en los casos ya mencionados.

Un requerimiento más es la protección (seguridad) adecuada. Desde la óptica del Derecho este requerimiento queda abarcado por el principio de seguridad que consiste en garantizar la seguridad y confidencialidad de los datos personales mediante la adopción de medidas tendientes a evitar la adulteración, pérdida, consulta o tratamiento no autorizado así como detectar desviaciones de información intencionales o no ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Los datos deberán ser almacenados en bases que reúnan condiciones técnicas de integridad y seguridad, y de modo que permitan el ejercicio del derecho de acceso de su titular.

Otro requerimiento es la portabilidad de los datos, este requerimiento amplía el derecho de acceso que está regulado a nivel nacional en los términos ya mencionados en virtud de que el titular no solo puede acceder sino que puede traslado de sus datos directamente o exigir su traslado de un prestador a otro.

También se contempla el requerimiento de notificación en los casos de violación de acceso a datos personales. Jurídicamente nuestra regulación lo contiene en el derecho de información ya descripto y en los principios de seguridad ya mencionados y de responsabilidad que implica que quien decida sobre el uso y tratamiento de datos responde por las violaciones a la normativa vigente en la materia. Es importante destacar que el artículo 8º del Decreto Nº 414/009, de 31 de agosto de 2009, reglamentario de la Ley, prevé expresamente la notificación a los titulares de datos cuando el responsable o encargado de la base de dato o tratamiento conozca de la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento que realice, que sean susceptibles de afectar de forma significativa los derechos del interesado, debiendo informarles de este extremo.

El último requerimiento consiste en auditoría y cumplimiento. Desde la perspectiva legal éstos básicamente contemplan todos los principios anteriores, con especial hincapié en los ya mencionados de legalidad, seguridad y responsabilidad y los derechos de acceso, rectificación, actualización, inclusión, supresión y de impugnación de valoraciones personales.

VII. Trabajo Futuro

Un objetivo a lograr en el corto plazo es la elaboración de un glosario de términos y conceptos que permiten caracterizar, entender y explicar las peculiaridades de la disciplina. En particular interesa documentar las visiones, ya sean convergentes o complementarias, que surgen desde el entendimiento e interpretaciones de esos conceptos tanto del dominio jurídico como del ingenieril.

Asimismo, importa promover la regulación expresa en Uruguay de la Privacidad por Diseño dentro del marco legal nacional de protección de datos personales, con la finalidad de exigir su efectivo cumplimiento, teniendo especialmente en cuenta la mirada técnico-ingenieril para evitar caer en exigencias irrealizables que transformen la ley en letra muerta.

En lo que respecta a metodologías y herramientas para el diseño e implementación de mecanismos que provean soporte automatizado para la aplicación de técnicas de PbD, en la actualidad se está investigando en dos líneas principales. Tomando como objetivo el

cumplimiento de las normas de privacidad que rigen sobre las bases de datos registrales en Uruguay, se está avanzando en la definición de herramientas que puedan ser utilizadas tanto por los proveedores de datos como por los colectores para garantizar/validar que la manipulación de los datos que albergan esas bases se realiza en forma acorde con lo estipulado por las normas referidas. En particular se está trabajando en el diseño de una API que exporta funcionalidades que permiten realizar consultas y modificaciones sobre una base de datos relacionales. La API está siendo concebida como un *wrapper* de consultas SQL que incorpora la interpretación de instrucciones orientadas a definir políticas de privacidad. Complementariamente se están investigando modelos algebraicos para la definición, manipulación y validación de políticas que incorporen reglas de los cuatro tipos esenciales de requerimientos de privacidad: Propósito, Visibilidad, Granularidad y Retención.

Concurrentemente se ha comenzado a investigar técnicas de anonimización y su aplicación en el dominio de Learning Analytics. Miembros del equipo están participando en un proyecto que tiene como principal objetivo desarrollar herramientas que permitan aplicar políticas de privacidad a los procesos de inferencia de información que se ejecuten sobre grandes colecciones de datos provenientes de un entorno educativo.

VIII. Agradecimientos

Los autores desean agradecer los comentarion e indicaciones brindados por los evaluadores anónimos.

Referencias

[1] M. Bauzá, *Derechos Fundamentales*, Privacidad y Tecnología en equilibrio. Unidad Reguladora y de Control de Datos Personales, Montevideo 2013.

[2] A. Cavoukian, *Privacy by Design: The 7 Foundational Principles*, reporte técnico, Comisionada de Información y Privacidad de Ontario, enero 2011 (versión revisada).

[3] D. Hurley, La estrella polar: Los derechos humanos en la sociedad de la información, versión en español, Auditoría Democrática Andina, Quito 2003.

[4] G. Romero, Interés público y protección de datos personales con especial referencia a los Derechos Humanos, Seminario regional de Protección de Datos REDIPD, Montevideo 2010.

[5] Resolución 2012/484/UE de la Comisión Europea, de 21 de agosto de 2012

[6] V. Pérez Asinari, Impacto en Uruguay del Nuevo Reglamento de la Unión Europea sobre Protección de Datos Personales, Revista Uruguaya de Protección de Datos Personales, Unidad Reguladora y de Control de Datos Personales, Número 1- Agosto 2016, Montevideo.

[7] A. Cavoukian y C. Popa, Privacy by ReDesign: A Practical Freamework for Implementation. Information and Privacy Commissioner of Ontario, Noviembre 2011.

[8] J. Hoepman, *Privacy Design Strategies*, ICT Syst. Secur. Priv. Prot. Adv. Inf. Commun. Technol., vol. 428, pp. 446–459, 2014.

[9] D. J. Solove, *A Taxonomy of Privacy*, Univ. Pa. Law Rev., vol. 154, no. 3, pp. 477–560, Jan. 2006.

[10] G. Dezanis, J. Domingo-Ferrer, m. Hansen, J-H Hoepman, D. le Métayer, R. Tirtea, S. Schiffner, *Privacy and Data Protection by Design – from policy to engineering,* ENISA, 2014.

[11] Bier C., Birnstill P., Krempel E., Vagts H., Beyerer J., *Enhancing Privacy by Design from a Developer's Perspective*. In: Preneel B., Ikonomou D. (eds) Privacy Technologies and Policy. APF 2012. LNCS, vol 8319. Springer, 2014.

[12] S. Gürses, C. Troncoso, C. Diaz, *Engineering Privacy by Design Reloaded*, Amst. Priv. Conf., 2015.

[13] S. Gürses, C. Troncoso, C. Diaz, *Engineering Privacy by Design,* In Computers, Privacy & Data Protection, page 25, Brussels, 2011.

[14] T. Antignac, D. Le Métaver, *Privacy by Design: From Technologies to Architectures (Position Paper)*. LNCS 8450, pp 1-17, 2014.

[15] K. Ghazinour, M. Majedi, K. Barker, A Lattice-based Privacy Aware Access Control Model. International Conference on Computational Science and Engineering, 2009.

[16] C. Levallois-Barth, H. Zylberberg, *A Purpose-Based Taxonomy for Better Governance of Personal Data in the Internet of Things Era: The Example of Wellness Data*, Data Protection and Privacy; (In)visibilities and Infraestructures, Law, Governance and Technology Series, volume 36, pp 139-161, Springer, 2016.