NOTA TÉCNICA

INTRODUCCIÓN A LIINE4DU 1.0: UNA NUEVA METODOLOGÍA PARA EL MODELADO DE AMENAZAS PARA LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS

Octubre 2024

CONTENIDOS

I. RESUMEN EJECUTIVO

La gestión de riesgos consiste en pensar en el futuro y lidiar con los problemas potenciales (amenazas) antes de que se conviertan en problemas reales (incidentes). Se trata de un proceso proactivo para gobernar las incertidumbres que amenazan el éxito de una actividad: hay que identificar, evaluar y priorizar los riesgos, para después coordinar esfuerzos y decisiones para minimizar, monitorizar y controlar su probabilidad o impacto. Este proceso permite incluso tomar decisiones sobre si llevar a cabo o no la actividad si se considera que el riesgo involucrado es inaceptable o no se puede gestionar.

Las organizaciones necesitan gestionar los riesgos de los proyectos, los riesgos financieros, los riesgos de protección (seguridad en el sentido de *safety*), los riesgos de ciberseguridad, los riesgos operativos, los riesgos de mercado, los riesgos reputacionales, los riesgos legales, etc. Cuando se tratan datos personales, es imprescindible llevar a cabo otro proceso de gestión de riesgos: el relativo a los derechos y libertades de los interesados, personas físicas potencialmente afectadas por dicho tratamiento de datos personales (empleados, clientes, usuarios, proveedores, etc.). Estos riesgos para los derechos y libertades pueden derivarse de la mera existencia de dicho tratamiento (tratamiento autorizado) o de violaciones de la seguridad de los datos personales (tratamiento no autorizado).

Esta nota se centra en el modelado de amenazas para la privacidad, el proceso sistemático de identificación, comprensión y comunicación de amenazas, y sus correspondientes métodos de prevención, para proteger los fines del tratamiento de datos personales. El modelado de amenazas para la privacidad implica comprender, de manera sistemática, lo que puede salir mal mediante un enfoque proactivo y estructurado.

Aunque el modelado de amenazas para la privacidad se puede utilizar al diseñar sistemas que preserven la privacidad, definir los requisitos de protección de datos y facilitar una mejor comunicación entre las partes interesadas durante las fases de diseño, implementación y prueba, esta nota explora, principalmente, la aplicación del modelado de amenazas para la privacidad en la gestión de riesgos. Cuando se revisan y actualizan periódicamente a medida que el tratamiento o su contexto evolucionan o surgen nuevas amenazas, los modelos de amenazas para la privacidad apoyan el análisis de riesgos y la evaluación de impacto, el análisis de errores, debilidades y vulnerabilidades y la planificación de mitigaciones de manera informada y consciente de las amenazas específicas que existen.

Por lo tanto, un modelo de amenazas para la privacidad puede ser esencial para llevar a cabo evaluaciones de impacto relativas a la protección de datos (EIPD) eficaces. El proceso de modelado de amenazas no es obligatorio y no sustituye a la EIPD ni al proceso de gestión de riesgos, pero puede ser una herramienta muy versátil y potente cuyo producto o salida (principalmente, los escenarios de riesgo e impactos potenciales para los derechos y libertades de los interesados) mejora los resultados obtenidos, permite ejercer mejor la responsabilidad proactiva y puede ahorrar tiempo y esfuerzo a las diferentes partes interesadas.

Si bien la metodología LINDDUN es un marco sólido y maduro para el modelado de amenazas para la privacidad, la AEPD ha encontrado algunos inconvenientes al usarlo específicamente para ayudar con el cumplimiento del RGPD y realizar una EIPD. Por ello se ha propuesto el nuevo marco LIINE4DU, basado en LINDDUN, pero centrado en la protección de los derechos y libertades. Las categorías de amenazas identificadas son diferentes, de ahí el nuevo acrónimo. Algunas categorías son coherentes con el enfoque de LINDDUN, y otras han sido modificadas o añadidas para alinearlas con el objetivo principal

del nuevo marco: la protección de datos, el cumplimiento normativo y la protección de los derechos y libertades individuales en el contexto de las EIPD.

Una vez identificadas y probadas las nuevas categorías de amenazas en diferentes proyectos e iniciativas, se está trabajando en el análisis de los impactos en los derechos y libertades de los interesados que conlleva cada tipo de amenaza de forma explícita y cómo se podrían mitigar estas amenazas. Además, se propondrán nuevos árboles de amenazas para la privacidad para ayudar a los profesionales a utilizar el marco propuesto.

II. TÉRMINOS Y DEFINICIONES

En el contexto de esta nota:

‘datos personales’ significa toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; (extraído del RGPD).

‘amenaza’ significa cualquier circunstancia o evento con el potencial de afectar negativamente a las operaciones de una organización (incluida la misión, las funciones, la imagen o la reputación), a los activos de una organización, a personas físicas, a otras organizaciones, al medio ambiente o a la Nación (extraído del NIST, adaptado).

‘incidente’ significa la ocurrencia o materialización de una amenaza que tiene efectos negativos reales (extraído del NIST, adaptado).

‘vulnerabilidad’ significa cualquier condición que permite que una amenaza se materialice y produzca un incidente (extraído del NIST, adaptado).

‘riesgo’ significa el grado en que una entidad se ve afectada por una amenaza y que, por lo general, es función de: (i) los impactos adversos que surgirían si la amenaza se materializa y produce un incidente; y (ii) la probabilidad de que esto ocurra (extraído del NIST, adaptado).

‘impacto’ significa la magnitud del daño que puede esperarse que resulte de los efectos que produce un incidente (extraído del NIST, adaptado).

‘probabilidad’ significa la posibilidad o expectativa de que algo suceda, ya sea definida, medida o estimada (objetiva o subjetivamente), o en términos de descriptores generales (como raro, improbable, probable, casi seguro), frecuencias o probabilidades matemáticas (extraído de ENISA).

‘gestión del riesgo’ significa el desarrollo y aplicación estructurados y continuos de la cultura, la política, los procedimientos y las prácticas de gestión dirigidas a las tareas de identificación, análisis, evaluación y control de la respuesta al riesgo (extraído de ENISA).

‘escenario’ significa un conjunto predefinido de eventos y condiciones que describen un incidente o daño relacionado con algún aspecto de las operaciones de una organización para respaldar la realización de un análisis, el desarrollo de una estrategia o un plan, o la realización de ejercicios (extraído de ENISA, adaptado).

‘proceso’ significa un conjunto organizado de tareas que emplea unos recursos para transformar unas entradas en salidas o resultados (extraído de ENISA).

III. INTRODUCCIÓN

La gestión de riesgos consiste, esencialmente, en pensar en el futuro y tomar medidas para lidiar con los problemas potenciales (amenazas) antes de que se conviertan en problemas reales (incidentes). Se trata de un proceso proactivo para gobernar las incertidumbres que amenazan el éxito de una actividad: hay que identificar, evaluar y priorizar los riesgos, para después coordinar esfuerzos y decisiones para minimizar, monitorizar y controlar su probabilidad o impacto. La gestión de riesgos se puede aplicar a las actividades personales (por ejemplo, en la planificación de un viaje por carretera) y a las actividades comerciales (por ejemplo, al lanzamiento de un nuevo servicio). La gestión de riesgos es una herramienta crucial para determinar qué actividades se pueden realizar y cuáles deben evitarse ya que representan un riesgo inmanejable o inaceptable para las personas u organizaciones.

Consideremos el ejemplo del viaje por carretera. Antes de tomar cualquier decisión, se comienza por anticipar lo que podría salir mal, todas las amenazas (pensar). Por ejemplo, el coche puede averiarse, nos podemos perder, quedarnos sin combustible o el tiempo puede ser malo para viajar. Una vez que se identifican estas amenazas, se intentan evaluar los riesgos específicos asociados, es decir, la probabilidad de que ocurran estas amenazas y la gravedad de sus impactos. Con esta información, para nuestro viaje en particular, capacidades de conducción, automóvil y ruta, podemos tratar de mitigar los riesgos evaluados que sean más significativos (actuar). Por ejemplo, podemos llevar nuestro viejo vehículo a revisión justo antes del viaje para reducir la posibilidad de una avería. O contratar una póliza de seguro. Podemos usar un GPS o mapa para seguir la ruta e incluso tener un sistema de respaldo en caso de que perdamos la señal porque no tenemos un buen sentido de la orientación en carreteras que no conocemos. Podemos asegurarnos de que el depósito de combustible esté lleno y planificar paradas en estaciones de servicio por el camino, etc. El pronóstico del tiempo podría sugerir que es mejor no emprender el viaje en absoluto. O podemos decidir que nuestro coche no es eléctrico no es un medio de transporte sostenible y, por lo tanto, no debemos utilizarlo.

En el ejemplo de la actividad comercial relacionado con el lanzamiento de un nuevo servicio, se deben gestionar al menos cuatro tipos de riesgo. En este caso, hay que tener en cuenta los riesgos del proyecto, como los retrasos en la planificación porque el desarrollo del software tarda más de lo esperado o porque hay problemas técnicos que implican errores o fallos que afectan a la experiencia del usuario. También se deben gestionar los riesgos financieros, como los excesos de presupuesto debido a gastos imprevistos o déficits de ingresos, ya que es posible que el servicio no atraiga inicialmente a suficientes clientes. Además, es necesario gestionar los riesgos de protección que afectan a la vida humana o al medio ambiente. Por ejemplo, si el servicio entrega alimentos o implica operaciones peligrosas para el personal. Por último, se deben gestionar los riesgos de ciberseguridad que podrían afectar a la continuidad del negocio, permitir actividades fraudulentas o comprometer los datos sensibles para el negocio. Si bien estos cuatro tipos de riesgo surgen de diferentes amenazas, tienen impactos diferentes y pueden ser gestionados con estrategias muy diferentes, todos ellos están interrelacionados y deben integrarse en un único proceso de gestión de riesgos. También podría ser necesario evaluar otro tipo de riesgos como los riesgos operativos, los riesgos de mercado, los riesgos reputacionales, los riesgos legales, etc. Al considerar estos riesgos adicionales y tomar las medidas adecuadas, la empresa puede mejorar las posibilidades de un lanzamiento exitoso del servicio. En algunos casos, por el contrario, se puede decidir cancelar el proyecto porque implica un riesgo inaceptable.

En los casos que impliquen el tratamiento de datos personales, es imprescindible llevar a cabo otro proceso de gestión de riesgos: el relativo a los derechos y libertades de los interesados, personas físicas potencialmente afectadas por dicho tratamiento de datos personales (empleados, clientes, usuarios, proveedores, etc.). Estos riesgos para los derechos y libertades pueden derivarse de la existencia de dicho tratamiento (tratamiento autorizado) o de violaciones de la seguridad de los datos personales (tratamiento no autorizado). Una vez más, la gestión de estos riesgos debe integrarse con la gestión global de riesgos del tratamiento (protección de datos desde el diseño).

Los riesgos de protección de datos provienen de amenazas relacionadas con cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. Además, dependen de la naturaleza, el alcance, el contexto y los fines del tratamiento.

Esta nota se centra en el modelado de amenazas, el proceso sistemático de identificación, comprensión y comunicación de amenazas, y sus correspondientes métodos de prevención, para proteger los fines del tratamiento. El modelado de amenazas para la privacidad implica comprender de manera sistemática lo que puede salir mal, utilizando un enfoque proactivo y estructurado. Es como una tormenta de ideas pesimista que sigue un método o marco específico y se basa en una colección de conocimientos reutilizables, como bibliotecas y catálogos de amenazas o árboles de ataque. Puede ser un proceso crucial para garantizar que se respete la privacidad y se cumpla con la normativa de protección de datos, pero sin duda se trata de una tarea compleja.

IV. MODELADO DE AMENAZAS PARA LA PRIVACIDAD

A. AMENAZAS PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS

Los métodos de modelado de amenazas más extendidos y maduros se centran en la seguridad y la ciberseguridad, pero no en la privacidad o la protección de datos[1]. De hecho, un error común en el modelado de amenazas para la privacidad es no tener en cuenta aspectos más allá de las brechas de datos personales y de los incidentes que afectan estrictamente a la confidencialidad de los datos.

A diferencia del modelado de amenazas para la ciberseguridad, el modelado de amenazas para la privacidad requiere considerar el daño potencial a los derechos y libertades de las personas en relación con el tratamiento de sus datos personales, no a los activos u organizaciones (daños financieros, de reputación, etc.). También debe tener en cuenta una fuerte dependencia del contexto (social, legal, geopolítico, etc.) y del ciclo de vida de los datos personales, entendiendo cómo fluyen a través de las organizaciones, sistemas y servicios e identificando posibles incidentes en cada etapa (las amenazas son diferentes durante la recogida de los datos que, durante la retención, por ejemplo).

Además, las amenazas pueden materializarse por el mero hecho de que el propio tratamiento se lleve a cabo, o a través de acciones neutras o incluso benignas (el daño puede ser completamente involuntario), no solo a través de actividades maliciosas realizadas por adversarios, como en el caso de la ciberseguridad. Hay que tener en cuenta que el modelado de amenazas para la ciberseguridad suele centrarse en la identificación de posibles vectores de ataque y vulnerabilidades que los actores maliciosos podrían explotar. Por último, el cumplimiento de las normativas es un aspecto esencial que debe analizarse a la hora de realizar el modelado de amenazas para la privacidad, no el cumplimiento tradicional de normas o marcos de seguridad como la ISO/IEC 27001 o los del NIST, considerados habitualmente al realizar modelado de amenazas para la ciberseguridad.

Algunas de las aplicaciones principales de los modelos de amenazas para la privacidad son el diseño de sistemas que preserven la privacidad, incluyendo requisitos de protección de datos desde el principio gracias a su capacidad para anticipar posibles problemas para los derechos y libertades de los interesados. Los modelos de amenazas dan soporte a la protección de datos desde el diseño, ya que permiten seleccionar las medidas técnicas y organizativas adecuadas para gestionar amenazas específicas. Además, facilitan una mejor comunicación con las partes interesadas durante las fases de diseño, implementación y prueba.

El modelado de amenazas para la privacidad también puede ser una herramienta poderosa para la gestión de riesgos de protección de datos, específicamente en tres áreas diferentes (figura 1):

1. Análisis de riesgos y evaluación de impacto conscientes de las amenazas específicas: Un análisis de riesgos puede considerarse como la combinación de un modelo de amenazas (identificar lo que puede salir mal), un modelo de consecuencias adversas (analizar lo que sucede cuando las cosas van mal, en relación con el impacto) y un modelo de vulnerabilidad (evaluar la posibilidad de que las cosas salgan mal, en relación con la probabilidad). El primero a menudo se olvida, lo que hace que los profesionales pierdan el tiempo analizando y evaluando escenarios imposibles, cuando estos escenarios podrían provenir directamente de un proceso de modelado de amenazas. Este tipo de procesos

[1] Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). Threat modeling: a summary of available methods. Software Engineering Institute, Carnegie Mellon University.

puede ser de gran ayuda en este sentido, así como en el modelado de los impactos sobre los derechos y libertades de los interesados (consecuencias adversas y su gravedad).

2. Análisis de errores, debilidades y vulnerabilidades conscientes de las amenazas específicas: Una vez más, estos tipos de análisis suelen basarse en escenarios y pueden guiarse por los resultados de un proceso de modelado de amenazas, buscando problemas reales porque ciertos escenarios específicos son los que deben generar más preocupación. Un modelo de amenazas para la privacidad proporciona una comprensión detallada de las amenazas que son realmente posibles, lo que ayuda a los equipos a crear escenarios más realistas y relevantes. También puede apoyar en la realización de ejercicios de preparación para respuesta a incidentes o de equipo rojo (*red teaming*) en diferentes contextos.

3. Planificación de la mitigación consciente de las amenazas específicas: El amplio catálogo de salvaguardas y controles de privacidad disponibles dificulta la toma de decisiones informadas sobre qué opción es la mejor para cada caso a la hora de diseñar e implementar las medidas técnicas y organizativas adecuadas. Un modelo de amenazas ofrece orientación para ayudar a los profesionales a abordar problemas específicos de privacidad con soluciones específicas, por escenario, en lugar de escoger soluciones de manera global o genérica. Este enfoque permite proponer una estrategia de mitigación adaptada a las necesidades reales.

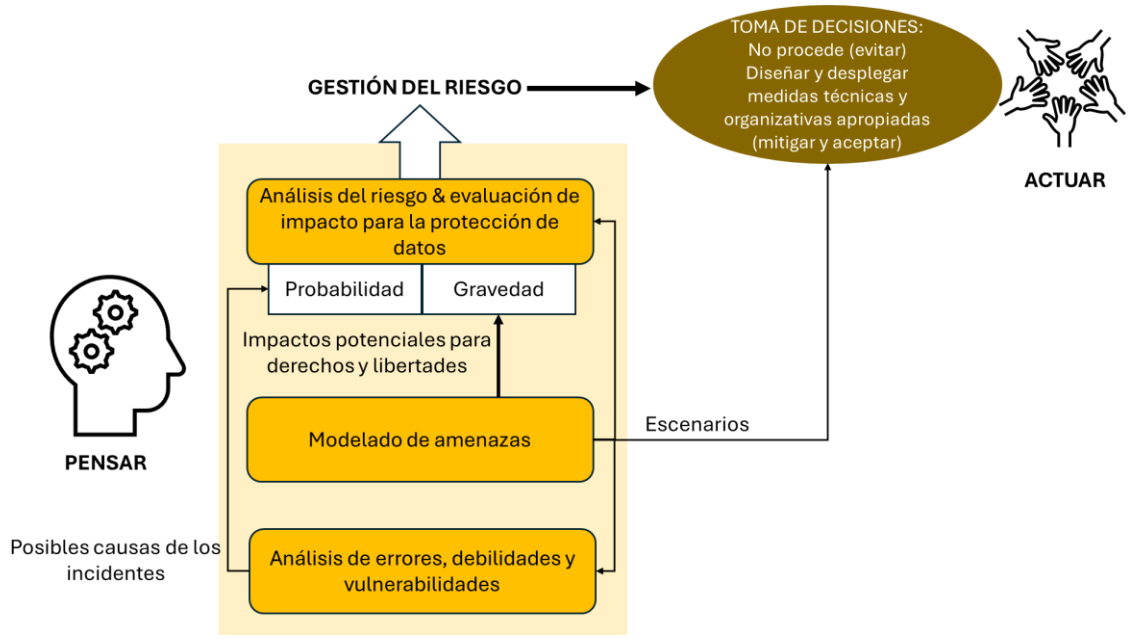

Figura 1. Modelado de amenazas para la privacidad que respalda la gestión de riesgos de protección de datos

La toma de decisiones de la figura 1 puede implicar no continuar con el tratamiento de datos personales que se estaba diseñando (gestión de riesgos basada en evitar el riesgo) o hacerlo mitigando adecuadamente los riesgos evaluados. Y hacerlo mediante el diseño y despliegue de medidas técnicas y organizativas adecuadas (gestión de riesgos basada en la mitigación del riesgo y en la aceptación proactiva).

Es esencial comprender que los modelos de amenazas solo son útiles si se revisan y actualizan periódicamente a medida que el tratamiento o su contexto evolucionan, o surgen

nuevas amenazas. Los modelos de amenazas obsoletos o incompletos solo pueden conducir a decisiones equivocadas. De todos modos, el proceso de modelado de amenazas debe llevarse a cabo teniendo en cuenta las características, matices y especificidades del tratamiento de datos en particular, teniendo en cuenta su contexto técnico, social, legal y organizativo.

B. MODELADO DE AMENAZAS PARA LA PRIVACIDAD Y EL RGPD

El RGPD establece principios y requisitos para la protección de los datos personales, incluida la minimización de datos, la limitación de la finalidad y la seguridad del tratamiento, por mencionar solo algunos ejemplos. Al identificar y ayudar a mitigar sistemáticamente las amenazas para la privacidad, el modelado de amenazas puede ayudar a las organizaciones a garantizar el cumplimiento de estos principios y requisitos del RGPD.

Además, como se ha mencionado anteriormente, el RGPD hace hincapié en el concepto de protección de datos desde el diseño, que requiere integrar medidas y garantías de protección de datos, teniendo en cuenta la naturaleza, el alcance, el contexto, la finalidad y los riesgos para los derechos de las personas físicas al diseñar las actividades de tratamiento de datos personales. Los modelos de amenazas para la privacidad pueden ayudar a integrar las consideraciones de privacidad en el diseño del tratamiento, abordando de forma proactiva las amenazas específicas que este implica.

El RGPD se centra en proteger los datos personales de diversas amenazas, como las provocadas por el tratamiento autorizado, el acceso no autorizado, las brechas de datos o el uso indebido. El modelado de amenazas para la privacidad puede ayudar a identificar amenazas específicas, como la vinculación, la identificación o la divulgación de datos, y a desarrollar mitigaciones específicas para hacer frente a todas ellas.

Además, el RGPD requiere que las organizaciones demuestren su cumplimiento a través de la documentación adecuada y medidas de responsabilidad proactiva. Un modelo de amenazas para la privacidad puede proporcionar documentación clara y estructurada de las amenazas identificadas, sus impactos y medidas de mitigación, que se puede utilizar para demostrar el cumplimiento requerido. El cumplimiento es un proceso continuo que requiere un seguimiento y una actualización constantes de las medidas de protección de datos. La mejora continua se puede lograr mediante la actualización periódica del modelo de amenazas.

Por último, el RGPD obliga a las organizaciones a realizar evaluaciones de impacto de la protección de datos (EIPD) para las actividades de tratamiento que entrañen un alto riesgo para los derechos y libertades de las personas. Las metodologías de modelado de amenazas para la privacidad proporcionan un enfoque estructurado para identificar y evaluar las amenazas que puede ser esencial para que las EIPD sean eficaces (véase la figura 1).

En primer lugar, permite la identificación y el análisis sistemáticos de todo lo que podría salir mal. Ayuda a desglosar las amenazas de alto nivel en elementos específicos y procesables y, como se ha explicado antes, garantiza que no se pase por alto ningún aspecto importante, lo que ayuda a priorizar.

En segundo lugar, el modelo de amenazas ayuda a identificar las contramedidas adecuadas para cada amenaza, lo que garantiza que la EIPD incluya estrategias específicas y prácticas para gestionar los riesgos para la privacidad.

En tercer lugar, el enfoque estructurado de un modelo de amenazas garantiza que todas las amenazas identificadas, su impacto en los derechos y libertades fundamentales y las medidas de mitigación estén bien documentadas. Esta documentación puede ser crucial para demostrar el cumplimiento de la normativa de protección de datos como el RGPD.

En cuarto lugar, como ya se ha mencionado, el modelo de amenazas para la privacidad permite la monitorización y la actualización continuas de la EIPD a medida que el tratamiento, o su contexto, evoluciona o surgen nuevas amenazas. Así se fomenta un enfoque proactivo de la privacidad, ayudando a anticipar y abordar posibles dificultades antes de que se conviertan en problemas significativos.

Por último, la naturaleza visual y estructurada de los modelos de amenazas facilita la comunicación de los riesgos para la privacidad y las estrategias de mitigación para las partes interesadas, incluidas la dirección, los organismos reguladores o las autoridades de control. Facilita la colaboración entre diferentes equipos, lo que garantiza una comprensión y un enfoque exhaustivos de la protección de datos.

En conclusión, cabe señalar que el proceso de modelado de amenazas no es obligatorio y no sustituye a la EIPD ni al proceso de gestión de riesgos. Puede ser un mecanismo adicional de responsabilidad proactiva y una herramienta muy poderosa cuyos productos mejoran la calidad de los resultados obtenidos en tareas específicas.

Por ejemplo, al llevar a cabo una EIPD, una vez que se haya elaborado una descripción sistemática de las operaciones de tratamiento previstas y los fines del tratamiento y se haya realizado una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con los fines, el modelo de amenazas puede ayudar a evaluar los riesgos para los derechos y libertades de los interesados y a seleccionar las medidas previstas para hacer frente a dichos riesgos. Incluidas las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. Además, puede ahorrar tiempo y esfuerzo a las diferentes partes interesadas.

Ejemplo 1

De acuerdo con la guía de la AEPD "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", la identificación y análisis de los factores de riesgo para los derechos y libertades de las personas físicas es el paso previo a la evaluación del nivel de riesgo inherente al tratamiento de datos personales. En esta guía, se enumeran diferentes factores de riesgo en función de los fines del tratamiento, los tipos de uso de los datos, etc. Los escenarios de brecha de datos se mencionan explícitamente, pero no se mencionan otros tipos de escenarios de riesgo.

La brecha de datos como escenario de riesgo y todos los factores de riesgo enumerados en dicha guía no son exhaustivos, sino un conjunto mínimo establecido en la normativa vigente[2], y el responsable del tratamiento debe identificar aquellos escenarios y factores de riesgo que son específicos del tratamiento e incluirlos en su evaluación.

El modelado de amenazas para la privacidad permite ampliar el conjunto mínimo de escenarios de riesgo identificados en la guía ya mencionada, teniendo en cuenta todas las amenazas que pueden materializarse. Es decir, todas las cosas que podrían salir mal y la gravedad de los impactos específicos que podrían tener en los derechos y libertades de los interesados (análisis de riesgos y evaluación de impacto conscientes de las amenazas específicas).

[2] Principalmente la normativa de protección de datos, los dictámenes y decisiones vinculantes del CEPD, y la normativa sectorial aplicable.

Ejemplo 2

Según la guía de la AEPD "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", debe evaluarse el impacto y la probabilidad de daño a las personas como resultado del tratamiento de datos personales.

El modelado de amenazas para la privacidad permite una evaluación más exhaustiva, por escenario de riesgo, del impacto y la probabilidad de daño a las personas, teniendo en cuenta las amenazas específicas que pueden materializarse y cómo podrían materializarse (análisis de errores, debilidades y vulnerabilidades conscientes de las amenazas específicas).

Ejemplo 3

De acuerdo con la guía de la AEPD "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", el responsable o el encargado del tratamiento debe gestionar el riesgo teniendo en cuenta las peculiaridades específicas de su tratamiento de datos. En este sentido, el responsable o encargado del tratamiento debe seleccionar o definir las medidas y salvaguardas más adecuadas para hacer frente a los riesgos específicos que se hayan identificado.

El modelado de amenazas para la privacidad permite una selección más fundamentada y específica, por escenario de riesgo, de medidas y salvaguardas de entre las enumeradas en la guía mencionada, teniendo en cuenta las amenazas específicas que pueden materializarse y cómo podrían evitarse o mitigarse (planificación de la mitigación consciente de las amenazas específicas).

V. ANTECEDENTES

Si bien muchas investigaciones y documentación describen amenazas para la privacidad y la protección de datos, muy pocas proporcionan un método para identificar realmente estas amenazas dentro de aplicaciones, servicios, procesos o proyectos específicos. Se requiere una orientación clara y práctica para determinar si existen amenazas concretas.

Existen extensiones específicas, extraoficiales, para los métodos tradicionales de modelado de amenazas para la ciberseguridad, como por ejemplo *Elevation of Privacy*[3] (una extensión para *Elevation of Privilege*). Pero esta nota se centra en los métodos y marcos dedicados de manera específica a la privacidad y la protección de datos.

El único método de modelado de amenazas para la privacidad de este tipo publicado y ampliamente utilizado es LINDDUN[4]. LINDDUN es un marco de modelado de amenazas para la privacidad diseñado para ayudar a identificar y mitigar las amenazas para dicha privacidad en los sistemas de software. LINDDUN es un acrónimo que representa los siete tipos de amenazas a la privacidad que aborda[5]:

- *Linking*: Asociar diferentes datos o actividades de un individuo entre sí para obtener más información sobre el individuo o su grupo.
- *Identifying*: Aprender la identidad de un individuo a través de filtraciones, deducciones o inferencias.
- *Non-repudiation*: Poder atribuir una actividad a un individuo.
- *Detecting*: Deducir la implicación de un individuo en una actividad a través de la observación.
- *Data disclosure*: Recoger, almacenar, procesar o compartir datos personales en exceso.
- *Unawareness*: Informar, involucrar o empoderar a los individuos en el tratamiento de sus datos personales de manera insuficiente
- *Non-compliance*: Desviarse de las mejores prácticas, normas y legislación en materia de seguridad y protección de los datos.

LINDDUN sigue los mismos principios que el conocido método de modelado de amenazas de ciberseguridad STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*)[6]. Su enfoque intenta responder a las mismas cuatro preguntas:

1. ¿Qué estamos construyendo? El punto de partida para entender el sistema modelado es un diagrama de flujo de datos (*Data Flow Diagram* o DFD) dibujado con las mismas convenciones y vocabulario. Este diagrama representa los flujos de datos, los almacenes de datos, los procesos y las entidades externas del sistema, y permite destacar elementos relevantes para la privacidad y la protección de datos.

2. ¿Qué puede salir mal? Los tipos de amenazas para la privacidad mencionados antes impulsan este análisis, iterando de forma estructurada sobre cada componente del sistema. Los tipos de amenazas LINDDUN se utilizan para identificar sistemáticamente las posibles amenazas para la privacidad en cada elemento del DFD. Los árboles de amenazas pueden ayudar a dividir las amenazas complejas en sub-amenazas más manejables.

[3] Elevation of Privacy, https://github.com/WithSecureOpenSource/elevation-of-privacy
[4] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering, 16(1), 3-32.
[5] LINDDUN Privacy Threat Modelling, https://linddun.org/
[6] Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

3. ¿Qué vamos a hacer al respecto? Este paso está guiado por un catálogo de estrategias de mitigación y salvaguardas, que permite determinar las contramedidas adecuadas para mitigar el riesgo asociado a cada amenaza identificada.

4. ¿Hemos hecho un buen trabajo? El modelo producido y el método seguido deben ser evaluados para reflexionar sobre las lecciones aprendidas y mejorar los resultados en el futuro.

LINDDUN se ha utilizado en el pasado porque proporciona un enfoque sistemático para identificar y abordar las amenazas para la privacidad en las primeras etapas del ciclo de vida del desarrollo de software. Cubre una amplia gama de amenazas para la privacidad y garantiza la realización de un análisis exhaustivo. Además, se puede adaptar a las diferentes necesidades y niveles de complejidad de un proyecto.

Si bien LINDDUN es un marco sólido y maduro para el modelado de amenazas para la privacidad, hemos encontrado algunos inconvenientes al usarlo específicamente para ayudar con el cumplimiento del RGPD y realizar una evaluación de impacto relativa a la protección de datos. LINDDUN no siempre se alinea directamente con los principios y requisitos específicos del RGPD. Si bien ayuda a identificar amenazas para la privacidad, traducir sus resultados en medidas de cumplimiento del RGPD puede implicar un desafío. Además, LINDDUN se centra principalmente en las amenazas técnicas y puede que no aborde plenamente los aspectos organizativos y procedimentales del cumplimiento del RGPD o los aspectos relativos a los derechos y libertades de los interesados. Por lo tanto, la integración de los resultados de LINDDUN en una EIPD puede ser compleja y puede requerir un esfuerzo adicional para garantizar que se cubran todos los aspectos esenciales del RGPD.

VI. NUESTRA PROPUESTA

LINDDUN puede ser una herramienta valiosa para garantizar el cumplimiento del RGPD o para respaldar EIPD eficaces. Sin embargo, adecuar LINDDUN a las necesidades específicas de cumplimiento del RGPD puede requerir una personalización y adaptación significativas. Por este motivo hemos comenzado a trabajar en la propuesta de un nuevo marco, LIINE4DU y a realizar algunas validaciones iniciales[7].

Algunos de los aspectos esenciales de LINDDUN que permanecen en nuestro marco son:

- Es independiente de los agentes de amenaza, se centra en la materialización de las amenazas para la privacidad y en sus impactos, no en quién las materializa o por qué.
- El diagrama de flujo de datos (DFD) es la herramienta gráfica fundamental para modelar el tratamiento bajo estudio y guiar el proceso de identificación y análisis de amenazas.
- Se han utilizado como punto de partida algunos catálogos y un *corpus* de conocimientos de LINDDUN.
- El enfoque seguido se basa en las cuatro preguntas tradicionales propuestas en STRIDE.

Los cambios más importantes que implica nuestra propuesta se pueden resumir en:

- La atención se centra en la protección de los derechos y libertades de las personas y en el cumplimiento normativo (en relación con el RGPD).
- Las categorías de amenazas identificadas son diferentes, de ahí el nuevo acrónimo. Algunas categorías son coherentes con el enfoque de LINDDUN, y otras han sido modificadas o añadidas para alinearlas con el objetivo principal de nuestro marco: la protección de datos, el cumplimiento normativo y la protección de los derechos y libertades de las personas en el contexto de las EIPD. En concreto, hemos eliminado la categoría de *Non-compliance* (Incumplimiento desde el punto de vista regulatorio), ya que el tratamiento de datos que no cumple con la normativa no se puede implementar y es una categoría demasiado genérica para ser útil en nuestro contexto. Además, hemos añadido cuatro nuevas categorías: *Inaccuracy* (Inexactitud), *Exclusion* (Exclusión), *Data breach* (Brecha de datos) y *Deception* (Engaño).

Las categorías propuestas se resumen en la Tabla 1. Las tres últimas categorías están intrínsecamente ligadas a los procesos de gestión de riesgos de la organización y al diseño del tratamiento de datos y conllevan un incumplimiento directo del RGPD. Por el contrario, el resto de las categorías propuestas pueden afectar directamente a los derechos y libertades individuales desde una perspectiva más amplia y pueden implicar o no el incumplimiento de la normativa de protección de datos.

La amenaza de Brecha de datos es la frontera entre estos dos grupos de amenazas, ya que algunas de ellas pueden producirse por incumplimiento del RGPD (por no incorporar medidas de seguridad adecuadas, artículo 32 del RGPD) mientras que otras pueden ser inevitables. Hay que tener en cuenta que la mayoría de las brechas podrían ser evitadas por el responsable y el encargado del tratamiento mediante la aplicación de medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

[7] Beltrán, M., & de Salvador, L. (2024, August). Implications of Age Assurance on Privacy and Data Protection: A Systematic Threat Model. In *Annual Privacy Forum* (pp. 1-22). Cham: Springer Nature Switzerland.

Linking/ Vinculación	Esta amenaza implica relacionar diferentes datos o actividades del interesado para obtener más información sobre el interesado o sobre un grupo de personas al que pertenece.
Identifying/ Identificación	Esta amenaza implica conocer la identidad de un interesado directamente (a través del tratamiento de información identificable o de filtraciones, por ejemplo) o indirectamente (a través de la deducción o la inferencia, por ejemplo).
Inaccuracy/ Inexactitud	Esta amenaza implica el uso de datos obsoletos, erróneos, incompletos, sesgados o de baja calidad que pueden llevar a decisiones o acciones incorrectas, y a causar inconvenientes o incluso daños al interesado.
Non-repudiation/ No repudio	Esta amenaza implica la capacidad de atribuir una característica o actividad al interesado (algo que sabe, que es, que hace, etc.) cuando esto implica un impacto para sus derechos y libertades fundamentales.
Exclusion/ Exclusión	Esta amenaza implica no atender adecuadamente a un interesado, obstaculizando involuntaria o deliberadamente su participación o implicación en la vida física o digital.
Detecting/ Detección	Esta amenaza implica deducir la existencia de datos o la implicación del interesado en una actividad a través de la observación.
Data Breach/ Brecha de datos	Esta amenaza implica la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales por error, personas de confianza maliciosas o ciberataques.
Deception/ Engaño	Esta amenaza implica intentar influir, coaccionar o manipular intencionalmente al interesado para que tome decisiones no intencionadas, involuntarias y potencialmente dañinas, a menudo en contra de sus propios intereses.
Data Disclosure/ Divulgación	Esta amenaza implica recoger, almacenar, tratar o compartir/transferir datos personales en exceso.
Unawareness and Unintervenability/ Desconocimiento y falta de capacidad para intervenir	Esta amenaza implica demostrar de manera insuficiente el cumplimiento o informar, involucrar o empoderar a los interesados en el tratamiento de sus datos personales también de manera insuficiente.

Tabla 1. Categorías de amenazas en el marco LIINE4DU.

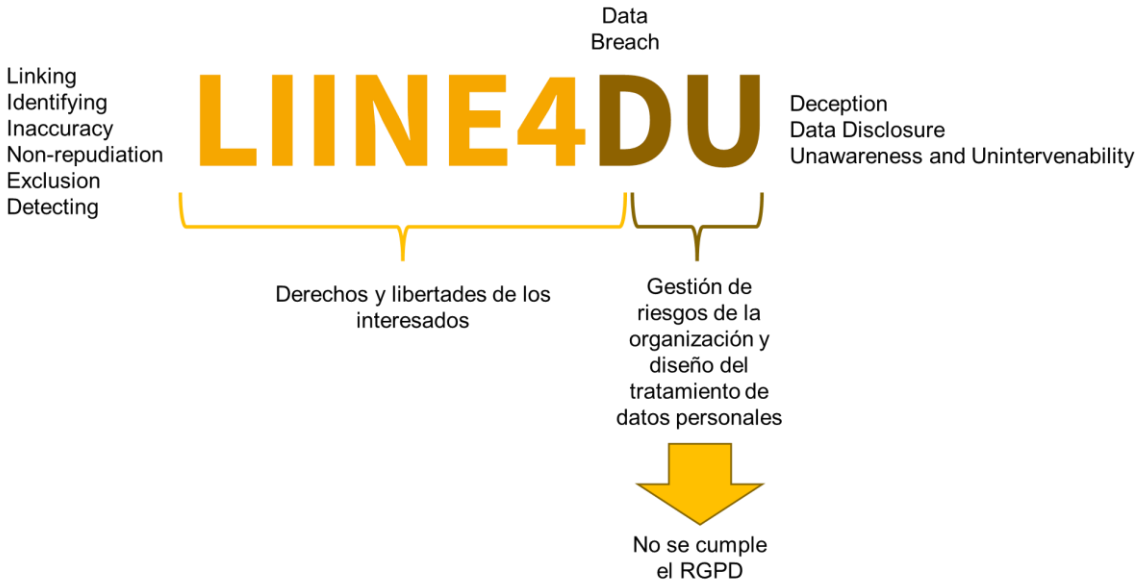

Figura 1. Resumen de las categorías de amenazas en el marco LIINE4DU.

Algunas aclaraciones adicionales pueden ser apropiadas en este punto:

- Un requisito previo para utilizar el marco LIINE4DU es la legitimidad y la licitud del tratamiento de datos personales modelado. El marco propuesto no considera el "incumplimiento" como una amenaza. Las amenazas relacionadas con tratamientos de datos personales con fines específicos ilegítimos determinados en el momento de la recogida de los datos personales, que no tienen una base legal o que violan claramente la normativa de protección de datos en cualquier otro aspecto (principalmente, en los artículos 5 a 50 del RGPD) no deberían modelarse, ya que no se puede llevar a cabo un tratamiento de datos personales que no cumpla con la normativa. No tendría sentido modelar sus potenciales impactos en los derechos y libertades de los interesados.
- De este modo, solo deben modelarse las amenazas derivadas de tratamientos de datos personales que ya se hayan evaluado inicialmente como legítimos, lícitos y que cumplen la normativa, ya que el marco propuesto se centra especialmente en cómo evitar o mitigar las amenazas identificadas y en comprender sus posibles impactos en los derechos y libertades de los interesados.
- Una vez utilizado el marco LIINE4DU, la existencia de amenazas en las últimas categorías del acrónimo (la mayor parte de las Brechas de datos, Engaño, Divulgación, Desconocimiento y falta de capacidad para intervenir) implica el incumplimiento del RGPD y directamente que el tratamiento de datos personales no debería llevarse a cabo hasta que se eviten dichas amenazas. En la siguiente tabla se ofrece una primera aproximación (no exhaustiva) a las infracciones más comunes en relación con estas categorías de amenazas:

Data Breach/ Brecha de datos	• Artículo 5: “Integridad y confidencialidad”. • Artículo 25: Protección de datos desde el diseño y por defecto. • Artículo 32: Seguridad del tratamiento.
Deception/ Engaño	• Artículo 5: “lealtad”, “transparencia”, “limitación de la finalidad”, “minimización de datos”. • Artículo 25: Protección de datos desde el diseño y por defecto.
Data Disclosure/ Divulgación	• Artículo 5: “lealtad”, “limitación de la finalidad”, “minimización de datos”, “limitación del plazo de conservación”. • Artículo 25: Protección de datos desde el diseño y por defecto.
Unawareness and Unintervenability/ Desconocimiento y falta de capacidad para intervenir	• Artículo 5: “transparencia”, “exactitud”, “responsabilidad proactiva”. • Artículos 12 a 21 en relación con los derechos del interesado. • Artículo 22: Decisiones individuales automatizadas, incluida la elaboración de perfiles. • Artículo 25: Protección de datos desde el diseño y por defecto.

- Las amenazas en el resto de categorías del acrónimo (Otros, en la figura 2) pueden implicar o no el incumplimiento de la normativa de protección de datos. El proceso de modelado de amenazas para la privacidad debe ayudar al responsable del tratamiento a identificar, evitar o mitigar suficientemente los riesgos asociados.
- Una vez que el tratamiento de datos cumple con la regulación (después de dos comprobaciones, la inicial y la que permite LIINE4DU), las salidas del proceso de modelado de amenazas se pueden utilizar para las diferentes aplicaciones “conscientes de las amenazas específicas” mencionadas en la sección IV de este documento.

En la figura 2 se resume el contexto para llevar a cabo el modelado de amenazas para la privacidad con LIINE4DU. Como se ha mostrado, puede ser una extensión muy versátil y potente (véanse los ejemplos en la sección IV.B) de la guía y las herramientas ya existentes para la gestión del riesgo y la evaluación de impacto en el tratamiento de datos personales.

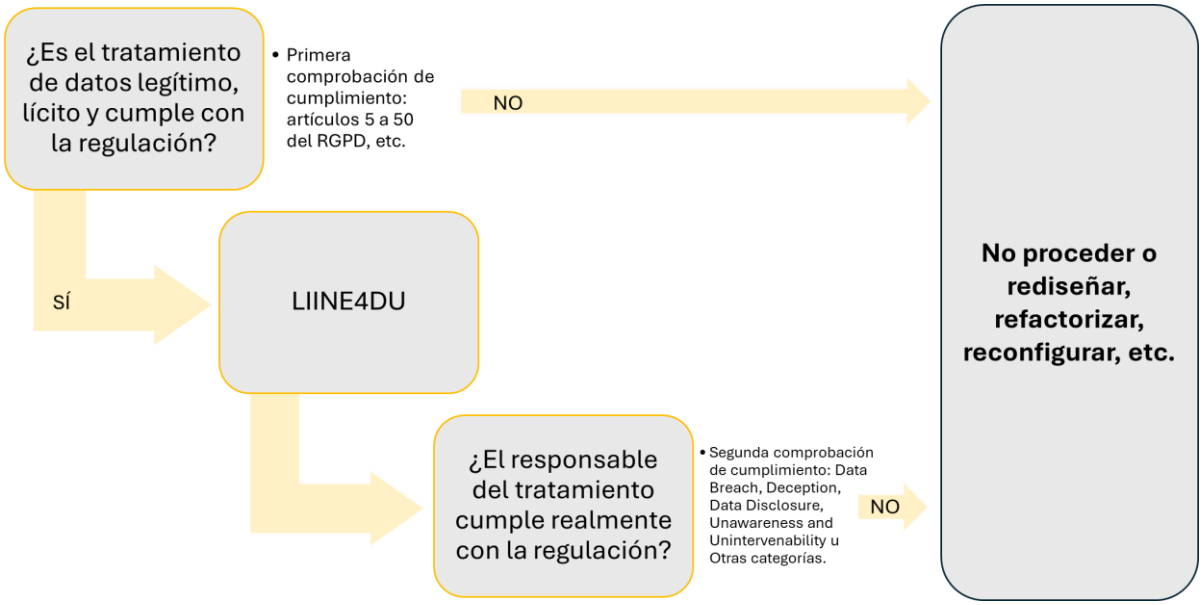

Figura 2. Aplicación del marco LIINE4DU en las etapas iniciales del diseño de un tratamiento de datos personales.

VII. SIGUIENTES PASOS

Una vez identificadas y validadas las nuevas categorías de amenazas en diferentes proyectos e iniciativas, estamos trabajando en el análisis de las primeras categorías de amenazas. Se trata de analizar LIINEDD (excluyendo el "Engaño", la "Divulgación" y el "Desconocimiento y falta de capacidad para intervenir", ya que, como ya se ha mencionado, implican un incumplimiento directo del RGPD), qué impactos en los derechos y libertades de los interesados conlleva cada amenaza de forma explícita, y cómo se podrían mitigar. Es esencial adoptar un enfoque basado en el riesgo, tan común en el ámbito de la protección de datos, para decidir sobre la implementación de las medidas técnicas y organizativas adecuadas para integrar las salvaguardas necesarias en el tratamiento para cumplir con los principios y requisitos del RGPD.

Además, es necesario generar nuevos árboles de amenazas. Los árboles de amenazas son útiles en el modelado de amenazas para la privacidad, como se ha demostrado en LINDDUN en los últimos años. Ayudan a dividir las amenazas complejas en componentes más manejables.

Hay que recordar que los árboles de amenazas son diagramas jerárquicos que representan amenazas potenciales, comenzando con un nodo raíz que representa una amenaza de alto nivel y ramificándose en sub-amenazas y factores contribuyentes. Un árbol de amenazas se compone de un nodo raíz (la amenaza principal o el problema de privacidad), ramas (sub-amenazas o aspectos específicos de la amenaza principal) y hojas (el nivel más granular de amenazas, que a menudo representan eventos, acciones, vulnerabilidades o vectores de ataque particulares).

Los árboles de amenazas garantizan claridad, ya que proporcionan una forma clara y estructurada de visualizar y comprender las amenazas complejas. Se aseguran de que se tengan en cuenta todas las posibles sub-amenazas y aspectos relevantes. Los árboles de amenazas se pueden completar y mejorar con preguntas y criterios orientativos, ejemplos e información adicional, como impactos o salvaguardas. Estamos trabajando en la creación de un primer árbol de amenazas para cada categoría de amenazas en nuestro modelo, junto con ejemplos detallados de su uso. Colegas de otras Autoridades de Protección de Datos, expertos en la realización de EIPD e investigadores ayudarán a revisar estos árboles para garantizar su completitud.

Los árboles se actualizarán a medida que evolucionen las amenazas o se identifiquen nuevas amenazas (esperamos nuevas versiones de LIINE4DU en el futuro). Tenemos la intención de involucrar a diferentes actores para analizar las amenazas potenciales de manera integral y aprovechar los proyectos e iniciativas existentes para guiar nuestros esfuerzos, tales como MITRE Pattern and Action Nomenclature Of Privacy Threats In Context (PANOPTIC)[8], Solove's taxonomy of privacy[9], NIST Problematic Data Actions[10] o el Data Privacy Vocabulary[11].

[8] MITRE PANOPTIC™, https://ptmworkshop.gitlab.io/#/panoptic
[9] Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3), 477–564. https://doi.org/10.2307/40041279
[10] NIST IR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems (2017), https://csrc.nist.gov/pubs/ir/8062/final
[11] W3C Data Privacy Vocabulary, https://w3c.github.io/dpv/2.0/dpv/