RESUMEN EJECUTIVO ESTUDIO AUTELSI "PRIVACY BY DESIGN"

DICIEMBRE 2014

RESUMEN EJECUTIVO ESTUDIO AUTELSI “PRIVACY BY DESIGN”

En el marco de actividades desarrolladas por el Grupo de Regulación de la Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI), se ha llevado a cabo durante los últimos meses un estudio acerca del principio de “Privacy by Design”, que junto a los principios de Privacidad por Defecto (“privacy by default”) y Responsabilidad (“accountability”) , todos ellos expresamente reconocidos en el Proyecto de Reglamento Europeo de Protección de Datos, en trámite de aprobación, en sus artículos 22 y 23, recogen los conceptos inspiradores de la prevención de la privacidad y el respeto a la protección de datos.

El objetivo del estudio no es otro que analizar las novedades e implicaciones que conlleva el cumplimiento de este principio y proponer aproximaciones que permitan a los asociados de AUTELSI y a las organizaciones, posicionarse en una mejor práctica de la privacidad y prepararse para abordar el cumplimiento del principio preventivo de la privacidad por diseño atendiendo a los previsibles requisitos legales recogidos en el proyecto Europeo de Protección de Datos.

Las conclusiones aquí recogidas se basan en la experiencia y conocimientos de los miembros participantes de este grupo de trabajo y en datos obtenidos a través de una encuesta dirigida a Asociados de AUTELSI que permitió entender el grado de sensibilización en cuanto a la gestión preventiva de la privacidad en el entorno de la organización.

El nuevo marco europeo de protección de datos está promoviendo el establecimiento de un “sistema de control de los riesgos” asociados al tratamiento de los datos personales, que, de manera preventiva, considere la necesidad de tener en cuenta la privacidad y la protección de los datos personales en ”todo” el ciclo de vida de la tecnología, desde la fase de diseño hasta su fin, tanto de los sistemas de información, como de las arquitecturas y redes de comunicación, los procesos productivos y de negocio, de tal manera que se entienda siempre la privacidad como una opción "por defecto".

Pero el reconocimiento del principio de PbD y su inclusión como principio general y como fuente de obligaciones en el proyecto de Reglamento Europeo de Protección de Datos, no es una novedad en el derecho europeo ni en la práctica de las organizaciones, sino que debe considerarse resultado de una evolución y que, bajo el concepto de “pensar antes de actuar”, orienta a la organización hacia la adopción de medidas preventivas frente a riesgos perjudiciales en el tratamiento.

Desde esa concepción, se nos plantea a las empresas y organizaciones, públicas o privadas o personas físicas en su ámbito profesional, como un principio ético, como una obligación preventiva, valorar la privacidad y el respeto al derecho a la protección de los datos personales desde la propia concepción de su tratamiento, desde que consideramos la posibilidad de utilizar tecnología susceptible de tratar datos personales, desde el mismo día en el que potencialmente podemos vulnerar la privacidad de nuestro conciudadanos, de los usuarios, de las personas.

La protección de los datos desde el diseño prestará especial atención a toda la gestión del ciclo de vida de los datos personales desde su recogida hasta su tratamiento y supresión, centrándose sistemáticamente en proporcionar amplias garantías procesales respecto de la exactitud, la confidencialidad, la integridad, la seguridad física y la supresión de los datos personales. Cuando el responsable del tratamiento haya llevado a cabo una evaluación de impacto relativa a la protección de datos, con arreglo a lo dispuesto en el artículo 33 del Proyecto de Reglamento Europeo de Protección de Datos, los resultados de dicha evaluación se tendrán en cuenta a la hora de desarrollar tales medidas y procedimientos.

Consideramos, por tanto, que hay tres aspectos (fases del tratamiento, obligaciones e intervinientes) que configuran el alcance general para la aplicación de este principio al que habrán de añadirse las obligaciones derivadas de los principios de Responsabilidad y

Privacidad por Defecto regulados en los arts. 22 y 23.2 del Reglamento Europeo que persiguen:

- Garantizar por defecto no solo que se trataran los datos necesarios y pertinentes en relación a la finalidad de uso, minimizando el tratamiento al máximo, evitando recoger ni conservar más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación e impidiendo que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas, garantizando que solo serán tratados por aquellos usuarios, trabajadores, colaboradores, que sean estrictamente necesario en atención al fin por el que se han recogido.
- Garantizar la información respecto a los tratamientos, proporcionando medios de control a los usuarios respecto a sus datos tratados, y la protección de los derechos de los usuarios, de los clientes personas físicas, de las personas identificadas o identificables, mediante la implantación de medidas de seguridad y procedimientos técnicos y organizativos apropiados, planificando y aplicando previamente el tratamiento, a lo largo de todo su ciclo de vida (recogida, generación, almacenamiento, conservación, comunicación, cancelación y eliminación del dato).
- Garantizar la rendición de cuentas por parte de los responsables de tratamiento, viéndose estos en la necesidad de documentar y acreditar la aplicación de las medidas determinadas en cada caso, dirigidas a garantizar el cumplimiento normativo en Protección de Datos “a lo largo de todo el ciclo de vida del tratamiento y de forma preventiva”.

Entendemos que la necesidad de gestionar la privacidad, ·”por defecto o por diseño”, puede estar vinculada a una necesidad del negocio, una nueva campaña, un nuevo producto o nuevas actividades que nunca antes se habían abordado dentro de la compañía u organización, por lo que será necesario analizar los riesgos relacionados con el tratamiento de datos personales y establecer medidas para prevenir, mediante la realización previa a los tratamientos de una evaluación de riesgos y amenazas. En definitiva, establecer un “sistema de control de los riesgos” asociados al tratamiento de los datos personales que obliga considerar que, previamente al tratamiento, se deben aplicar medidas que permitan garantizar la adecuada protección de los datos a lo largo de todo el tratamiento (recogida, generación, almacenamiento, conservación, comunicación, cancelación y eliminación del dato).

Así, una de las principales conclusiones a las que llegamos en este estudio es la de considerar la necesidad de contar con un catálogo de riesgos y amenazas y unas medidas preventivas predeterminadas, de forma que este catálogo este adaptado a las actividades y estructura de la organización, y permita retroalimentarse de múltiples fuentes, ya sean internas, mediante la gestión de los incidentes, como externas, aprovechando los incidentes que han sufrido terceros o simplemente valorando como otras organizaciones evalúan y analizan sus amenazas.

En este trabajo se acompaña un catálogo de riesgos y amenazas (que no pretende ser completo ni absoluto), asociándolo a la fase dentro del ciclo de vida del dato, como si de una herramienta de autoayuda se tratara y tratando de definir una acción que permita mitigar dicho riesgo, debiendo tenerse en cuenta que ni las medidas son limitadas, ni es aplicable a todas las tipologías de organizaciones o procesos.

No obstante, las amenazas y riesgos cambian y no podemos conformarnos con garantizar que el impacto de un incidente o un evento no previsto no afectarán a nuestro nuevo proyecto o proceso.

Por último, la implementación de las medidas identificadas, así como las tareas relacionadas con la gestión de los datos y tratamiento en todo el ciclo de vida, exige la participación de las distintas áreas de la empresa implicadas, y no solo el área de Informática (TI) o Asesoría Jurídica, por lo que será necesaria su identificación y participación.

En definitiva, el legislador exige prevención y respeto y, además de articular medidas para garantizar los derechos de los ciudadanos, de los usuarios, en un entorno, en una sociedad cada vez más dependiente del uso de las tecnologías, obliga a las empresas a tomar medidas, a prevenir, a identificar riesgos, a planificar, a controlar, a documentar, a exigir responsabilidades y a garantizar el tratamiento de los datos personales desde el diseño de sus proceso de negocio y la implantación o diseño de tecnologías.

A través de este estudio, en el Grupo de Regulación de AUTELSI ha tratado de acercarse a este principio y elaborar recomendaciones para su implantación práctica.

Queremos manifestar nuestro agradecimiento a las empresas representadas en este Grupo de Trabajo de AUTELSI, y a sus vocales, que han contribuido activamente al desarrollo y resultado positivo de esta iniciativa.

También queremos agradecer a todas las personas que asistieron al desayuno, celebrado el 10 de diciembre de 2014, en el que se presentó este informe; así como a **Telefónica** por el patrocinio del evento y a la Entidad Pública **Red.es** por la cesión de sus intalaciones para la celebración del mismo.

RESUMEN EJECUTIVO ESTUDIO PRINCIPIO "PRIVACY BY DESIGN"

GRUPO DE REGULACIÓN DE AUTELSI
DICIEMBRE 2014