PRIVACIDAD EN EL DISEÑO

DE LA INTELIGENCIA

ARTIFICIAL

"PRIVACY BY DESIGN IN AI".

Eduardo Riestra Herrera.

RIESTRA ABOGADOS MARKETING LEGAL

Junio de 2017

1. INTRODUCCIÓN

El nuevo Reglamento (UE) 2016/679 ha incluido el concepto de *"privacidad en el diseño"*, lo que supone un paso importante en la consolidación de la protección de los datos personales en el derecho comunitario. El trabajo que ha continuación se presenta trata de analizar el encaje de la idea de *"privacidad en el diseño"* en la incipiente Inteligencia Artificial (IA).

Para ello es necesario conocer los principios básicos de nuestro modelo actual de protección de datos, así como la diferentes propuestas que tratan de encajar la privacidad en el mundo online. Sin embargo la idea de Big Data, como fuente de alimentación de la IA, desestabiliza las ideas preconcebidas, obligando a replantearse conceptos mismos como el de privacidad, si pretendemos preservarla en el futuro.

2. MARCO JURÍDICO

El trabajo se desarrolla principalmente teniendo como referencia el ámbito europeo y nuestra normativa nacional, la cual deberá adaptarse en las próximas fechas. Pero un tema tan apasionante, además de complejo, como la IA requiere conocer la opinión imprescindible de autores y autoridades estadounidenses, además de ciertas bases legales que tratan de dar sentido al hilo argumental del presente trabajo. Por ello las principales referencias legales tratadas son:

- ✓ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- ✓ Directiva 95/46 / CE y del artículo 4.1, b) y c), del Reglamento (CE) nº 45/2001
- ✓ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- ✓ Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- ✓ Fair Information Practice Principles (FIPPs). Federal Trade Commission.

**negritas, cursivas y subrayados son del autor.*

3. ANTECEDENTES: FAIR INFORMATION PRACTICES ("FIPS") y el REGLAMENTO (UE) 2016/679

El informe ***"Privacidad personal en una sociedad de la información",*** ("*Personal Privacy in an Information Society"), elaborado* en 1977 *por la comisión de privacidad del gobierno federal de los Estados Unidos,* establece y define los derechos de las personas respecto a sus datos personales y las obligaciones de los responsables de datos *("Controllers"),* siendo una referencia e inspiración para la mayor parte de los ordenamientos de privacidad de todo el mundo. La Comisión Federal de Comercio de EE.UU, más conocida como la *Federal Trade Commission ("FTC"),* (agencia estatal independiente de Estados Unidos, bajo responsabilidad directa del Congreso), sin olvidar su cometido principal en defensa de los consumidores, ha asumido los principios señalados en dicho informe, los cuales pueden resumirse en, **(i) aviso / conocimiento, (ii) elección / consentimiento, (iii) acceso / participación, y (iv) integridad / seguridad,** veamos:

1. Aviso / conocimiento:

Esta es la base de todos los principios de la privacidad. Se basa en que los consumidores deben ser notificados de las prácticas de una entidad antes de que se recoja cualquier información personal de los mismos.

Que nuestro actual Reglamento (UE) 2016/679 expone en el considerando (39):

> *(39) "(…) el principio de transparencia exige que* ***toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender****, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la* ***información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo*** *y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento (…)"*

Se incluye el elemento fundamental del principio de aviso / conocimiento que es la ***facilidad,*** tanto en el acceso a la información como en su comprensión, lo que origina, como veremos más adelante, la necesidad de adoptar, de cara al consumidor, la idea de *usabilidad* en el desarrollo de las aplicaciones informáticas. En el siguiente artículo del Reglamento (UE) 2016/679 ya se incluye el mínimo de información, que es obligatorio ofrecer cuando se captan datos personales:

Artículo 13: ***Información que debe ponerse a disposición del interesado o que se le debe proporcionar***

> *1.Los Estados miembros dispondrán que el responsable del tratamiento de los datos ponga a disposición del interesado al menos la siguiente información: a)* ***la identidad y los datos de contacto del responsable del tratamiento****; b) en su caso, los datos de contacto del delegado de protección de datos; c) los* ***fines del tratamiento*** *a que se destinen los datos personales; d) el* ***derecho a presentar una reclamación ante la autoridad de control*** *y los datos de contacto de la misma; e) la existencia del* ***derecho*** *a solicitar del responsable del tratamiento el* ***acceso*** *a los datos personales relativos al interesado, y su* ***rectificación*** *o su* ***supresión****, o la limitación de su tratamiento.*
>
> *2.Además de la información indicada en el apartado 1, los Estados miembros dispondrán por ley que* ***el responsable del tratamiento de los datos proporcione***

> ***al interesado**, en casos concretos, la siguiente información adicional, a fin de permitir el ejercicio de sus derechos: a) la **base jurídica del tratamiento**; b) el **plazo durante el cual se conservarán los datos personales** o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo;*
> *cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales; d**) cuando sea necesario, más información, en particular cuando los datos personales se hayan recogido sin conocimiento del interesado**.*

Incluyendo, además, una serie de limitaciones a tal derecho, llamando la atención la apelación previa del legislador a acotar tales limitaciones a aquellas medidas *"**necesarias y proporcionales en una sociedad democrática**"*:

> *3.Los Estados miembros podrán adoptar medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información en virtud del apartado 2 siempre y cuando dicha medida constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para: a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas.*

Este primer principio es el punto de partida de todo tratamiento de datos personales, también reconocido en el art.5 de nuestra Ley Orgánica de Protección de Datos 15/1999, bajo el epígrafe *"Derecho de información en la recogida de datos"*.

2. Elección / consentimiento:

La elección y el consentimiento cuando se captan datos personales online significa dar a los consumidores opciones para controlar el uso de los mismos.
En concreto, la elección se refiere a los usos secundarios de la información más allá de las necesidades inmediatas del recopilador de información. Los dos modelos típicos de elección son el *opt-in (consentimiento expreso)* o *opt-out (consentimiento tácito).*

El método de *"opt-in"* requiere que los consumidores otorguen un permiso afirmativo para que su información sea usada para otros propósitos frente al método de *"opt-out"* que requiere que los consumidores denieguen el permiso para otros usos, lo que se conoce también como un sistema de "exclusión voluntaria", pudiendo utilizarse los datos mientras el usuario no manifieste lo contrario.

Lógicamente cada uno de estos sistemas debe diseñarse para permitir que un usuario pueda determinar sus preferencias marcando casillas para otorgar permisos para finalidades específicas, en lugar de usar un método simple de *"todo o nada"*, como ya ha dejado patente el Reglamento (UE) 2016/679 en sus considerando (32), (42) y (43), así como en su artículo 7:

> *Considerando (32)*
>
> ***El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado*** *de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.* ***El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o***

> ***los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos**. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.*

Importante, tener presente la idea del consentimiento que se incluye a través del considerando 32, porque ya no sirven las casillas en internet marcadas por defecto del tipo *(x) quiero recibir información comercial*, sino que tiene que ser activamente el usuario quien la marque, añadiendo además que tal acción deberá ser ejecutada para cada una de las finalidades, por lo tanto habrá tantas casillas por marcar como finalidades distintas. Todo ello derivado de las características del consentimiento que deberá ser *"libre, específico, informado, e… inequívoco"* como así confirma el siguiente considerando:

> *(42)* ***Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento**. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace.*

Recordando que el consentimiento informado deber ser fácil, tanto en el acceso como en su comprensión.

> *De acuerdo con la Directiva 93/13/CEE del Consejo (1),* ***debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas**. Para que el **consentimiento sea informado**, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o*

libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

Y libre,… según el considerando

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. ***Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento****.*

Por ejemplo, el entorno laboral es muy proclive a prestar un consentimiento *no libre* para el tratamiento de los datos. Son los casos en los que a los empleados se les pide el consentimiento para otros fines distintos de los estrictamente necesarios para la relación laboral, y lógicamente el empleado lo presta pensando en posibles represalias por parte de la empresa si se negara.

En todo caso, ya en las definiciones del Reglamento queda clara la idea de consentimiento:

Artículo 4 ***Definiciones*** *A efectos del presente Reglamento se entenderá por:*

11) «consentimiento del interesado»: ***toda manifestación de voluntad libre, específica, informada e inequívoca*** *por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;*

Trasladando la carga de la prueba del consentimiento dado al responsable del tratamiento, lo que obliga a estos a conservar las pruebas o los soportes en los cuales se otorgó el consentimiento, como por ejemplo formularios, cupones, grabaciones, etc.

> *Artículo 7* ***Condiciones para el consentimiento***
>
> *1.Cuando el tratamiento se base en el consentimiento del interesado,* ***el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.***

Y por supuesto facilitando al afectado la retirada del consentimiento y en cualquier momento:

> *3.****El interesado tendrá derecho a retirar su consentimiento en cualquier momento****. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.*
>
> *4.****Al evaluar si el consentimiento se ha dado libremente****, **se tendrá en cuenta** en la mayor medida posible el hecho de si, entre otras cosas,* ***la ejecución de un contrato,*** *incluida la prestación de un servicio,* ***se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.***

El poder de otorgar un consentimiento efectivo se basa en el deber correcto de información por parte del responsable del tratamiento. En los últimos años, y fruto del trabajo de la Agencia Española de Protección de Datos, entre otras, ya sea a través de resoluciones o recomendaciones, el concepto de consentimiento como ***manifestación de voluntad libre, específica, informada, e inequívoca*** ha quedado claro sirviendo como base del modelo actual de la protección de datos personales.

3. Acceso / participación:

El deber de información y el consentimiento, se completan con el derecho de acceso por parte de los interesados. El derecho de acceso incluye no sólo la capacidad del usuario para ver los datos recopilados, sino también para verificar su exactitud. Este acceso debe ser accesible y oportuno.

En el Reglamento (UE) 2016/679 se regula en el *Artículo*

> *14* ***Derecho de acceso del interesado a los datos personales*** *Con sujeción a lo dispuesto en el artículo 15, los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, acceso a dichos datos personales y la siguiente información:* ***a) los fines y la base jurídica del tratamiento****;* ***b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales; d) cuando sea posible, el plazo contemplado durante el cual se conservarán los datos personales o, de no ser posible, los criterios utilizados para determinar dicho plazo; e) la existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado, o la limitación de su tratamiento; f) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma; g) la comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen****.*

El derecho de acceso lo entendemos como una forma de *control* que el interesado tiene sobre sus propios datos personales. Recordemos, por ejemplo el caso Schrems, que partió de un derecho de acceso a facebook por parte del irlandés, Maximillian Schrems, solicitando los datos que dicha compañía tenía de su persona, lo que provocó finalmente

la anulación de la decisión 2000/520 (Puerto Seguro) por parte del Tribunal de Justicia Europea, en su sentencia de 6 de octubre de 2015, que hasta entonces regulaba las transferencias internacionales de datos personales entre la EU y EE.UU.

En la Ley Orgánica de Protección de Datos 15/1999 el derecho de acceso, junto otros, como el derecho de rectificación, cancelación u oposición se regulan en el TÍTULO III bajo el epígrafe *"Derechos de las personas"*, constituyéndose como unos derechos que proporcionan eficacia a la protección de los datos personales.

4. Integridad / seguridad:

Los anteriores principios, deber de información, consentimiento, derecho de acceso, carecerían de sentido si no se puede garantizar la seguridad en la custodia de los mismos. Quien capta datos debe asegurarse de que los datos que recoge son exactos y seguros, además debe mantenerlos protegidos frente a amenazas internas y externas de seguridad. Se puede limitar el acceso dentro de la empresa a los empleados estrictamente necesarios para protegerlos contra las amenazas internas, y pueden utilizar el cifrado y otros sistemas de seguridad para detener las amenazas externas.

En el Reglamento (UE) 2016/679 se regula en el *Artículo 29* ***Seguridad del tratamiento*** *1.Los Estados miembros dispondrán que* ***el responsable y el encargado del tratamiento,*** *teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas****, apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10.***

Los Fair Information Practices ("FIPS") como base del sistema actual de privacidad encuentra en el nuevo Reglamento Europeo un destacado desarrollo que sin duda otorga a nuestro sistema europeo el honor de ser el más garantista del mundo en la protección de los datos personales. ***Información, consentimiento, acceso, integridad y seguridad***

son principios básicos de nuestra regulación, pero ¿servirán como modelo para el futuro que actualmente se está construyendo?

4. LOS PRINCIPIOS DE PRIVACIDAD EN EL DISEÑO, SECURITY BY DESIGN, Y TECNOLOGÍAS QUE MEJORAN LA PRIVACIDAD EN LA AGENDA EUROPEA 2020:

La Comisión Europea hace una llamada para promover la *"privacidad en el diseño"*, la *"seguridad en el diseño"*, y *"las tecnologías que mejoran la privacidad"*, como una forma de abordar los cambios tecnológicos en la protección de los datos personales.

En la comunicación de la Comisión COM(2010) 245, titulada ***"Una Agenda Digital para Europa"*** la cual se define en su introducción como

> *"una de las siete iniciativas emblemáticas de la estrategia Europa 2020, y su propósito es definir la función capacitadora esencial que deberá desempeñar el uso de las tecnologías de la información y la comunicación (TIC) si Europa quiere hacer realidad sus ambiciones para 2020"*.

aborda en la *pag19* de dicho informe la idea de la privacidad en el diseño:

> *"**El derecho a la intimidad y a la protección de los datos personales constituye un derecho fundamental en la UE que es preciso hacer aplicar –también en línea– eficazmente utilizando un amplio abanico de métodos: desde la aplicación generalizada del principio de «privacidad a través del diseño»** en las tecnologías de TIC pertinentes, hasta las sanciones disuasorias cuando resulte necesario"*

Explicando que el principio de privacidad en el diseño:

> *"significa que la protección de los datos y de la intimidad está imbricada en* ***todo el ciclo de vida de las tecnologías****, desde la primera fase de diseño a su despliegue, utilización y eliminación definitiva".*

Lo mismo que en la comunicación de la Comisión COM/2010 titulada *"**Un enfoque global de la protección de los datos personales en la Unión Europea"*** donde se valora el impacto de las nuevas tecnologías en la protección de datos personales, donde incluye la idea en su epígrafe 2.2.4, que para reforzar la responsabilidad de los responsables del tratamiento

> *"la Comisión* ***proseguirá la promoción de la utilización de las PET (Privacy Enhancing Technologies) y de las posibilidades de aplicación concreta del concepto de "privacidad desde el diseño"****… incluso para garantizar la seguridad de los datos"*

Vemos que la privacidad en el diseño cobra especial relevancia en un entorno con innumerables fallos de seguridad, ya sea corporativo, institucional o doméstico.

Recordemos el considerando 88 del Reglamento (UE) 2016/679:

> *"Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive* ***si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas****, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido".*

Por todo ello haremos una introducción por cada uno de estos tres conceptos, *"privacidad en el diseño",* la *"seguridad en el diseño",* y *"las tecnologías que mejoran la privacidad"*, para tratar de entender su encaje en la Inteligencia Artificial.

4.1 PRIVACIDAD EN EL DISEÑO.

4.1.1 El diseño de un producto.

El proceso del diseño de un software comienza con una idea, que bien puede ser fruto de una tormenta de ideas ("*brainstorming*") en el seno de una compañía, comenzando la *fase conceptual*, donde se pueden plantear los siguientes interrogantes:

- *¿Existe una necesidad?*
- *¿Qué piensan los clientes?*
- *¿Cómo está el mercado?*
- *¿Disponemos de recursos?*

Según el diccionario de Cambridge[2] diseño de producto lo define como:

> *"El proceso de crear o mejorar un producto aprendiendo lo que desean los consumidores y examinando productos similares que ya están disponibles".*

Diseño *front-end* versus *back-end*:

En diseño de software el *front-end* [3] es la parte del software que ven los usuarios, es decir donde se interactúa, frente *al back-end* que es la parte del programa que el usuario no ve. Estos dos conceptos son muy utilizados en la práctica del diseño de software.
Por lo general, y en teoría, el *front end* es la parte donde se recolectan los datos de entrada del usuario, y el *back end* es donde los procesa para devolver una respuesta inteligible al usuario a través de lo que se conoce como interfaz [4], es decir el medio a través del cual un usuario se comunica con la máquina.

Por lo general los diseños de privacidad que siguen los principios de los *Fair Information Practices ("FIPs")*, se han basado en un diseño de *back-end*, llegando a considerar al diseño de la privacidad en un complemento de la ingeniería de seguridad ("*Security by design*") opción que rechaza Ira S. Rubinstein and Nathaniel Good [5] por dos razones:

> *"Primera: la ingeniería de la privacidad es una disciplina emergente con su propia estructura y no es reducible a la ingeniería de seguridad.*

Segunda, no todos los problemas de privacidad son resueltos por referencia a los FIPs o el uso de Controles basados en la seguridad".

Es interesante anotar que los autores hacen referencia a la ingeniería de la privacidad ("*privacy engineering*"), frente a la ingeniería de la seguridad ("*security engineering*"), añadiendo que la usabilidad de las herramientas ("*UX Usability Experience*"), es decir la facilidad de uso de las mismas junto con el diseño que hace fácil y sencillo su manejo, deben tener un rol importante en el diseño de la privacidad. Ingenieros y juristas trabajando conjuntamente sobre la experiencia y modo de uso de las herramientas por parte de los usuarios finales.

Un ejemplo de cómo incorporar la privacidad en el diseño en la propia fase incipiente de desarrollo de un software sería definiendo en el mismo software el tiempo que los datos deben mantenerse según la norma legal aplicable, estableciéndose el procedimiento de borrado de forma automática cuando proceda.

En cualquier diseño de un producto el elemento de la privacidad debe tenerse en cuenta tanto en la fase de *back end*, incluyendo la seguridad, como en la fase de *front end*, es decir creando mecanismos "amigables", sencillos y prácticos para que sea el usuario quien controle sus datos y preferencias, de ahí que la usabilidad de las aplicaciones sea fundamental. Recordemos el Considerando (39) del Reglamento (UE) 2016/679, que establecía que "***toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender".*** De todo ello se aprecia por lo tanto la necesidad de desarrollar la privacidad en el diseño desde una perspectiva interdisciplinar, aglutinando a la ingeniería de privacidad, con ingeniería de seguridad y los expertos en usabilidad, si queremos conseguir una privacidad en el diseño efectiva.

4.1.2 Los 7 principios fundamentales (y crítica).

Privacy by design *(PbD)* es un concepto desarrollado en los años 90 por la Dr. Ann Cavoukian, directora ejecutiva del *Privacy and Big Data Institute*, ***que se fundamenta***

en alcanzar el CONTROL sobre la información personal. Para obtener tal propósito la autora propone que tal control debe desarrollarse en los siguientes ámbitos, o como ella lo denomina, *"la trilogía":*

1) En los sistemas IT.
2) En los sistemas de responsabilidad social, o *corporate accountability*.
3) En el diseño físico de la infraestructura de redes.

Lo que le lleva a plantear un modelo basado en lo que denomina los *7 Principios Fundamentales.* [6]

Y que básicamente son:

1- ***Proactivo, no reactivo. Preventivo, no remediador.***
Su principal característica es la anticipación al daño frente a la improvisación del remedio, en definitiva prevenir antes de que ocurra la infracción en la privacidad.

2- ***Privacidad por defecto.***
La privacidad se mantiene salvaguardada sin necesidad de que las personas realicen ninguna acción para protegerla, por lo que los datos personales estarán por defecto y automáticamente protegidos en los sistemas IT o en las prácticas corporativas.

3- ***Privacidad integrada en el diseño.***
La privacidad formará parte de la arquitectura IT o de las prácticas corporativas, no siendo un componente añadido a posteriori, sino que formará parte del desarrollo técnico y funcional de los propios sistemas.

4- ***Funcionalidad total. Suma positiva, no suma cero.***
Frente a falsas dicotomías donde el diseño de la privacidad perjudica otros intereses como por ejemplo la seguridad.

5- ***Seguridad de principio a fin. Protección total durante todo el ciclo.***

Seguridad ya desde antes de la recolección de la información personal, así como durante todo el proceso con medidas de seguridad garantistas hasta la destrucción de la información, bien sea al finalizar el ciclo o periodo vital de la información captada.

6- ***Visibilidad y transparencia.***

Independientemente del sector comercial o del tipo de tecnología aplicada, la privacidad en el diseño debe permitir que un tercero pueda verificar, que efectivamente, las políticas de privacidad y sus medidas de seguridad son ciertas y se cumplen, lo que se conoce también como "c*onfía pero verifica"(trust but verify),* utilizado por el presidente Ronald Reagan en sus relaciones con la Unión Soviética citando el proverbio ruso "*doveryai, no proveryai"*.

7- ***El usuario en el epicentro de su privacidad.***

Basado en sistemas sencillos para el usuario donde primen sus preferencias pudiendo controlar y tener opciones más altas de seguridad.

Crítica a los 7 principios fundamentales:

Como idea, es interesante, porque traslada la privacidad a todos los niveles, tanto de creación como de gestión corporativa, asumiendo que todos sus responsables conocen y son sensibles a las cuestiones de privacidad, sin embargo hoy en día no podemos estar más lejos de la realidad, porque las grandes tecnológicas han demostrado que prácticamente en casi todos los grandes productos que han lanzado no han tenido en cuenta la privacidad en el diseño.

Como por ejemplo:

GOOGLE

Gmail y el buscador:

En 2004 se lanzó el servicio de Gmail en el que se ofrecía un alto almacenamiento de datos a cambio de recibir publicidad personalizada según el contenido de sus correos

electrónicos, por lo que era necesario que el buscador escaneara previamente el contenidos de tales correos electrónicos para que, a través de algoritmos, identificaran y asociaran por ejemplo palabras clave, tomando también en cuenta para ello sus hábitos de navegación en el buscador. A Google se le criticó en este caso la falta de transparencia e información,

Es en este caso cuando saltan las alarmas acerca de la trazabilidad e interconexión de todas las herramientas de Google, es decir el usuario utiliza el buscador de Google, utiliza su correo electrónico Gmail, almacena sus datos en Google Drive, y así con más productos de Google, por lo que Google al aglutinar todos los servicios en su compañía tiene la capacidad de conocer mejor que nadie a sus propios usuarios creando perfiles con total fiabilidad, y para cerrar el círculo, Google compró en 2007 la mayor red de publicidad online en el mundo, DoubleClick[7]. No hay duda que la idea es controlar todo el sistema de publicidad, y éste se nutre… de los datos de los usuarios. Cuanto mejor conozca al usuario *más y mejor* publicidad venderá.

Google Street View:

En 2010 se hace público que cuando el coche de Google recorría las calles de las ciudades para crear los callejeros, no sólo se estaban grabando las imágenes de tales calles sino que se captaban los datos de todas las redes wifi que no estaban correctamente protegidas durante su recorrido, incluyendo passwords, direcciones de correo electrónico, etc. La propia Federal Communications Commission ("FCC") reconoció que no se trató de un fallo o error de diseño, por lo que podemos entenderlo como un acto deliberado y consciente. Es importante esta apreciación de la "FFC" porque se demuestra la falta de sensibilidad de Google por la privacidad en el diseño.

Si bien es cierto que fue un acierto el sistema de pixelación de las personas o matrículas de vehículos, así como la introducción de un sistema de opt-out, también es verdad que hubo una manifiesta infracción al captar *deliberadamente* datos personales de las redes wifi.

Buzz and Google+:

En Febrero de 2010, Google lanzó Buzz, para competir con Facebook, teniendo la característica de que a todos sus usuarios de Gmail, sin previo consentimiento, les creaba automáticamente una lista de seguidores según la lista de contactos de cada usuario, por lo que en muchos casos podrían ser accesibles los contactos de un usuario.

Sin embargo, y tratando de paliar el fiasco de Buzz, se lanzó Google+ siendo la primera red social pensada para que los usuarios pudieran crear "círculos" (p.e., familia, amigos, colegas de trabajo).

FACEBOOK.

News Feed:

Fue el primer gran incidente de Facebook en 2006, ya que este servicio permitía a los usuarios recibir diariamente un informe de la actividad de sus amigos, como cambios en sus amistades, etc. Esto supone una infracción de los derechos de privacidad de los usuarios porque se basa en un sistema de seguimiento permanente de la actividad de una persona por toda su comunidad.

Beacon:

Un año después se lanzó Beacon, un producto de su red publicitaria que ofrecía publicidad personalizada en función de las compras que el usuario realizaba en web sites asociados con Facebook, y que además esa información se compartía con sus amistades a través de News Feed, lo que le supuso una reclamación por 9,5 millones de dólares. En este caso se ceden datos sin consentimiento de los usuarios.

Facebook Apps:

Otro incidente en la privacidad fue cuando Facebook permitía que los proveedores de las aplicaciones accedieran a la información de aquellos usuarios que se las instalaban. Esto provocó que la entidad de control de protección de datos canadiense exigiese a

Facebook medidas para evitar tales accesos, y por ello Facebook incorporó la exigencia del consentimiento expreso del usuario para dar acceso a su información por el proveedor de aplicaciones, pero la controversia continuó al conocerse por el Wall Street Journal[8] que incluso otorgando ese consentimiento expreso la información de contactos del usuario también era accesible por parte del proveedor.

Lo mismo que en el caso anterior, se están cediendo datos a terceros sin consentimiento de los usuarios, práctica muy habitual al descargarse aplicaciones, sobre todo las gratuitas, que como nos recuerda la industria, *"el producto es el consumidor"*.

Photo Sharing:

Controvertido igualmente en sus comienzos, la acción de etiquetar *("taggin")* las fotografías con el nombre de las personas que aparecen en las imágenes suscitó incomodidad en distintas entidades de control de protección de datos por todo el mundo, lo que impulsó a Facebook crear una opción donde la persona que era etiquetada podría, antes de su publicación, oponerse a que dicha fotografía estuviera etiquetada con su nombre.

Sin embargo el problema de fondo es mucho más complejo, ya que en una fotografía, a modo de resumen, hay tres partes, una el autor de la fotografía, otra quien la publica en Facebook que puede ser distinto, y una tercera el retratado. No sólo hay una implicación en protección de datos personales, porque la imagen se considera como tal,

sino que se pueden ver afectados otros derechos, como los de propiedad intelectual o derechos de imagen.

Conclusión:

Los casos anteriormente expuestos podrían haberse evitado si se hubiera aplicado un modelo práctico de *Privacy by design*, pero es evidente que tanto Google como Facebook, ponderan los riesgos de privacidad con su *core business*, que es la venta de publicidad, y prevalece ésta última porque la privacidad o lo que es lo mismo, *el dato*, es su materia prima. Por ello las soluciones que plantean tanto Google como Facebook son por lo general a posteriori del hecho consumado, y como reacción de las quejas de

las entidades de control de protección de datos, de Ongs de defensa de los derechos de privacidad, de periodistas o de usuarios.

Y es evidente que Google y Facebook han actuado de forma contraria a los 7 principios fundamentales:

1- *Principio* ***proactivo No reactivo. Preventivo No remediador.***

   Siempre han actuado a posteriori. Cuando la opinión pública o una entidad de control denuncia.

2- *Principio de* ***privacidad por defecto.***
   Este principio se impone cuando las tecnológicas se han visto obligadas.

3- *Principio de* ***privacidad integrada en el diseño.***
   La privacidad no es una prioridad.

4- *Principio de* ***funcionalidad total. Suma positiva No suma cero.***
   Siempre y cuando no afecte al negocio, de lo contrario no se aplica.

5- *Principio de* ***seguridad de principio a fin. Protección total durante todo el ciclo.***
   No hay durante el proceso medidas de seguridad garantistas, porque además no se prevé la destrucción de la información al finalizar el ciclo o periodo vital de la información captada.

6- *Principio de* ***visibilidad y transparencia.***
   Los sistemas de las tecnológicas son poco transparentes basándose en el secretismo.

7- ***El usuario en el epicentro de su privacidad.***
   Actualmente esta afirmación es incompatible con su modelo actual de negocio.

Como vemos, la idea de los 7 principios fundamentales, no carente de buenas intenciones, es ignorada por las grandes tecnológicas, que de paso son la referencia del grueso de resto de empresas del mundo digital, por lo que partimos de un mal inicio.

Además, la privacidad en el diseño no es reconocida en el mundo de la innovación tecnológica y empresarial, como podemos apreciar en cualquier foro o conferencia pública, como por ejemplo en España, donde salvo los juristas de privacidad "y allegados" (Ongs, fundaciones…), todo el ámbito empresarial, de marketing y publicidad, manifiestan que la excesiva privacidad es un límite para *el negocio* y supone una pérdida en la innovación.

Recordemos que en el año 2016 solamente cuatro compañías estadounidenses, Google, Amazon, Facebook y Apple, han tenido una capitalización bursátil de casi **¡2 billones de dólares!** [9], prácticamente el doble del PIB en España.

La exposición de estos casos se han basado en el artículo de Rubinstein Ira y Good Nathaniel. "***Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents"*** [10]**.**

Para Ira Rubinstein[11], miembro del Instituto de Derecho de la Información de la Universidad de Nueva York, no está del todo claro que los *7 principios*, de la Dr. Ann Cavoukian, sean de mayor ayuda que los *Fair Information Practices ("FIPS")*, apreciando que los 7 principios son más ambiciosos que prácticos u operativos, por eso realiza el siguiente análisis de los mismos:

> Principios (1) a (3): critica que*" no ofrezcan cualquier orientación de diseño"*; y con toda razón, porque se necesita un modelo o referencia práctica como si se hace, por ejemplo, en la seguridad en el diseño que trataremos a continuación.
>
> Principio (4): le parece poco realista *"en una época en que los datos son el nuevo maná de Internet y los controles de privacidad sólo tienden a limitar la explotación de este valioso producto"*,
>
> Principio (5): y siempre según el autor, *"enfatiza la gestión del ciclo de vida, que es un aspecto clave de la ingeniería de la privacidad" ("Privacy Engineering")*;

Principio (6): se asemejaría al principio familiar de transparencia que se encuentra en todas las versiones de los *Fair Information Practices*;

Principio (7) funcionaría principalmente como un resumen de los otros principios.

En definitiva se critica que no se especifica qué es la privacidad en el diseño, *¿una rama de la mejora de la privacidad?, ¿un enfoque del ciclo de vida del software?, ¿etapas de diseño y desarrollo del producto? o ¿mecanismos basados en la rendición de cuentas?* y sobre todo concluye el autor que en los 7 principios, **no indica cómo debe traducirse la privacidad en el diseño en la práctica de la ingeniería,** cuestión que creo es crucial en el estudio de la privacidad en el diseño, en definitiva una buena declaración de buenas intenciones sin efectos prácticos.

4.2 SEGURIDAD EN EL DISEÑO: *SECURITY BY DESIGN.*

En la ingeniería de seguridad, "*Security Engineering*", hay un estudio más profundo que en la privacidad en el diseño, con una serie de normas internacionales comúnmente aceptadas con una serie de principios que regulan y dan sentido a tal concepto, todo lo contrario que con el concepto de *Privacy by design.*

La seguridad de la información se ha basado en los siguientes pilares:

i. ***Confidencialidad:*** sólo permite el acceso (a los datos) a los usuarios autorizados.

ii. ***Integridad:*** asegúrese de que los datos no sean manipulados por usuarios no autorizados.

iii. ***Disponibilidad:*** garantizar que los sistemas y datos estén disponibles para los usuarios autorizados cuando así lo necesiten.

Principios:

Por ejemplo, la Fundación OWASP[12] (“***Open Web Application Security Project”***), fundada en el 2001en EEUU, es una organización sin ánimo de lucro de código abierto y multidisciplinar cuyo objetivo es incrementar la seguridad del software, que establece los siguientes principios en el *Security by Design,* cuestión que considero de interés para clarificar la privacidad en el diseño*:*

1- ***Minimizar la superficie de ataque.*** *Minimize attack surface area.*

“Cada característica que se añade a una aplicación agrega cierta cantidad de riesgo a la aplicación general. El objetivo de un desarrollo seguro es reducir el riesgo global reduciendo la superficie de ataque”.

2- ***Establecer valores predeterminados seguros.*** *Establish secure defaults.*

“(…) por defecto, la experiencia debe ser segura, y debe ser, si se le permite, hasta que el propio usuario reduzca su seguridad…y aumente su riesgo”.

3- ***Principio de privilegios mínimos.*** *Principle of Least privilege.*

El principio de privilegios mínimos recomienda que las cuentas tengan la menor cantidad de privilegios requeridos para realizar sus procesos de negocio. Esto abarca derechos de usuario, permisos de recursos como límites de CPU, memoria, red y permisos de sistema de archivos.

4- **Principio de Defensa en profundidad.** *Principle of Defense in depth.*

El principio de la defensa en profundidad sugiere que cuando un control sea necesario, más controles que abordan riesgos en diferentes escenarios son mejores. Por ejemplo, es poco probable que una interfaz administrativa defectuosa sea vulnerable al ataque anónimo si se protege correctamente el acceso a las redes de gestión de producción, se compruebe la autorización administrativa del usuario y se registren todos los accesos.

5- **Fallo en la seguridad.** *Fail securely.*

Las aplicaciones fallan regularmente y por muchas razones al procesar transacciones. El código puede generar errores que por ejemplo establezcan administradores por error. Muchas organizaciones utilizan las capacidades de procesamiento de socios externos y estos pueden contener vulnerabilidades.
Todos los sistemas externos deben ser tratados de manera similar a los internos.

6- **Evite la seguridad por oscuridad.** *Avoid security by obscurity.*

La seguridad a través de la ocultación es un control de seguridad débil, y casi siempre falla cuando es el único control. Esto no quiere decir que guardar secretos es una mala idea, simplemente significa que la seguridad de los sistemas clave no debe depender de mantener los detalles ocultos.

Por ejemplo, la seguridad de una aplicación no debe basarse en el conocimiento del código fuente que se mantiene en secreto. La seguridad debe basarse en muchos otros factores, como las políticas de contraseñas razonables, la defensa en profundidad, los límites de las transacciones comerciales, la sólida arquitectura de red y los controles de fraude y auditoría.

Un ejemplo práctico es Linux. El código fuente de Linux está ampliamente disponible y, sin embargo, cuando está correctamente protegido, Linux es un sistema operativo seguro y robusto.

7- **Mantenga una seguridad sencilla.** *Keep security simple.*

La superficie de ataque y la simplicidad van de la mano. Ciertas modas de ingeniería de software prefieren enfoques excesivamente complejos a lo que de otro modo sería un código relativamente simple y sencillo.

Los desarrolladores deben evitar complejas arquitecturas cuando un enfoque más simple sería más rápido y mejor.

8- **Solucionar problemas de seguridad correctamente.** *Fix security issues correctly*

Una vez que se ha identificado un problema de seguridad es importante desarrollar una prueba y comprender la causa raíz del problema. Cuando se utilizan patrones de diseño, es probable que la cuestión de seguridad esté muy extendida entre todas las bases de código, por lo que es esencial desarrollar la corrección sin introducir regresiones. Por ejemplo, un usuario ha encontrado que pueden ver el equilibrio de otro usuario ajustando su cookie. La corrección parece ser relativamente sencilla, pero como el código de manejo de cookies se comparte entre todas las aplicaciones, el cambio a una sola aplicación llegará a todas las demás aplicaciones.
Por lo tanto, la revisión debe probarse en todas las aplicaciones afectadas.

El listado anterior de principios nos sirve como referencia para proponer un modelo de principios de privacidad en el diseño, que es fundamental para dotar de sentido a tal figura, y no se quede en una mera propuesta teórica.

4.3 TECNOLOGÍAS QUE MEJORAN LA PRIVACIDAD. Privacy Enhancing Technologies (PET).

Hemos realizado una introducción al concepto de privacidad en el diseño, y visto un ejemplo de modelo básico en la seguridad en el diseño, con la idea de pasar a analizar la idea que subyace en "*las tecnologías que mejoran la privacidad*". Tecnologías como son por ejemplo, los sistemas de autenticación, encriptación o anonimización.

El concepto de *Privacy by design* está relacionado con el de "***Privacy Enhancing Technologies (PET)"***, *("las tecnologías que mejoran la privacidad")*, siendo utilizado en 1995 por primera vez en el informe ***"Privacy-enhancing technologies: the path to anonymity*** [13]".

Dicho informe fue fruto de un proyecto conjunto entre la autoridad de protección de datos holandesa (John Borking) y el comisionado de información de Ontario (Ann Cavoukian), afirmando que el concepto de "***Privacy Enhancing Technologies (PET)"*** está directamente relacionado con el principio de **minimización de datos (**"*data minimization"*).

¿Qué es el principio de minimización de datos?

Recordemos que el principio de minimización de datos proviene del artículo 6.1, b) y c), de la Directiva 95/46 / CE y del artículo 4.1, b) y c), del Reglamento (CE) nº 45/2001, y significa que **un responsable del tratamiento debe limitar la recopilación de información personal a lo que es directamente relevante y necesario para lograr un propósito específico, conservando los datos sólo durante el tiempo que sea necesario para cumplir con dicho propósito**.

Actualmente el Reglamento (UE) 2016/679 recoge la minimización de datos en el **Artículo 5. Principios relativos al tratamiento:**

> *1.Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c)* ***adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*** *(«****minimización de datos****»);*

En definitiva, los datos serán tratados de manera:

- ✓ **Lícita, leal y transparente.**
- ✓ **Para fines específicos, explícitos y legítimos.**

- ✓ **Adecuados, pertinentes y no excesivos en relación con los fines para los que se recogen.**

Por lo tanto el principio de minimización de datos queda totalmente acotado, y sin dejar lugar a dudas sobre su alcance. Esta cuestión la abordaremos de nuevo al tratar el encaje de este principio en la idea de Big Data.

La idea de minimización de datos se recoge en el mismo artículo del Reglamento que aborda la privacidad en el diseño:

Artículo 25 Protección de datos desde el diseño y por defecto:

> *1.Los Estados miembros dispondrán que el responsable del tratamiento, teniendo en cuenta el estado de la técnica y 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 para los derechos y libertades de las personas físicas planteados por el tratamiento,* ***aplique, tanto en el momento de determinar los medios para el tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas****, como por ejemplo la* ***seudonimización****, concebidas para aplicar los principios de protección de datos, como por ejemplo la* ***minimización de datos****, de forma efectiva y para integrar las garantías necesarias en el tratamiento (…).*

Protección de datos que se debe realizar desde el momento en el que se determinan los medios para el tratamiento, es decir, cuando se están concibiendo tales medios, así como en el mismo momento del tratamiento, que era básicamente como se estaba realizando hasta la fecha. Pero además, se proponen ejemplos como la seudonimización, eficacia que valoraremos en páginas posteriores. En cuanto a la protección de datos en el diseño por defecto, recogido en el apartado 2, importante destacar que sólo se tratarán los datos para los fines específicos propios de su captación. Es decir no se podrán tratar más datos que los necesarios para la finalidad consentida por el interesado.

> *2. Los Estados miembros dispondrán que el responsable del tratamiento aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad.* ***En concreto, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin intervención de la persona, a un número indeterminado de personas físicas.***

También se recoge el principio de minimización en el ***Artículo 89 (1). Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos:***

> *1.El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del* ***principio de minimización*** *de los datos personales. Tales medidas podrán incluir la* ***seudonimización****, siempre que de esa forma puedan alcanzarse dichos fines.*

Donde se incluyen unas excepciones en el tratamiento de datos, que deben someterse a una serie de garantías y que respeten el principio de minimización, y si es posible utilizando la seudonimización, pero advirtiendo

> *Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.*

Cuestión que como demostraremos más adelante no está ni mucho menos garantizada en los sistemas de seudonimización.

Ya la directiva 45/96 en su Artículo 17, incluía la obligatoriedad de ***implementar "Privacy Enhancing Technologies (PET)"*** *como así se preveía respecto a la seguridad del tratamiento,*

> *1. Los Estados miembros* ***establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados,*** *en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.*
>
> ***Dichas medidas deberán garantizar****, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación,* ***un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.***
>
> *2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.*

Cuestiones que fueron ampliamente desarrollas por nuestra **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona en el artículo 6 bajo el epígrafe *"seguridad de los datos"*, y en el capítulo III** del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el **Reglamento de desarrollo de la LOPD.**
Pero es que además, el Reglamento (UE) 2016/679, prevé en el artículo 27, que cuando un tipo de tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas habrá de realizarse una evaluación de impacto relativa a la protección de datos. Esto es importante, porque habrá que detallar en la evaluación de impacto, las medidas y *mecanismos destinados a garantizar la protección de los datos personales,* lo

que implica el desarrollo de *tecnologías que mejoren la privacidad,* dentro del contexto de la minimización de datos.

> ***Artículo 27 Evaluación de impacto relativa a la protección de datos***
>
> *1.**Cuando sea probable que un tipo de tratamiento**, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, **suponga un alto riesgo para los derechos y libertades de las personas físicas,** los Estados miembros dispondrán que **el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.** 2.La evaluación mencionada en el apartado 1 incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas.*

Adelantándonos el considerando 75 el siguiente listado de riesgos para los derechos y libertades de los interesados en el tratamiento de sus datos personales;

> *- Tratamiento de datos capaz de **provocar daños físicos, materiales o inmateriales;***
> *- Cuando el tratamiento pueda dar lugar a problemas de **discriminación**, **usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, inversión no autorizada de la seudonimización, o cualquier otro perjuicio económico o social significativo**;*
> *- Cuando los interesados se vean **privados de** sus derechos y libertades o de la posibilidad de **ejercer el control** sobre sus datos personales;*

*- Cuando los datos personales tratados pongan de manifiesto el **origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical**,*

*- Cuando se traten **datos genéticos o datos biométricos** que permiten la identificación unívoca de una persona*

*- Cuando se traten datos relativos a la **salud o a la vida y orientación sexuales o a los antecedentes e infracciones penales u otras medidas de seguridad relacionadas**;*

*- **Cuando se evalúen aspectos personales**, en particular en el marco del análisis y la predicción de aspectos referidos al rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la ubicación o los movimientos, con el fin de crear o utilizar perfiles personales;*

*- Cuando se traten datos **personales de personas físicas vulnerables**, en particular los **niños**; o cuando el **tratamiento se refiera a una gran cantidad de datos personales y afecte a un elevado número de interesados**.*

Y todo ello reforzado por el Artículo 24 del Reglamento, ***Responsabilidad del responsable del tratamiento:***

1. *Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, **el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento**. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

La evaluación de impacto la podemos contemplar como una parte de la privacidad en el diseño porque anticipa al momento previo del tratamiento la previsión de las consecuencias de dicho tratamiento. Es positiva la inclusión de esta obligación como refuerzo de la privacidad en el diseño que deberá adoptarse cuando "***suponga un alto riesgo para los derechos y libertades de las personas físicas",*** y que para nuestro

estudio sobre Inteligencia Artificial, significa que habrá de adoptarse siempre, porque incluye cualquiera de los elementos de la lista anterior del considerando 75.

¿Cómo se integra la minimización de datos en un sistema de información?

En el informe elaborado por el Comisionado de Privacidad e Información de Ontario del año 2000, ***"Privacy-enhancing technologies: the path to anonymity"*** identificaba tres tipos de sistemas de información:

1- Sistemas de procesamiento.
2- Sistemas de toma de decisiones programados.
3- Sistemas de apoyo a la toma de decisiones.

Recordemos antes la definición de Sistemas de información que ofrece la Enciclopedia Britannica[14]:

> *"Sistemas de información es aquel* ***sistema integrado de componentes para recopilar, almacenar y procesar datos y para proporcionar información, conocimiento y productos digitales.*** *Las empresas y otras organizaciones confían en sistemas de información para llevar a cabo y gestionar sus operaciones, interactuar con sus clientes, proveedores y competir así en el mercado. Los sistemas de información se utilizan para ejecutar cadenas de suministro entre organizaciones y mercados electrónicos. Por ejemplo, las corporaciones utilizan sistemas de información para procesar cuentas financieras, administrar sus recursos humanos y alcanzar a sus clientes potenciales con promociones en línea. Muchas empresas importantes se construyen enteramente en torno a los sistemas de información".*

Veamos como desgrana el informe ***"Privacy-enhancing technologies: the path to anonymity"*** los sistemas de información:

1- Sistemas de procesamiento. *Processing systems.*

Los sistemas de procesamiento de transacciones recogen y llevan un registro de la información relacionada con una transacción. Los ejemplos abarcan desde sistemas de marketing directo hasta compras de bases de datos.

2- Sistemas de toma de decisiones programados. *Programmed decision-making systems.*

Los sistemas de toma de decisiones programados procesan los datos de acuerdo con procedimientos formales y estructurados. El sistema está programado, por sí solo, para ejecutar todo el proceso de pedido desde el momento en que se recibe. Por ejemplo los sistemas de reserva de hoteles o aviones, sistemas de contabilidad de nómina, sistemas de transacciones monetarias para cajeros automáticos, etc

3- Sistemas de apoyo a la toma de decisiones. *Decision-support systems.*

Los sistemas de apoyo a las decisiones ayudan en el proceso de toma de decisiones mediante el uso de la información recopilada para generar soluciones o información adicional que ayude en la toma de esas decisiones. Por ejemplo, sistemas para calcular hipotecas, sistemas de información de gestión, sistemas de itinerario recomendados, etc.

La característica común de todos estos sistemas es que su uso implica la recogida y procesamiento de información personal siempre que un individuo (el usuario) entra en contacto con un sistema, y para ello actualmente, no hace falta ni que el usuario se identifique porque para eso están los sistemas de trazabilidad o seguimiento.

Del informe ***"Privacy-enhancing technologies: the path to anonymity"*** cabe también destacar dos cuestiones que deben abordarse:

i- ***¿Qué condiciones deben tenerse en cuenta al diseñar un sistema de información para garantizar que el sistema se utilice de manera eficaz y eficiente sin revelar la identidad del usuario?***

Y nos planteamos, ¿realmente los nuevos sistemas de información se diseñan sobre la base de la información anónima? Recordemos que el negocio actual de las grandes tecnológicas es la publicidad personalizada.

ii- ¿Qué tipos de tecnologías de la información y la comunicación pueden contribuir a lograr este objetivo?

¿Podrá ser la Inteligencia Artificial un aliado para proteger la privacidad?, o ¿será el principio del fin de la misma?. Esta cuestión la abordaremos más adelante.

El informe del Comisionado de Privacidad e Información de Ontario esbozó algunos modelos para preservar la privacidad, y a modo de ejemplo, al configurar los sistemas de información para diseñadores, desarrolladores y comercializadores, sin embargo, hoy día tales buenas intenciones confrontan con la intención de los actuales sistemas de información desarrollados por las empresas tecnológicas que tratan de captar la máxima información posible para nutrir sus estrategias de Big Data, como ya adelantaron Julia Angwin and Jeremy Singer-Vine en el Wall Street Journal en 2012[15]:

> *"Este apetito por los datos personales refleja una verdad fundamental de Facebook y, por extensión, la economía de Internet en su conjunto. Facebook proporciona un servicio gratuito que los usuarios pagan, en efecto, proporcionando detalles sobre sus vidas, amistades, intereses y actividades. Facebook, a su vez, utiliza esa información para atraer a anunciantes, fabricantes de aplicaciones y otras oportunidades de negocio".*

A pesar de todo, el recién aprobado Reglamento Europeo 2016/679 de protección de datos, comienza a limitar la captación indiscriminada de datos personales, pudiendo entenderlo de forma extensa, como cualquier tipo de información que se pueda asociar a una persona. Así en el siguiente considerando se obliga al responsable del tratamiento a adoptar los principios de protección de datos desde el diseño y por defecto a través del principio de minimización de datos.

> *(78) (…) A fin de poder demostrar la conformidad con el presente Reglamento,* ***el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, 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.***

Y también exhorta, en el mismo considerando, a los productores de productos y servicios a que tengan en cuenta la protección de datos personales cuando diseñan los mismos:

> *Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función,* ***ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones,*** *y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. 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.*

Como vemos en el considerando anterior se propone para la privacidad en el diseño y por defecto medidas como seudonomización, y la reducción al máximo en el tratamiento de los datos personales, que entre otras cosas, evitarían los incidentes en la privacidad.

¿Hay voluntad de aplicar las medidas de la privacidad en el diseño?

Los incidentes en privacidad conllevan consecuencias negativas como mala imagen corporativa, indignación de los usuarios, supervisión de las entidades de control de

protección de datos, imposición de sanciones, nuevos marcos regulatorios, y sin embargo tales incidentes son cometidos por unas compañías con un talento y unos medios tecnológicos fuera de toda duda. ¿Por qué entonces no se implantan programas basados en Privacy by design?, porque como otras falsas dicotomías, que ya hemos comentado, las consideraciones comerciales están por encima de las de privacidad, y por lo tanto lo que prima es el negocio, bajo eufemismos del tipo*"queremos cambiar el mundo"*, pero hasta que el legislador u otros órganos potestativos no creen un modelo de privacidad en el diseño que las empresas puedan tomar como referencia, la privacidad estará siempre relegada a un segundo plano. Es muy probable que compañías como Google y Facebook, con la cantidad de recursos que tienen, cuando diseñan un nuevo producto prevean las consecuencias en la privacidad de tal producto, pero que su aplicación quedaría supeditada a cómo afecta a su modelo comercial, tal y como hemos explicado en páginas precedentes.

Estamos viendo por lo tanto un choque entre nuestra normativa actual y la realidad, liderada por las empresas tecnológicas de Internet. Por ello es necesario encontrar soluciones prácticas que garanticen la eficacia de las normas actuales.

5. PROPUESTAS TÉCNICAS A LA PRIVACIDAD ONLINE

Hay una idea generalizada que apunta a la solución técnica como una posibilidad viable de solución a la privacidad online. La solución técnica es primordial para dotar de eficacia a la privacidad online porque en caso contrario la normas quedan, como se está comprobando, con una eficacia limitada. Aunque creo que no se debe prescindir, sin más, de la parte jurídica, porque se trata de un derecho fundamental y una cuestión de derechos humanos, como así se ha reconocido en la decisión del Consejo de Derechos Humanos[16] de crear el mandato para la ONU del *"Relator Especial sobre Privacidad" ("rapporteur"),* afirmando que la privacidad se aplica a las comunicaciones digitales.

En cualquier caso, la privacidad en el diseño debe partir de una serie de propuestas técnicas, adoptadas a través de modelos, estándares o normas de obligado cumplimiento si queremos dotarle de sentido. Por ello es interesante ver a continuación una serie de

propuestas técnicas que nos sirvan de orientación para intentar formar un modelo de privacidad en el diseño.

5.1 Consideraciones del "Internet Engineering Task Force" (IETF) e "Internet Architecture Board (IAB)".

El Grupo de Trabajo de Ingeniería de Internet ("Internet Engineering Task Force") (IETF) es una organización sin ánimo de lucro y de carácter abierto, creada en 1986 y formado por un equipo interdisciplinar, cuya misión es crear propuestas y estándares de Internet, conocidos como RFC, *("Request for Comments")* que se remontan a 1969, cuando Steve Crocker inventó un sistema de comunicación en ARPANET, la precursora de Internet. Esta organización es la referencia en Internet para configurar los aspectos técnicos de la operatividad en la red.

"Internet Architecture Board (**IAB**)"[17] es un comité ejecutivo del IETF que propone directrices técnicas para el desarrollo de Internet.

El IETF y el IAB, con una clara vocación técnica, prescinden de todo prejuicio legal y no entra dentro de sus objetivos principales crear un marco de protección de la privacidad como un derecho reconocido, entre otras cosas porque existen diferentes interpretaciones de regulación de la privacidad a lo largo y ancho del mundo. Sin embargo hay un hecho que les hace reaccionar, y es la revelación, o confirmación para otros, de Edward Snowden, del seguimiento y acceso masivo a los datos de los usuarios de Internet y demás redes de telecomunicaciones, y esto supone un torpedo a la línea de flotación de Internet, que es LA CONFIANZA.

Una de las consecuencias en Europa de tales hechos fue la anulación del acuerdo de Puerto Seguro, que regulaba la transferencia internacional de datos entre EEUU y la UE, por la sentencia del Tribunal de Justicia Europeo de 6 de octubre de 2015[18] (caso Puerto Seguro) recordándonos en dicha sentencia que

> *"el acceso masivo de los datos de ciudadanos europeos por parte de las autoridades estadounidenses va más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional"*, y además recuerda que *"no está prevista la posibilidad de que los titulares de los datos, ya sean estadounidenses o de la [Unión], puedan acceder a sus datos, rectificarlos o suprimirlos, ni obtener reparación administrativa o judicial, en lo que respecta a la recogida y el tratamiento posterior de sus datos personales en virtud de los programas de vigilancia estadounidenses»*

lo que es una evidente contradicción con la **Carta de los Derechos Fundamentales de la Unión Europea en sus arts, 7, 8 y 47,** sobre todo en éste último artículo en cuanto a la tutela judicial efectiva. Pero es que además se reconoce en dicha sentencia del Tribunal de Justicia que las autoridades públicas se extralimitaron en sus funciones.

> *"En dicha sentencia el tribunal apreció que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la Unión a Estados Unidos servían a finalidades necesarias e indispensables para el interés público. No obstante, el referido tribunal añadió que las revelaciones del Sr. Snowden habían demostrado que la NSA y otros organismos federales habían cometido* ***«importantes excesos»".***

Lo que motiva esta sentencia en Europa no es más que una pérdida de confianza sobre el uso de los datos en EEUU por sus autoridades públicas, sin olvidar que los países de la UE *hacían* lo mismo, en mayor o menor medida, y según sus posibilidades.

Todo ello preocupa a entidades como la "**Internet Engineering Task Force** (**IETF**)", proponiendo que la privacidad deje de ser un asunto que recaiga sobre el usuario final, y que sea prioritario en el diseño de los nuevos protocolos o actualización de los existentes.

Para ello lo introducen un glosario de privacidad *(privacy vocabulary)*, así como la encriptación y privacidad en el diseño en todas las capas de la Red. La regulación de los estándares de Internet no está exento de dificultades, bien por las restricciones que

imponen ciertos estados, o bien por la dificultad que se adopten uniformemente tales estándares por los proveedores de servicios.

Para la IETF la seguridad y la encriptación es fundamental para dotarle de sentido a la privacidad en la Red. Conviene recordar iniciativas de entidades certificadoras como *Let's Encrypt*.[19]

Recordemos, que el Grupo de Trabajo del Artículo 29 [20] recomienda la aplicación del *Privacy by Design y Security by Design*, incluyendo la criptogafría a la hora de diseñar nueva tecnología.

> *"Los fabricantes de dispositivos deben seguir un proceso de seguridad por diseño y dedicar algunos componentes a las primitivas clave de criptografía".*

Así como en su opinión sobre geolocalización y aparatos inteligentes[21]:

> *"El desarrollador del sistema operativo de el dispositivo móvil inteligente puede ser un responsable del tratamiento de los datos de geolocalización cuando interactúa directamente con el usuario y recopila sus datos personales (ya sea a través de un registro o recolectando información sobre la ubicación a efectos de mejorar los servicios). Como controlador, el desarrollador debe adoptar los principios de la privacidad por diseño para prevenir el seguimiento secreto, ya sea por el propio dispositivo o por otros dispositivos o aplicaciones".*

En cuanto a la encriptación hemos visto actualmente como Apple ha blindado el acceso a los datos del Iphone, o como WhatsApp[22] ha encriptado los mensajes de punto a punto, o como hay países que son más proclives a la encriptación como Alemania u Holanda frente a otros más represores de los derechos civiles como Rusia, Marruecos, Pakistán o Irán, quienes prohíben la encriptación en las comunicaciones. Por ejemplo Alemania ha ido más allá y en la ***"Charta for Strengthening Confidential Communication"*** [23] ha proclamado que la encriptación debe ser el estándar para las comunicaciones privadas.

5.2 Estandarización y protocolos.

El gobierno de Internet está descentralizado, regulándose a través de estándares, reglas, o principios desarrollados por equipos interdisciplinares y de distintas organizaciones y que en teoría no están sometidos a una autoridad formal.

Internet se construye sobre diferentes protocolos como el TCP/IP (Transmission Control Protocol/Internet Protocol) que facilita la transmisión de datos a través de las distintas capas de la red como son:

- **Capa 4** o **capa de aplicación.** *Applications' layer.*
- **Capa 3** o **capa de transporte**: *Transport layer.*
- **Capa 2** o **capa de internet**: *Network layer.*
- **Capa 1** o **capa de acceso al medio**: *Link layer.*

La capa 4 es la más conocida, porque en ella se incluyen protocolos de aplicación como FTP (File Transfer Protocol), HTTP (HyperText Transfer Protocol) Y HTML (HyperText Markup Language).

Tales protocolos están basados en estándares técnicos *("Intenet standars")* creados por la IETF, IAB, los cuales son de adhesión voluntaria y en los que nadie tiene el control o la propiedad sobre tales protocolos.

Una de las características innovadoras que el nuevo modelo de privacidad de IETF es que propone la implementación de la privacidad por diseño en todas las capas de Internet y no sólo en los protocolos de Internet de núcleo (capa baja como la 1).

5.3 Amenazas en la privacidad.

The Internet Architecture Board (IAB), en su informe ***"Privacy Considerations for Internet Protocols"*** [24] hace un alegato a modo de introducción sobre las consecuencias

de la pérdida de privacidad cuando los ciudadanos están siendo espiados de forma masiva.

Por ejemplo la falta de privacidad

> ***"puede dañar la reputación, haciendo que la información de un individuo, sea verdadera o falsa, puede provocarle un estigma, vergüenza, o pérdida de dignidad personal", puede dañar "la libertad de expresión", "libertad de asociación", o incluso puede poner en peligro su "integridad física", además de los daños económicos cuando por ejemplo un ciudadano es víctima de una "estafa", "suplantación de identidad" u otro delito en la red.***

Una verdadera declaración de las consecuencias de falta de privacidad, y no quedándose solo en una declaración pasa a enumerar las amenazas para la privacidad:

- ✓ ***Vigilancia.***

En el informe se señala que la vigilancia como *observación* o *seguimiento* de las comunicaciones puede generar "*desde ansiedad e incomodidad hasta actitudes como la inhibición y la autocensura, e incluso la perpetración de la violencia sobre el individuo"*.

El informe lanza la siguiente idea que merece tomarse en cuenta:

> ***"La vigilancia puede afectar a la privacidad, incluso si los individuos vigilados no son identificables o si sus comunicaciones son cifradas".***

Afirmando que *"la sola posibilidad de ser vigilado puede ser suficiente para anular la autonomía de una persona"*, y tenemos que añadir, que la vigilancia afecta además al *"libre desarrollo de la personalidad"* reconocido en el artículo 10 de la Constitución Española.

- ✓ ***Almacenamiento de datos.***

El almacenamiento de datos está continuamente amenazado por ataques externos, con los consabidos daños financieros y en la reputación. En este apartado las normativas de protección de datos inciden en la obligación de implementar las medidas técnicas y organizativas que impidan el acceso no autorizado.

- ✓ ***Intrusión.***

Como acto invasivo, que perturba el "derecho de estar solo" *(to be left alone)*, siendo los más comunes el *spam*, o correo no solicitado, y la denegación de servicio.

- ✓ ***Falsa atribución***

Cuando por ejemplo, a un usuario se le atribuyen los datos o las comunicaciones de un tercero, igualmente puede afectar a su reputación con consecuencias legales indeseadas en muchos casos. Desde el punto de vista de los protocolos, este daño se produce porque el sistema de identificación o autenticación no es el correcto, o porque una misma dirección IP es compartida por distintos usuarios con un sistema deficiente de gestión de identidad o autenticación.

- ✓ ***Correlación o cruce de datos.***

El cruce de datos de una sola persona obtenido de una única fuente o de distintas genera la posibilidad de aumentar el conocimiento de esa propia persona y la capacidad de juzgarla y, cómo no, de predecir futuros comportamientos lo que indudablemente amenaza *"su autonomía individual y reputación"*.

- ✓ ***Identificación.***

Según el diccionario de la lengua española, en su cuarta acepción, identificar lo define como *"dar los datos personales necesarios para ser reconocido"*.
Lógicamente, la identificación la entendemos como obligatoria o forzada según el escenario en el que se actúa, por ejemplo, la identificación obligatoria es la realizada por los fuerzas y cuerpos de seguridad del estado, o aquella identificación de identidad necesaria para acceder a determinados servicios. No se nos escapa que la identificación también es un arma de control propia del gobierno, y legítima dentro de un contexto de estado de derecho. En todo caso existe un derecho de anonimización o pseudonimización, ya contemplado por el propio Reglamento europeo de protección de datos.

Art. 4 definiciones. Reglamento (UE) 2016/679

> *4)* ***«seudonimización»:*** *el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;*

Considerando (78)

> *La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento,* ***el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto****. Dichas medidas podrían consistir, entre otras, 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 (…).

Se insiste por parte del legislador en la utilización de medidas como la seudonimización, y muy importante, como recuerda la directiva 2016/680 "*relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos"*, en su considerando (53), que *tales medidas no pueden quedar supeditadas a intereses o criterios económicos*, prevaleciendo la privacidad. Esto tiene una especial relevancia cuando el dato (personal) es considerado como el nuevo petróleo del siglo XXI.

- ✓ ***Usos secundarios.***

Es el uso de información para otros usos distintos de los que fueron inicialmente previstos en la captación, incluyendo la revelación de tal información a terceros. Tal protección está fuera del alcance de los protocolos de la IETF, tal y como ellos afirman.

- ✓ ***Revelación o divulgación.***

La revelación de información sobre un individuo, o su mera posibilidad, no sólo merma la confianza de las personas, sino que puede ser origen de innumerables daños en dicha persona. Muchas veces, la revelación de la información no es intencionada porque el propio sistema no la asocia a datos personales. La IETF, por ejemplo, propone que en la geolocalización los usuarios puedan decidir si tales datos pueden revelarse a terceros.

- ✓ ***Exclusión.***

Es el negación a una persona de conocer qué datos se tienen sobre la misma y no permitirle participar en su forma de recolección y uso, es por lo tanto una negación del control de la propia información y su capacidad para disponer libremente de ella.

5.4 Mitigación de amenazas.

Según la IEFT, y como buenos ingenieros, afirman que la privacidad es difícil de medir y cuantificar, y que los mecanismos de protección dependen de distintos factores como su *diseño, uso, o su mal uso*, y proponen una serie de medidas para mitigar las amenazas:

a) Minimización de datos.

Por minimización de datos se entiende la captación de aquellos datos que son estrictamente necesarios para la finalidad inicialmente prevista, *(collection limitation).*

Lógicamente los diseñadores de protocolos únicamente pueden aconsejar sobre esta limitación, pero se trata de una decisión, en parte subjetiva, de quien se propone recolectar datos personales. Sin embargo, según la IEFT la mejor opción para el diseño de protocolos en la minimización de datos es limitar la identificación bien a través de pseudonimización o anulación total de la identificación.

La minimización de datos, como indica la IEFT, mitiga las siguientes amenazas: *vigilancia, datos almacenados compromiso, correlación, identificación, uso secundario, y divulgación*

b) Anonimización. (Anonymity).

Para conseguir la anonimización, según la IEFT, tienen que existir unas serie de individuos con un conjunto de características comunes o parecidas, de tal manera que para un intruso no haya posibilidad de identificarlos individualmente, a esto se les trata

como conjuntos de anonimato,(set anonymity) aunque sus miembros pueden ir variando con el tiempo.

c) ***Pseudonimización. (Pseudonymity).***

En los protocolos de Internet casi todos los sistemas de identificación permiten el uso de apodos *("nickname")* o pseudonimización, no siendo necesaria la aportación de datos personales, salvo en determinados contextos.

La IEFT añade las siguientes consideraciones de importancia para los protocolos de Internet: *si los protocolos de identificación pueden cambiarse sin la intervención humana, ¿a quién se exponen los seudónimos?, ¿cómo pueden controlar los individuos la divulgación?, ¿cada cuánto pueden cambiarse los seudónimos y sus consecuencias?.*

d) ***Confidencialidad de Identidad.*** (*Identity Confidentiality).*

Cuanto más pequeño es un conjunto de anonimización más posibilidades existen de ser identificado.

La IEFT indica el ejemplo los procedimientos de autenticación de acceso a la red utilizando el protocolo de autenticación extensible (EAP), (*Extensible Authentication Protocol),donde se invita a utilizar los medios de encriptación que facilita el propio sistema EAP.*

e) ***Minimización de datos dentro de la gestión de identidades. (****Data Minimization within Identity Management).*

La IEFT nos recuerda que los sistemas actuales para autenticar a los individuos dependen cada vez más de la interacción entre diferentes partes, y que muchos de estos sistemas utilizan proveedor de identidad que es responsable de proporcionar funcionalidad AAA *(Authentication, Authorization, Accounting)* a una entidad de confianza, asumiendo ambas la responsabilidad de la autorización y minimizando en

muchos casos la recolección de datos, porque por ejemplo una entidad de confianza no necesitará tener conocimiento de ciertos datos.

f) Participación del usuario. *(User Participation).*

Lo sistemas normativos de protección de datos incluyen la obligatoriedad del derecho de información en la recopilación de datos personales. Para la IEFT la participación de los usuarios mitiga las siguientes amenazas: vigilancia, uso secundario, divulgación y exclusión.

g) Seguridad. *(Security).*

Mantener la seguridad de los datos tanto en la custodia como en el tránsito, lo que incluye:

- *Confidencialidad.*
- *Autenticación de entidades pares. Peer entity authentication.Asegurar que el destinatario final de la comunicación es quien debe ser.*
- *Uso autorizado.*
- *Uso apropiado.*

Si bien son loables las intenciones del Internet Engineering Task Force" ("IETF"), sobre todo en la idea de aportar soluciones técnicas a la privacidad online, no deja de ser una exposición de buenas intenciones con soluciones puntuales, pero que en cualquier caso supera la iniciativa de nuestros legisladores que no entran a abordar el problema, o siquiera debatirlo en profundidad desde el punto de vista técnico.

Si hasta el momento hemos podido apreciar el conflicto, o la dificultad, de armonizar nuestro ordenamiento jurídico de protección de datos con la práctica de las empresas tecnológicas y gobiernos, más complicado será todavía integrar el Big Data.

6. BIG DATA COMO FUENTE DEL ALGORITMO

Big Data es el combustible de la Inteligencia Artificial (IA) mediante el cual los algoritmos se desarrollan. La IA puede tener distintas variantes como APRENDIZAJE DE MÁQUINAS *(machine learning)*, APRENDIZAJE PROFUNDO *(deep learning)* o ROBÓTICA.

Antes veamos las siguientes

6.1 Definiciones:

(i) Big Data:

IBM [25] *lo define como:*

> *"En términos generales podríamos referirnos como a la tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la cual es utilizada para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a un base de datos relacional para su análisis. De tal manera que, el concepto de Big Data aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales".*

En el año 2015 se produjo un volumen de datos de 8.591 exabytes y para el 2020 de prevé un volumen de 40.026 exabytes. *Cifras expresadas en exabytes (1 exabyte=1.000 millones de GB). Fuente: IDC*

> *"Los seres humanos estamos creando y almacenando información constantemente y cada vez más en cantidades astronómicas. Se podría decir que si todos los bits y bytes de datos del último año fueran guardados en CD's, se generaría una gran torre desde la Tierra hasta la Luna y de regreso".*

(ii) Inteligencia artificial:

Según el diccionario de la Real Academia Española

1. f. Inform. Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.

Inteligencia emocional.

1. f. Capacidad de percibir y controlar los propios sentimientos y saber interpretar los de los demás.

(iii) Algoritmo:

Según la Real Academia Española:

> *"Quizá del lat. Tardío* algobarismus*, y este abrev. del ár. clás. 'cálculo mediante cifras arábigas'.*
>
> *1. m. Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.*
>
> *2. m. Método y notación en las distintas formas del cálculo".*

(iv) Aprendizaje de máquinas (machine learning):

En 1998 la Universidad de Stanford definió el aprendizaje de máquinas[26] de la siguiente manera:

> *"En el descubrimiento del conocimiento (Knowledge Discovery),el aprendizaje automático se utiliza comúnmente para describir la aplicación de algoritmos de inducción, que es un paso en el proceso de descubrimiento del conocimiento. Esto es similar a la definición de aprendizaje empírico o aprendizaje inductivo (…). Obsérvese que en su definición, los ejemplos de entrenamiento son "suministrados externamente", mientras que aquí se supone que son*

suministrados por una etapa anterior del proceso de descubrimiento de conocimiento. El Aprendizaje Automático es el campo del estudio científico que se concentra en los algoritmos de inducción y en otros algoritmos donde se puede decir que "aprenden".

Y según wikipedia[27]:

> *"El aprendizaje automático o aprendizaje de las máquinas (del inglés, "Machine Learning") es el subcampo de las ciencias de la computación y una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas que permitan a las computadoras aprender. De forma más concreta, se trata de crear programas capaces de generalizar comportamientos a partir de una información suministrada en forma de ejemplos. Es, por lo tanto, un proceso de inducción del conocimiento. (…)"*

Siendo importantes las aplicaciones prácticas del aprendizaje de las máquinas, como por ejemplo en el buscador de Google que se utiliza para ir (auto)mejorando, o sobre todo en actual sistema financiero para prevenir el fraude.

> *"El aprendizaje automático tiene una amplia gama de aplicaciones, incluyendo motores de búsqueda, diagnósticos médicos, detección de fraude en el uso de tarjetas de crédito, análisis del mercado de valores, clasificación de secuencias de ADN, reconocimiento del habla y del lenguaje escrito, juegos y robótica".*

En su informe de la Federal Trade Commission de enero de 2016, "***Big Data, a tool for inclusion or exclusion?"*** [28] *c*onsidera que el Big Data se fundamenta en las tres uves, **volumen, velocidad y variedad de datos.**

Todo esto se ha conseguido en el 2016 por el avance tecnológico que permite un gran almacenamiento de datos más barato, mayor velocidad de procesamiento y por lo tanto más variedad de datos. Es decir, se cumple la ley de Moore que establece que cada dos años se duplica la capacidad de procesamiento de la computación lo contrario que el precio, que baja.

¿Es infalible el Big Data?

La Federal Trade Commission lanza una advertencia cuestionando le predicciones basadas en el Big data, porque si bien se detectan correlaciones de datos de forma muy precisa no se explican cuáles son válidas, y pone como ejemplo el caso de Google Flu Trends, que es un modelo de aprendizaje de máquinas predecía los casos de gripe en regiones según las búsquedas en Google, este sistema en principio consagró el Big Data porque Google era capaz de conocer antes que las autoridades sanitarias de cualquier lugar si existía una epidemia de gripe. Pero como pone de manifiesto la Federal Trade Commission este sistema no era válido porque el propio algoritmo no tenía en cuenta ciertas variables, como por ejemplo, que había personas que al oír una noticia acerca de un brote de gripe, aunque fuera en un lugar remoto, realizaban búsquedas en Google, por lo que producía predicciones inexactas.

Igualmente la Federal Trade Commission se pregunta si en la confianza que se tiene en un proceso de Big Data se han tenido en cuenta aspectos éticos, como por ejemplo, y expone el caso, de una compañía que según su análisis de Big Data quienes viven cerca de la oficina pasan más tiempo en la misma frente a los que viven lejos que no lo hacen, teniendo en cuenta que en ciertas localidades la distancia puede ser un indicador de vivir en un barrio menos favorecido o marginal, produciéndose por lo tanto un efecto discriminatorio. El ejemplo es ilustrativo aunque la Federal Trade Commission podía haber elegido un ejemplo más acertado, porque no haría falta un análisis de Big Data para llegar a tal conclusión.

Hay sin embargo otras compañías, según la Federal Trade Commission, que están teniendo en cuenta los aspectos éticos a la hora de diseñar sus estrategias de Big Data con el objeto de obtener ventajas competitivas.

6.2 ¿Qué tipos de datos se recopilan en el big data?

IBM, y siguiendo el informe anterior, los clasifica según provengan de:

1-Web sites y redes sociales.

2-Tecnologías "Máquina- Maquina" *Machine-to-Machine (M2M).*

También podemos incluir el ***Internet de las cosas (Internet of Things** or **IoT)***, donde los aparatos se conectan entre sí a través de Internet, siendo de aplicación no sólo a nivel doméstico, como las llamadas casas inteligentes, si no a nivel empresarial afectando a todo tipo de sectores optimizando los recursos, reduciendo costes y aumentando la efectividad, propio de un modelo basado en el conocimiento y la información.

> Según Intel [29]:
>
> *"Internet de las Cosas" está explotando. Se compone de miles de millones de dispositivos "inteligentes" -desde virutas minúsculas a máquinas gigantescas- que utilizan la tecnología inalámbrica para hablar entre sí (y con nosotros). Nuestro mundo de IoT está creciendo a un ritmo impresionante, de 2 mil millones de objetos en 2006 a un proyectado 200 mil millones en 2020. Eso será alrededor de 26 objetos inteligentes para cada ser humano en la Tierra.*

Su implantación actual en EEUU, y siguiendo el informe de Intel, el Big Data se desarrolla de la siguiente manera:

> - *40.2 % en negocios y manufactura*: análisis en tiempo real de las cadenas de suministro y equipos, maquinaria robótica.
>
> - *30.3 % en salud:* vigilancia sanitaria portátil, registro electrónico, salvaguardias farmacéuticas.
>
> - *8.3 % en minorista*: seguimiento de inventario, compras de teléfonos inteligentes, análisis anónimo de las opciones de los consumidores.
>
> - *7.7 % en seguridad*: bloqueos de reconocimiento biométrico y facial, sensores remotos.

3.- *Operaciones transaccionales*: pensemos en el volumen de datos generados sólo por el sector financiero y el de telecomunicaciones.

4.- *Biométricos*: información biométrica como escaneo de la retina, huellas digitales, reconocimiento facial, datos genéticos, etc. Pensemos en la importancia que tienen este tipo de datos actualmente para la seguridad.

5.- *Generados por las propias personas*: todos aquellos datos provenientes por ejemplo de nuestros correos electrónicos o llamadas, entre otros.

- ✓ ***Big Data v minimización de datos:***

Los beneficios del Big Data son incuestionables y como nuevo modelo de negocio el Big Data es un auténtico reto para preservar el derecho de la privacidad y de la protección de datos personales. El principio de minimización de datos, por ejemplo, resulta totalmente incompatible con la idea del Big Data, que precisamente se basa en la recopilación indiscriminada de datos.

Como expone Ira S. Rubinstein en su artículo ***"Big Data: The End of Privacy or a New Beginning?"*** [30]*:*

> "*el Big Data generará en los Estados Unidos 300 mil millones de dólares en la industria de la salud, 250 millones de dólares por año en la administración del sector público europeo, 100.000 millones de dólares en ingresos adicionales para los proveedores de servicios de datos de localización, 60% en los márgenes netos de la industria minorista y hasta 50% en el desarrollo de productos y los costos de montaje en la manufactura. En estos tiempos de recesión, las cifras de esta magnitud difícilmente pueden ser ignoradas".*

La recolección de datos basados en el Big Data tiene una serie de características que chocan frontalmente con principios básicos de las normativas de protección de datos personales. Como nos recuerda Ira S. Rubinstein, en el artículo citado anteriormente, en

los procesos de ingeniería de datos (“*data mining”*), por ejemplo, no se puede informar a los usuarios de la finalidad del tratamiento porque realmente se desconoce qué es lo que se va a extraer de la recolección de datos, es decir, el Big Data es impredecible porque recopila información, pero no se sabe para qué, hasta que no se produce un análisis de conclusiones. De este análisis, por parte de Ira S. Rubinstein, podemos llegar por lo tanto a la conclusión, que si no podemos informar de lo que no sabemos, el consentimiento, otro pilar en la protección de datos de carácter personal es imperfecto, al no ser *libre, específico e informado*, siendo por lo tanto inválido.

Recordemos del Reglamento Europeo de Protección de Datos:

> *Considerando 32*
>
> *“El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado.”*

En un proceso de Big Data, el consentimiento informado y específico no se cumpliría, ni tampoco lo señalado en el mismo considerando respecto a que dicho consentimiento debe darse para todas las actividades del tratamiento, porque se desconoce el resultado.

> *“El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.”*

Como también un proceso de Big Data tendría un difícil encaje en:

> - El artículo 5.1. “*Principios relativos al tratamiento: Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)”*, porque básicamente al desconocerse las previsiones del Big Data no puede haber transparencia, así como en el apartado de dicho artículo, … “*los datos personales serán… c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)”*, porque la finalidad del tratamiento se desconoce.

- El artículo 7.3. "*Condiciones para el consentimiento. El interesado tendrá derecho a retirar su consentimiento en cualquier momento*". También de difícil aplicación porque el poder de control de los datos se diluye a través de distintos procesos de Big Data que pueden estar en distintas manos.

- El artículo 14. "*Derecho de acceso del interesado a los datos personales,* porque se desconocen, *"(…) (a) los fines y la base jurídica del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales; d) cuando sea posible, el plazo contemplado durante el cual se conservarán los datos personales o, de no ser posible, los criterios utilizados para determinar dicho plazo (…)*

Y además,

- El Artículo 27. *"Evaluación de impacto relativa a la protección de datos"*, que debería aplicarse en todo proceso de Big Data, porque son imprevisibles las conclusiones que pueden derivarse del mismo.

- ✓ ***Big data v anonimización:***

Las normas de protección de datos se basan en datos de carácter personal, pero en el Big Data se recopilan todo tipo de datos (personales o no) de manera indiscriminada, y el gran problema surge cuando se produce la **re-identificación**, es decir cuando los datos anónimos los podemos asociar a una determinada persona.

El Informe de la Agencia Española de Protección de Datos de 2016 ***" Procedimientos y garantías en los procesos de anonimización de datos personales***[31]***"*** en un ejercicio de realidad concluye:

"Los procesos de anonimización y seudonimización son una herramienta válida para garantizar la privacidad de los datos personales y sus limitaciones son inherentes al avance de la tecnología. ***Existe una proporcionalidad manifiesta en lo que respecta a la capacidad tecnológica de anonimizar y la posibilidad de la reidentificación de las personas cuyos datos han sido anonimizados,*** *es decir,* ***la misma capacidad de la tecnología para anonimizar datos personales puede ser utilizada para la reidentificación de las personas.*** *Además, hay que tener en cuenta el riesgo que la propia sociedad de la información añade a los datos anonimizados, riesgo que por otra parte evoluciona a lo largo del tiempo, por lo que habrá que contemplar el riesgo de los procesos de anonimización como una contingencia latente a lo largo de la vida de la información y no en un momento concreto, y, en consecuencia, las medidas encaminadas a valorar y gestionar los riesgos deben tener carácter periódico.* ***No es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen".***

Y, por ejemplo, en un estudio realizado por la revista Science[32] en 2015 lo demuestra:

"Los conjuntos de datos a gran escala del comportamiento humano tienen el potencial de transformar fundamentalmente la forma en que luchamos contra enfermedades, diseñamos ciudades o realizamos investigaciones. Los metadatos, sin embargo, contienen información sensible. La comprensión de la privacidad de estos conjuntos de datos es clave para su amplio uso y, en última instancia, su impacto. Estudiamos durante 3 meses los registros de tarjetas de crédito de 1,1 millón de personas y demostramos que cuatro parámetros espacio temporales son suficientes para reidentificar de manera única al 90% de los individuos. Mostramos que el conocer el precio de una transacción aumenta de promedio el riesgo de re-identificación en un 22%. Finalmente, vimos que incluso en los conjuntos de datos que proporcionan información aproximada en cualquiera o todas las dimensiones se garantiza poco

anonimato, y que las mujeres son más reidentificables que los hombres en los metadatos de tarjetas de crédito".

O en datos de salud, como puso de relevancia, la Universidad de Harvard en 2013[33], identificando entre el 84% y 97% de los que participaron en un proyecto anónimo del genoma.

Y por eso el Reglamento (UE) 2016/679 prevé:

> *Considerando (75) "Los riesgos para los derechos y libertades de los interesados, de diversa probabilidad y gravedad, pueden producirse debido a un tratamiento de datos capaz de provocar daños físicos, materiales o inmateriales, en particular cuando el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional,* ***inversión no autorizada de la seudonimización****, o cualquier otro perjuicio económico o social significativo"…*

Interesante la inclusión expresa a la "*inversión no autorizada de la seudonimización*", donde ya el propio reglamento es consciente de este hecho.

Como hemos podido observar a través de estos ejemplos, el Big Data cuestiona el principio fundamental de minimización de datos, que es uno de los pilares de nuestro actual sistema, porque no sabemos qué uso van a tener los datos, y en consecuencia los principios de información y consentimiento quedan limitados, y todo esto sin perder de vista los evidentes beneficios del Big Data en nuestra sociedad. Pero parece que ni los gobiernos ni las empresas van a querer perder una oportunidad y quedarse descolgados frente a terceros países donde además juegan con ventaja porque en muchos de ellos sus ciudadanos no tienen garantizados sus derechos y libertades individuales, incluyendo la privacidad. En cualquier caso, y a raíz de las revelaciones de Snowden, ¿a existido alguna responsabilidad penal?, o ¿algún gobierno de las llamadas democracias liberales lo ha exigido, salvo la persecución a Assange o Snowden?

Pero no solamente se pone en cuestión el principio de minimización de datos, si no el mismo concepto de dato personal, porque el Big Data engulle todo tipo de datos, sean o no personales ya que estos pueden finalmente asociarse a una persona como trataremos a continuación.

6.3 ¿Cómo se compatibiliza el big data con el nuevo Reglamento Europeo de Protección de Datos?

Pues difícilmente, veamos por ejemplo la definición de elaboración de perfiles del art 4, **Reglamento (UE) 2016/679**

> *"Definiciones 4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física";*

¿Sólo datos personales?

Se alude en todo momento a datos personales, pero recordemos que en el Big Data se recopilan datos personales y no personales, y estos últimos pueden asociarse a una persona determinada y por lo tanto "*analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*".

> *"Considerando (30):* ***Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos****, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos*

por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas"·.

¿ No podría ser cualquier dato de un individuo en la red un identificador en línea?

Tal y como hemos visto anteriormente, un simple dato combinado con otro, u otros más, pueden producir un proceso de reidentificación.
Hay una consideración especial a los menores, pero en un proceso de Big Data para discriminar los datos de los niños tendría que producirse a través de un modelo de privacidad en el diseño desde la propia fuente u origen de captación, es decir preverse.

"Considerando (38): Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

¿Deber de información en el Big Data?

Al menos así lo prevé el Reglamento,

Considerando (60) "Los principios de tratamiento leal y ***transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines.*** *El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales.* ***Se debe además informar al interesado de la***

> ***existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración.*** *Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.*

Se insiste en el deber del derecho de la información cuando se captan datos personales, pero como ya se adelantó al tratar el Big Data, es imposible prever las finalidades del tratamiento porque este modelo es impredecible.

Incluyendo en el *considerando (51)* como un riesgo para los derechos y libertades de los individuos, por ejemplo, cuando un tratamiento puede dar lugar a discriminación, como pueden ser los derivados de un proceso de Big Data o cuando se re-identifica un dato anónimo.

> *Considerando (51) "****Los riesgos para los derechos y libertades de los interesados, de diversa probabilidad y gravedad, pueden producirse debido a un tratamiento de datos capaz de provocar daños físicos, materiales o inmateriales, en particular cuando el tratamiento pueda dar lugar a problemas de discriminación,*** *usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional,* ***inversión no autorizada de la seudonimización****,*

Incluyendo cuando se realizan predicciones de la personalidad

> *(…) o* ***cuando se evalúen aspectos personales, en particular en el marco del análisis y la predicción de aspectos referidos al rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la ubicación o los movimientos, con el fin de crear o utilizar perfiles personales; (…) o cuando el tratamiento se refiera a***

una gran cantidad de datos personales y afecte a un elevado número de interesados".

¿Un derecho de acceso en el Big Data?

*Considerando (63) "**Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho** con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. (…) Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos **cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento.** Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. (…).*

El derecho de acceso a los datos personales en principio no debería ser un problema si el proceso de Big Data está controlado por una única entidad o procesador y no es un proceso de retroalimentación continua, es decir que la realidad puede ser más compleja, otra cuestión es acceder a las predicciones efectuadas con otros parámetros ajenos a los datos personales del afectado, sin olvidar pero que podrían someterse a un proceso de re-identificación de la persona.

¿Un tratamiento en el Big Data libre de error?

Recordemos que el Big Data se nutre de datos en estado bruto.

*Considerando (71): "A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, **el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados***

> ***para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error****, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas,* ***efectos discriminatorios*** *en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.* ***Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas".***

En este considerando se exige la utilización de medios técnicos o matemáticos como pueden ser algoritmos que eviten por un lado el error de la muestra, que eviten daños o que induzca a generar discriminación en las personas. Como ya advertía la "FTC" el error se produce en el sesgo. Es importante esta declaración, y nunca está de menos recordar que los sistemas de tratamiento automatizado de datos siempre han sido una tentación por regímenes autoritarios con la idea de diseccionar a la sociedad en grupos y su consecuente opresión, como por ejemplo, con relación al papel que algunos autores atribuyen a IBM en el holocausto:

> *IBM y el holocausto*[34]*:*
>
> *"Cada persona internada en los campos de exterminio nazi tenía una ficha informática. Se trataba de tarjetas perforadas, el material avanzado de la época. Si el interno era judío, su número clave era el 8. Si era homosexual, el 3. Si era gitano, el 12. Esas tarjetas, que permitieron al régimen de Adolf Hitler identificar, localizar y clasificar a millones de víctimas, eran fabricadas por IBM en Estados Unidos. Y los directivos de la compañía sabían perfectamente cuál era su uso en Alemania. (…)"*

Prohibición de las decisiones basadas únicamente en un tratamiento automatizado.

A través del art 11 del Reglamento (UE) 2016/679 se regula la prohibición absoluta del cruce de datos que generen decisiones con efectos jurídicos negativos para las personas. Es importante el matiz que introduce el reglamento, acerca de la *"prohibición en las decisiones"*, y no la *"prohibición en el tratamiento"*, cuestión fundamental en el Big Data, aunque muchas decisiones se tomarán de forma subjetiva, difícil de demostrar que fue fruto de un tratamiento automatizado. El artículo introduce también otro matiz importante, y es el de la exclusividad, *"decisiones basadas* ***únicamente*** *en un tratamiento automatizado"*, una excepción que puede generar más conflicto en la interpretación de la norma y que será interesante observar en la casuística.

> *Artículo 11* ***Mecanismo de decisión individual automatizado***
>
> *1.****Los Estados miembros dispondrán la prohibición de las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado*** *o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento.*

El tratamiento de datos personales relativos a condenas e infracciones penales

> *2.****Las decisiones a que se refiere el apartado 1 del presente artículo no se basarán en las categorías especiales de datos personales contempladas en el artículo 10,*** *salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*
>
> *3.La elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 quedará prohibida, de conformidad con el Derecho de la Unión.*

Y en el artículo 22 del Reglamento (UE) 2016/679 se prevé el **derecho a oponerse a los cruces de datos que puedan producir efectos jurídicos en una persona**. Se trata de una declaración de principios que reafirma el derecho de las personas frente a esta práctica aunque no estará exenta de discrepancias por las diferentes interpretaciones y casuística, entre otras cosas porque la toma de decisiones vendrán determinadas por los resultados del Big Data, y así es como la industria lo prevé.

> *Reglamento Artículo 22* ***Decisiones individuales automatizadas, incluida la elaboración de perfiles***
>
> ***1.Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.***

El apartado 2 enumera una serie de excepciones, entre las que destaca, como siempre el consentimiento explícito del interesado. Será interesante ver cómo se ejecuta el consentimiento expreso en cada caso, si es libre y legítimo ya que éste puede generar *a posteriori* efectos negativos en dicha persona.

> *2.El apartado 1 no se aplicará si la decisión:*
> *a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;*
> *b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o*
> *c) se basa en el consentimiento explícito del interesado.*

Otorgando a la persona afectada el derecho a impugnar tales decisiones basadas en la generación de un perfil. De nuevo estamos ante una figura de derecho de oposición que no estará exenta de polémica porque en parte anula la esencia misma del Big Data, considerado como un fenómeno imparable.

3.En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo ***el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.***

4.Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Parece difícil por lo tanto oponerse al tratamiento de los datos en procesos de Big Data, tanto por la propia naturaleza del Big Data como las intenciones de la industria y gobiernos de aprovechar sus oportunidades. Otro tema será las consecuencias derivadas de dichas predicciones para las personas, que habrá que vigilar para evitar discriminaciones. En cualquier caso el asunto es complejo, porque hay predicciones que no tienen ninguna base objetiva, y se utilizan. Por ejemplo te pueden denegar un crédito porque no tienes ingresos suficientes (criterio objetivo), pero ¿te lo pueden negar porque compras con la tarjeta de crédito música reguetón? (criterio subjetivo).

6.4 Propuestas a la dicotomía Big Data , privacidad.

Viendo la dificultad que existe de integrar el Big Data en los actuales modelos de privacidad, no está de más tener en cuenta propuestas como las siguientes, que no hacen más que abrir un debate y reflexión necesaria:

- ✓ COMPARTIENDO LA RIQUEZA. *'Sharing the wealt*[35]*'*. Propuesto por Jules Polonetsky, profesor en Washington de la facultad de derecho de *Lee y* CEO de *"the Future of Privacy Forum"*.

Partiendo de los innegables beneficios que aporta el uso del Big Data, tanto en la productividad, eficiencia y desarrollo, ya sea de las personas físicas, empresas o gobiernos, el autor comienza argumentando que otros valores como la libertad de expresión, seguridad, o desarrollo no pueden quedar supeditados o limitados por un derecho fundamental como es el de privacidad, debiendo tenerse en cuenta esas otras consideraciones sociales. Partiendo de la idea de que el dato es un valor, el responsable del tratamiento debería facilitar el acceso a esos datos para que las personas puedan obtener beneficios de los mismos creándose nuevas oportunidades de negocio.

- ✓ EMPODERAMIENTO DEL CONSUMIDOR. "Consumer empowerment". Propuesto por Doc Searls[36].

Siguiendo el argumento de Jules Polonetsky & Omer Tene, a los individuos se les debe de dotar de herramientas para que puedan gestionar su propia información, controlarla y poder compartirla en un entorno económico del que puedan obtener un beneficio creándose por lo tanto un nuevo modelo de negocio. A través de su libro "***The Intention Economy: When Customers Take Charge"*** , el autor anticipa un nuevo orden comercial donde los individuos, a través del control de sus datos, serán actores libres e independientes en un mercado donde podrán decir a las empresas qué quieren, cómo, dónde , cuándo y a qué precio.

Para ello Doc Searls propone un modelo que denomina **Gestión de relaciones con proveedores** ("**VRM**", "Vendor Relations Management"), frente al conocido CRM (*Customer Relationship Management*), pudiendo establecerse ocho elementos principales:

1- El individuo como el centro de la captación y gestión de los datos personales.
2- La divulgación selectiva de datos según el criterio de cada individuo.
3- El control sobre la finalidad y uso de sus datos en usos primarios y secundarios. Este control puede desarrollarse a través de contratos, o soluciones técnicas como DRM ("*Digital Rights Management"*) o metatags.
4- La indicación o medios a través de los cuales el individuo expresa sus demandas.

5- La gestión de la identidad, bien sea través de la autenticación o cualquier otra y que evite la correlación o cruce de sus datos sin autorización.
6- Una alta seguridad.
7- La responsabilidad (*"accountability")* y normas que custodien el derecho de los individuos.

La novedad de este tipo de planteamientos es el otorgamiento al individuo del poder de control de sus datos personales desde un punto de vista económico, cuestión que no ha pasado desapercibida para compañías de telecomunicaciones como Telefónica[37], en su pugna con las GAFA (Google, Amazon, Facebook, Apple) proponiendo nuevos modelo de negocio:

> *"Telefónica quiere que sus clientes cobren a Google y Facebook por usar sus datos. La operadora prepara una plataforma que permita a sus abonados controlar la información que manejan sobre ellos las firmas de Internet"*.

O surgiendo nuevos web sites como https://www.citizenme.com donde incluso se pueden donar los datos personales para "causas justas".

6.5 Porque ¿cuánto cuestan nuestros datos?

Recordemos que el 90 % de los datos en el mundo de hoy se han creado sólo en los últimos dos años[38].

Pensemos los beneficios que obtienen las tecnológicas como Googgle y Facebook en la venta de publicidad, tal y como se manifiesta en el artículo ***"The economic value of personal data for online platforms, firms and consumers"*** [39].

> *"Dado que tales plataformas no cobran a los consumidores por sus servicios de Internet, basan una alta proporción de sus ingresos en la publicidad (lo cual, por supuesto, depende del número de consumidores que atraen). En 2014, 2013*

y 2012, la publicidad representó el 92 por ciento, 89 por ciento y 84 por ciento, respectivamente, de los ingresos de Facebook".

Y recordemos que la capitalización en el 2015 de Facebook ha sido de 271.539 millones de dólares, siendo la séptima compañía mundial en capitalización bursátil.

¿Y en el mercado negro? ¿cuál es el valor de los datos?

En su informe de 2016 "*Underground Hacker Markets*"[40], (también conocido como "*Dark web" o "deep Web*"), la compañía Dell detalla el valor de los datos en el mercado negro, veamos unos ejemplos:

- ✓ *Datos de una tarejeta Visa and MasterCard (U.S.): 7 $.*
- ✓ *Datos de una tarejeta Visa Classic and MasterCard (U.S.) con Track 1 and Track 2 Data: 15 $*
- ✓ *Datos de una tarejeta Visa Classic and MasterCard Standard (EU) (Track 1 and 2 Data): 40 $*
- ✓ *Datos de una tarejeta Premium Visa and MasterCard (EU and U.K.) (Track 1 and 2 Data): 50 $ – 60 $.*
- ✓ *Cuentas de correo electrónico (Gmail, Hotmail, Yahoo): 129 $*
- ✓ *Cuentas de correo electrónico corporativas: 500 $ por mailbox*
- ✓ *Dirección IP de un terminal: 90 $.*
- ✓ *Cuentas bancarias con balances entre 70,000 $ y 150,000 $: 6% del balance total.*

6.6 Normas nacionales frente a los efectos discriminatorios del Big Data.

La Federal Trade Commission recomienda a las compañías que usen estrategias de Big Data:

- ✓ *Tener en cuenta si en los paquetes de datos se pierde información de determinada población y si es así habrá que tomar medidas rectificativas.*

- ✓ *Revisar si en los datos o algoritmos hay sesgos ocultos que puedan afectar a una determinada población.*

- ✓ *Recordar que si bien el Big Data realiza correlaciones no significa que estas sean correctas.*

- ✓ *Importante que haya una supervisión "humana" de los algoritmos y resultados sobre todo para ciertos sectores como el crediticio, salud o empleo.*

… y por supuesto además de las consideraciones éticas, la Federal Trade Commission recuerda que hay un cuerpo normativo que cumplir. Desde un punto de vista comparativo, tal y como hemos venido exponiendo a nivel europeo, existen también otra serie de obligaciones legales impuestas por Reglamento (UE) 2016/679, que se basan en los principios de calidad de los datos, derecho de información, consentimiento y ejercicio de derechos, y que como ya hemos adelantado, son de difícil aplicación en el entorno del Big Data, aunque ese es el reto.

Pero es que además de las normas de protección de datos existe una batería de normas nacionales como por ejemplo la Ley General para la Defensa de los Consumidores y Usuarios de 2007, Ley de ordenación, supervisión y solvencia de entidades de crédito de 2014, ley de Contrato de Seguro de 1980, o Ley General de Salud Pública de 2011, entre otras, que sancionan cualquier forma de discriminación como a continuación se detalla:

- Constitución española:

> *"Derechos y libertades*
>
> *Artículo 14*
>
> *Los españoles son iguales ante la ley,* ***sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social".***

"Artículo 35

*1. **Todos los españoles tienen el deber de trabajar y el derecho al trabajo**, a la libre elección de profesión u oficio, a la promoción a través del trabajo y a una remuneración suficiente para satisfacer sus necesidades y las de su familia, **sin que en ningún caso pueda hacerse discriminación por razón de sexo".***

- Ley General para la Defensa de los Consumidores y Usuarios (Real Decreto Legislativo 1/2007):

"Artículo 49. Infracciones en materia de defensa de los consumidores y usuarios.

*k) La negativa a satisfacer las demandas del consumidor o usuario, cualquiera que sea su nacionalidad o lugar de residencia, cuando su satisfacción esté dentro de las disponibilidades del empresario, así como cualquier forma de discriminación con respecto a las referidas demandas**, sin que ello menoscabe la posibilidad de establecer diferencias en las condiciones de acceso directamente justificadas por criterios objetivos".***

*"m) **Las conductas discriminatorias en el acceso a los bienes y la prestación de los servicios, y en especial las previstas como tales en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres".***

- Ley 33/2011, de 4 de octubre, General de Salud Pública:

"Artículo 6. Derecho a la igualdad.

*1. **Todas las personas tienen derecho a que las actuaciones de salud pública** se realicen en condiciones de igualdad **sin que pueda producirse discriminación por razón de nacimiento, origen racial o étnico, sexo, religión, convicción u opinión, edad, discapacidad, orientación o identidad sexual, enfermedad o cualquier otra condición o circunstancia personal o social.***

2. En especial, ***queda prohibida toda discriminación entre mujeres y hombres*** *en las actuaciones de salud pública, de acuerdo con lo establecido por la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, así como por la demás normativa existente en esta materia.*

3. ***La enfermedad no podrá amparar diferencias de trato*** *distintas de las que deriven del propio proceso de tratamiento de la misma, de las limitaciones objetivas que imponga para el ejercicio de determinadas actividades o de las exigidas por razones de salud pública".*

"Artículo 17. Medidas de fomento.

1. ***Las Administraciones públicas apoyarán y colaborarán*** *con las entidades y organizaciones que desarrollen actividades de salud pública, especialmente, en* ***relación con los grupos más desfavorecidos o discriminados en cuestiones de salud pública".***

- Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito:

"Disposición final primera. Modificación de la Ley 24/1988, de 28 de julio, del Mercado de Valores.

(…) La Comisión Nacional del Mercado de Valores podrá requerir a la entidad de contrapartida central la ampliación de la documentación recibida y podrá establecer excepciones o limitaciones a los precios máximos de esos servicios cuando puedan afectar a la solvencia financiera de la entidad de contrapartida central, provocar consecuencias perturbadoras para el desarrollo del mercado de valores o los principios que lo rigen, ***o introducir discriminaciones injustificadas entre los distintos usuarios de los servicios de la entidad".***

- Ley 50/1980, de 8 de octubre, de Contrato de Seguro:

"Disposición adicional cuarta. No discriminación por razón de discapacidad.

No se podrá discriminar a las personas con discapacidad en la contratación de seguros. *En particular, se prohíbe la denegación de acceso a la contratación, el establecimiento de procedimientos de contratación diferentes de los habitualmente utilizados por el asegurador o la imposición de condiciones más onerosas, por razón de discapacidad, salvo que se encuentren fundadas en causas justificadas, proporcionadas y razonables, que se hallen documentadas previa y objetivamente".*

Podemos afirmar que hay una base sólida legal que evita la discriminación que deberá interpretarse y aplicarse en el caso del Big Data.

6.7 Riesgos del Big Data según la Federal Trade Commission

La FTC enumera una serie de riesgos del Big Data[39]:

i) Verse afectado por las predicciones basadas en otros individuos con perfiles similares.

La FTC pone el siguiente ejemplo ilustrativo del Big Data. Entidades financieras que bajan el límite crediticio a una persona porque otros individuos con mal historial han comprado en las mismas tiendas que aquel. Incluso la FTC comenta que una compañía de crédito en concreto le reveló que el riesgo crediticio podía aumentar si había realizado compras con la tarjeta de servicios de consultoría matrimonial o terapias, basándose en la experiencia crediticia de otros clientes.

ii) Crear o reforzar disparidades existentes.

Por ejemplo, cuando el Big Data es utilizado para la personalización de publicidad, normalmente a las personas con menos recursos no les llega publicidad financiera.

iii) Exposición de información sensible.

Por ejemplo un estudio en facebook a través de los likes. Podía determinar en un 88% la orientación sexual de un usuario masculino, en 95% su origen étnico, en un 82% si era cristiano o mulsulmán, y entre un 65% y 75% si bebía alcohol, tomaba drogas o fumaba.

iv) Dirigirse a un público más vulnerable.

EL Big Data proporciona información sobre perfiles de usuarios que son más propensos al juego, a las compras compulsivas o que simplemente carecen de un juicio mínimo para interpretar ofertas online.

v) Crear nuevas justificaciones para realizar exclusiones.

Por ejemplo, un análisis de Big Data concluyó que aquellos que completaban formularios de empleo desde navegadores que no estaban instalados por defecto (como Firefox o Google Chrome) eran mejores trabajadores y cambiaban menos de trabajo.

vi) Precios más caros para población con menos recursos.

No aprovechándose de las ventajas de la competencia online y offline, ya que en ciertas comunidades con menos recursos hay menos tiendas de calle que puedan competir con las tiendas online.

vii) Debilita la efectividad de las opciones de privacidad de los usuarios.

Incluso cuando las compañías ofrezcan a los usuarios la posibilidad de no autorizar la captación de datos o hacerlo de manera limitada, el uso del Big Data sirve para crear perfiles precisamente de aquellos que se opusieron a determinados tratamientos.

En definitiva uno de los usos del Big Data por ejemplo en el sistema financiero o de seguros es el de minimizar los riesgos, y por lo tanto la negación de un crédito lo basarán en causas objetivas o subjetivas derivadas de un estrategia de Big Data, y donde si la decisión final depende de un humano será difícil demostrar que la decisión únicamente se ha tomado como resultado de un cruce de datos.

Es evidente la correlación existente entre Big Data e Inteligencia Artificial, porque ambas se necesitan. La IA se nutre del Big Data para aprender, y el Big Data necesita la IA para extraer nuevas y mejores predicciones.

7. REFLEXIONES SOBRE IA DE LA 38 CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD.

La conferencia internacional de Comisionados de Protección de Datos y Privacidad *("International Conference of Data Protection and Privacy Commissioners"),* se remonta a 1979, momento desde el cual las principales autoridades de control de protección de datos personales de los estados crean un foro para debatir cuestiones de actualidad e interés que afectan a la privacidad.

El pasado octubre de 2016 la conferencia debatió en Marrakesh cuestiones relativas a la Inteligencia Artificial[40], cuyas conclusiones de sumo interés se irán esbozando a lo largo de las siguientes páginas.

Un primer problema que apunta la Conferencia Internacional es la FALTA DE TRANSPARENCIA por parte de las empresas en el uso de algoritmos de IA con la idea de proteger sus secretos industriales, también es cierto que la lógica utilizada por un algoritmo basado en el aprendizaje de las máquinas *("machined learning")* no puede ser expresado en términos humanos.

Otro tema importante que plantea la Conferencia Internacional es que no se puede obviar que los sesgos introducidos inicialmente para entrenar la IA influirán lógicamente en las predicciones finales, un dato que ya adelantaba la Federal Trade Commission cuando alertaba sobre los riesgos del Big Data.

Y en la Conferencia Internacional, también se advierte a las autoridades de control de protección de datos, que cuando se analice un proceso de IA o un algoritmo no se

busque en el algoritmo en sí, si no que se analice el mismo proceso de alimentación de los datos y sus sesgos, teniendo incluso, las mismas autoridades de control, que crear algoritmos para analizar a aquellos.

Cuestiones planteadas en la conferencia.

- ✓ *¿Cómo pueden las autoridades de control supervisar apropiadamente a una organización que usa Big Data, inteligencia artificial y aprendizaje automático?*

- ✓ *¿Deberían las autoridades de control crear su propio grupo de expertos en Inteligencia Artificial?*

No es mala idea, esta última sugerencia para las autoridades de control teniendo en cuenta que el impacto de la IA sobre la privacidad será contundente, y este es el momento de crear departamentos especializados dentro de las autoridades de protección de datos, pero no sólo para que puedan desarrollar eficazmente sus funciones de control, si no para poder *dialogar* con todas las partes implicadas en la evolución de la misma IA.

En la Conferencia Internacional se abordan los siguientes temas:

i) ***Reconocimiento de imagen. (****Image recognition).*

El reconocimiento de los objetos que componen una imagen ha sido un reto de la ingeniería informática, no sólo se trata de reconocer los elementos que componen una imagen o secuencia si no de reconocer a las propias personas que aparecen a través de un reconocimiento facial. Tales técnicas están basadas en el un modelo inspirado en la operatividad del cortex cerebral con la visión también llamado *"Convolutional Neural Networks" (*CNN).

Este tipo de algoritmos se nutren de la cantidad de información que hay en la red de imágenes etiquetadas (*"tagged images"*). Se crea una gran base de datos y como la cara, al igual que nuestras huellas dactilares, no cambian apenas con el paso del tiempo, se

pueden crear asociaciones midiendo las proporciones de nuestra cara, como la distancia entre los ojos o el tamaño de la barbilla.

Teniendo en cuenta que las imagen de la cara, al igual que los huellas dactilares, son datos biométricos considerados de carácter personal, la conferencia internacional de Comisionados de Protección de Datos y Privacidad plantea la siguientes cuestiones que trataré de responder:

- ✓ *¿Cuál debe ser la política de uso de la información pública basada en fotos etiquetadas para el entrenamiento del machine learning para el reconocimiento facial?*

Actualmente no existe ninguna restricción expresa para tal asunto, pero desde un punto de vista estricto y sin ir más lejos, nuestra propia normativa prohíbe, en principio, la generación de ficheros de datos personales sin el consentimiento de su titular. En cualquier caso me parece improbable que en los sistemas de entrenamiento de *machine learning* se tengan en cuenta tales consideraciones.

- ✓ *¿Cómo supervisar el uso de reconocimiento facial para motivos de seguridad o inteligencia?*

Otro tema que resulta difícil de creer es que los gobiernos renuncien a las posibilidades del reconocimiento facial, pero no es óbice para que haya un control judicial.

ii) ***Procesamiento de lenguaje natural. (****pln) natural language processing (nlp).*

Wikipedia lo define como:

> *"El procesamiento de lenguajes naturales —abreviado PLN, o NLP del idioma inglés Natural Language Processing— es un campo de las ciencias de la computación, inteligencia artificial y lingüística que estudia las interacciones entre las computadoras y el lenguaje humano. El PLN se ocupa de la formulación e investigación de mecanismos eficaces computacionalmente para la comunicación entre personas y máquinas por medio de lenguajes naturales. El*

PLN no trata de la comunicación por medio de lenguajes naturales de una forma abstracta, sino de diseñar mecanismos para comunicarse que sean eficaces computacionalmente —que se puedan realizar por medio de programas que ejecuten o simulen la comunicación—. Los modelos aplicados se enfocan no solo a la comprensión del lenguaje de por sí, sino a aspectos generales cognitivos humanos y a la organización de la memoria. El lenguaje natural sirve solo de medio para estudiar estos fenómenos. Hasta la década de 1980, la mayoría de los sistemas de PLN se basaban en un complejo conjunto de reglas diseñadas a mano. A partir de finales de 1980, sin embargo, hubo una revolución en PLN con la introducción de algoritmos de aprendizaje automático para el procesamiento del lenguaje".

Remontémonos a 1950, cuando Alan Touring propuso su famoso Test por el cual se reconocería la inteligencia de una máquina si las respuestas de ésta no pudieran diferenciarse de las de un ser humano. Existen actualmente distintas aplicaciones de procesamiento de lenguaje natural, como asistentes personales (Google Now, Apple Siri or Microsoft Cortana), o traductores (Google Translate or Bing Translator) que como no, están aprovechando la cantidad de información que hay en la red y la capacidad de procesamiento.

Por ejemplo Google no utiliza ningún traductor o lingüista en su traductor, si no que se basa en el Big Data, buceando en toda la información que hay en la red en forma de textos, y de esta forma a través de algoritmos se crean correlaciones que le permiten ir perfecccionándose, todo lo contrario que lo que hizo en su momento Microsoft con su traductor fracasado al intentar enseñarle al programa las reglas gramaticales de todos los idiomas.

¿Qué capacidades tiene el procesamiento de lenguaje natural?

Desde la traducción, respuestas a preguntas, y extracción de información como por ejemplo el sistema informático de inteligencia artificial Watson ideado por IBM.

Independientemente de las implicaciones que el procesamiento de lenguaje natural pueda tener en la protección de datos personales, las autoridades de control ven este tipo de tecnología como un aliado en sus cometidos de supervisión.

iii) Máquinas autónomas o robots (*Autonomous machines).*

O robots, son aquellas máquinas que realizan tareas de una forma autónoma. En el informe de la 38 conferencia internacional de comisionados, se considera que una máquina es autónoma si:

- *Percibe y reacciona en un entorno.*
- *Planifica y realiza tareas programadas.*
- *Opera sin intervención humana.*

Existe también la posibilidad que las máquinas autónomas aprendan de su propia experiencia a través de la reprogramación.

Actualmente ya hay algoritmos que envían y aceptan ofertas, y toman decisiones fundamentales en el sector financiero. En Wikipedia por ejemplo, y en lo que respecta a los sistema automáticos en el comercio ("*Automated Trading System"*) o (ATS) se dice:

> *"A partir de 2014, más del 75 % de las acciones negociadas en las bolsas de Estados Unidos (incluyendo la Bolsa de Nueva York y NASDAQ) se originan de las órdenes del sistema de comercio automatizado. Los ATS pueden ser diseñados para negociar acciones, opciones, futuros y productos de divisas basados en un conjunto predefinido de reglas que determinan cuándo ingresar una orden, cuándo salir de una posición y cuánto dinero invertir en cada producto comercial. Las estrategias de negociación difieren; Algunos están diseñados para recoger los tops y fondos del mercado, otros para seguir una tendencia y otros implican estrategias complejas, incluyendo ordenar al azar las órdenes para hacerlas menos visibles en el mercado".*

Cathy O'Neil, ex profesora del *Barnard College* de la Universidad de Columbia, en EE.UU, quien trabajó como analista de datos en Wall Street, acaba de publicar su libro, ***"Weapons of Math Destruction"*** *(*"armas de destrucción matemática") que en una entrevista para *BBC.com* [40] afirmó:

> *"Cada vez en mayor medida,* ***las decisiones*** *que afectan nuestras vidas -a qué escuela ir, si podemos o no obtener un préstamo o cuánto pagamos por nuestro seguro sanitario-* ***no están tomadas por humanos, sino pormodelos matemáticos****".*
>
> *(Algunos algoritmos) son opacos: la gente no comprende cómo funcionan. Y, a veces, son secretos.*

En un reciente artículo del New York Times[41] ***"The Robots Are Coming for Wall Street"*** se anuncia que cientos analistas financieros de Wall Street están siendo sustituidos por algoritmos, o el artículo ***"Algorithms Take Control of Wall Street"*** [42] escrito en 2010 por Felix Salmon and Jon Stokes en Wired Magazine, donde se anticipaba la toma de control de Wall Street por dichos algoritmos.

La conferencia internacional de Comisionados de Protección de Datos y Privacidad abre un interesante debate a través de una serie de cuestiones que *intentaré* igualmente responder:

- ✓ *¿ Responsabilidad tanto civil como penal por las acciones de la IA?*

La casuística puede ser amplísima y no puede reducirse a los marcos actuales de responsabilidad.

- ✓ *¿Cómo podría aplicarse el marco de protección de datos / privacidad para las decisiones automatizadas de las máquinas autónomas?*

Es probable que el actual marco de protección de datos no sirva para las máquinas autónomas como veremos más adelante.

- ✓ *¿Quién es el responsable del tratamiento (Data controller) para una máquina autónoma con capacidades de autoaprendizaje?*

Quizás este es uno de los problemas, utilizar conceptos desfasados para entender la complejidad de las máquinas autónomas, quizás ya no tenga sentido hablar del responsable del tratamiento cuando los datos no estén centralizados por una organización y sean de libre acceso, como por ejemplo los que hay en la Red y se utilizan por las propias máquinas autónomas para incrementar su capacidad de autoaprendizaje.

- ✓ *¿Debe la comunidad de protección de datos / privacidad traducir el marco legal en una ley legible por la máquina?*

Sin duda, pero no sólo se trata de traducirlo si no reinventarlo.

iv) Vehículos autónomos.

Otro ejemplo clarificador de la idea de máquinas autónomas, y también interesante desde el punto de vista ético, y que ha abierto un debate, es la decisión que tiene que tomar un sistema autónomo, entre preservar la vida del ocupante de su vehículo, o el de una tercera persona implicada en un accidente.

En cualquier caso son evidentes las ventajas de una conducción autónoma, como la descongestión de las ciudades y reducción de accidentes.

Desde el punto de vista de protección de datos, sin embargo este modelo confrontaría con el sistema normativo actual porque los vehículos deberían estar interconectados entre sí partiendo de la geolocalización de los mismos.

- ✓ *¿Cómo regular las máquinas de autoaprendizaje (incluyendo vehículos autónomos) que procesan enormes cantidades de datos de geolocalización?*

En realidad es un problema con las normas actuales, porque para que el sistema, por ejemplo, de vehículos autónomos sea eficaz, todos los vehículos deben estar interconectados mediante sus datos de geolocalización.

- ✓ *¿Cuál será el impacto de los nuevos modelos de negocios en las relaciones entre el responsable de los datos y el procesador de datos?*

Es indudable que existirán nuevos modelos de negocio, pero más allá del simple concepto responsable/procesador de datos.

v) **Sistemas semiautónomos de aviones no tripulados.** *(Semiautonomous unmanned aircraft systems).*

Unmanned aircraft systems (UAS) o también conocidos como Drones.

No solamente son de aplicación en el campo militar sino que van integrándose cada vez más en toda la sociedad, tanto para controlar infraestructuras, prestar servicios de vigilancia o simplemente como un hobby para otros, en cualquier caso, se basa igualmente en el procesamiento y captación de datos personales y ello tiene implicaciones, bien porque los Drones vayan equipados con sistema de IA o porque captan datos que son posteriormente procesados por estos sistemas.

- ✓ *¿Cuáles son los puntos más apremiantes con respecto a los Drones desde el punto de vista de protección de datos y privacidad?*

A día de hoy, la invasión del espacio público grabando datos personales (caras, matrículas…).

- ✓ *¿Cómo controlar eficazmente estas máquinas de vigilancia de vuelo?*

Salvo restricciones de vuelo en espacios determinados, únicamente existe la posibilidad que en la grabación se cree un sistema de privacidad en el diseño basado en la pixelación de caras u otros datos personales, pero esto es prácticamente imposible porque ni hay intención por parte de la industria, ni los usuarios ven necesaria esta medida, como vemos actualmente con todo el video que se sube a las redes sociales.

- ✓ *¿Deben tener las autoridades de control su propia flota de Drones para la vigilancia de otros Drones? Drones anti Drones*

No es descabellada la idea, pero más sencillo sería si nuestra propia IA nos protegiera.

¿Qué hacer por lo tanto con las normas actuales?

Parece que llegados a estos niveles de sofisticación tecnológica, conviene recordar de dónde venimos, y aferrarnos a principios clásicos o universales como modelo, por eso en las conclusiones de la Conferencia Internacional en ningún momento se duda del potencial de esta nueva tecnología pero se invoca la CUESTIÓN ÉTICA, LA DIGNIDAD Y LOS DERECHOS INDIVIDUALES.

Recordemos, la dignidad como elemento fundamental de la Declaración Universal de los Derechos Humanos que sirve de partida fundacional para otros derechos como el de privacidad y de datos personales. Una violación de la dignidad, como se apunta en la Conferencia Internacional, puede suponer la *"cosificación"* de una persona al servicio de un tercero, y esto no es casualidad en un mundo donde *"el producto es el consumidor"*.

Declaración Universal de Derechos Humanos. Dic 1948.

> *Preámbulo:*
>
> *Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana (…)*
>
> *Artículo 1:*
>
> *Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros.*

El uso de la IA para predecir comportamientos de las personas es un riesgo no sólo para la dignidad como acabamos de comentar, si no que como expone la Conferencia Internacional:

- ✓ *Estigmatiza;*
- ✓ *Crea estereotiopos y exclusión en determinados colectivos;*

- ✓ *Menoscaba la libertad de elección y oportunidades, y si además se monitoriza el seguimiento de las personas se atenta contra el alma de la sociedad que según mi criterio es la libertad.*

La Conferencia Internacional alerta sobre la necesidad de tener en cuenta esta serie de amenazas e invita a abordarlo antes que la IA esté masivamente implantada. Para ello se necesitan ideas innovadoras, y cómo no, aprovecharse de las posibilidades que brinda la propia IA para mantener intacta la libertad de las personas.

La solución tiene que venir fruto de un trabajo interdisciplinar, que agrupe a la parte del negocio como ejecutivos, con desarrolladores, ingenieros, expertos en privacidad, tanto del ámbito privado como público o académico, y sin olvidar a sociólogos, psicólogos o psquiatras, ya que se trata de un cambio de paradigma que afecta estructuralmente a todo nuestro ámbito sociocultural.

Existen iniciativas como el IPEN – (*"Internet Privacy Engineering Network"),* una iniciativa del Supervisor Europeo de Protección de Datos que como explican en su web site:

> *"La iniciativa IPEN fue fundada en 2014. Apoya la creación de grupos de ingenieros que trabajan en bloques de construcción (re) -utilizables, patrones de diseño y otras herramientas para casos seleccionados de uso de Internet donde la privacidad está en juego.*
>
> *IPEN invita a participantes de diferentes áreas como autoridades de protección de datos, academia, desarrollo de código abierto y negocios, y otras personas que están comprometidas a encontrar soluciones de ingeniería para los desafíos de privacidad.* ***El objetivo del trabajo debería ser integrar la protección de datos y la privacidad en todas las fases del proceso de desarrollo, desde la fase de requisitos hasta la producción, ya que es más apropiado para el modelo de desarrollo y el entorno de aplicación.***

Apoya la creación de redes entre grupos de ingenieros y las iniciativas existentes para la privacidad de la ingeniería en Internet. Esta red facilita el intercambio con el fin de coordinar el trabajo y evitar la duplicación, además de discutir qué casos de uso orientados a la privacidad deben ser abordados con prioridad".

Son de agradecer este tipo de iniciativas, más teniendo en cuenta si se trata de aunar a los ingenieros para dar con ideas técnicas, sin embargo tal y como hemos estado viendo a lo largo de estas páginas la normas actuales, como el nuevo Reglamento Europeo de protección de datos, no sirven para regular todo lo que se viene encima con el Big Data, porque simplemente las supera, sin embargo esto no quiere decir que se tenga que renunciar a nuestros principios básicos como son la dignidad y la defensa de los derechos individuales, que en ningún caso deberán ser superados bajo ninguna excusa o tecnología, por muy sofisticada que ésta sea.

8. PRINCIPIOS ÉTICOS DE LA INTELIGENCIA ARTIFICIAL.

A continuación examinaremos el borrador de proyecto[44] con recomendaciones a la Comisión de normas de derecho civil sobre robótica (2015/2103) (inl), Comité de Asuntos Legales. Ponente Mady Delvaux. iniciativa del art. 46 del Reglamento del Parlamento Europeo (8ª legislatura - septiembre 2016), el cual nos sirve de referencia para intuir las advertencias del impacto de la IA sobre la privacidad.

La base jurídica de la redacción de este proyecto es el Reglamento interno del Parlamento Europeo:

Título ii: de la legislación, presupuesto y otros procedimientos.

Capítulo 1: de los procedimientos legislativos - disposiciones generales.

Artículo 46 : Iniciativa de conformidad con el artículo 225 del Tratado de Funcionamiento de la Unión Europea

1. El Parlamento podrá solicitar a la Comisión que le presente, para la adopción de actos nuevos o la modificación de actos existentes, las propuestas oportunas, de conformidad con el artículo 225 del Tratado de Funcionamiento de la Unión Europea, mediante resolución basada en un informe de propia iniciativa de la comisión competente, elaborado de conformidad con el artículo

52. La resolución deberá ser aprobada por mayoría de los diputados que integran el Parlamento en la votación final. Al mismo tiempo, el Parlamento podrá fijar un plazo para la presentación de la propuesta.

Como adelanta el borrador de proyecto, la robótica ha tenido un crecimiento muy importante en los últimos años destacando el crecimiento de las ventas en 2014 de un 29%, principalmente en la industria electrónica y de automoción, sin perder de vista la cantidad de patentes solicitadas por la industria robótica que se ha triplicado en la última década.

La complejidad de los robots autónomos cuestiona los principios de responsabilidad, planteándose la posibilidad de otorgar algún tipo de estatuto legal a los mismos, ¿personas naturales?, ¿capacidad legal?, ¿animales?, ¿objetos? o ¿una nueva categoría?, bajo las actuales reglas de responsabilidad hoy día se atribuye la responsabilidad a una persona, ya sea el dueño del robot, su fabricante o cualquier tercero que se haya visto envuelto en el desarrollo de la acción u omisión del daño producido, sin embargo todo esto se complica cuando es el propio robot quien toma las decisiones, negociando y formalizando contratos por su cuenta, recordemos su uso en el sistema financiero.
También es cierto, que bajo la actual normativa el robot no es un sujeto de derecho y por lo tanto cualquier acto negocial deberá ir finalmente refrendado por una persona.

El informe alerta que si bien a la responsabilidad contractual se le aplicaría la directiva 85/374/EEC de 25 de julio de 1985, sólo es efectiva para los daños producidos por robots derivados de defectos de fabricación, “responsabilidad objetiva o sin culpa”, pero que no serviría para la responsabilidad por hechos derivados de las decisiones tomadas por el propio robot.

El informe propone la siguiente definición de robots autónomos:

- *Adquiere autonomía a través de sensores y / o intercambiando datos con su entorno (Conectividad), comercia y analiza datos.*
- *Autoaprendizaje. (Criterio opcional).*
- *Tiene soporte físico.*
- *Adapta su comportamiento al entorno.*

Propone además que exista un registro de robots para aquellos que sea necesario. Este tipo de iniciativas, recuerda, deben desarrollarse en la actual fase de investigación antes que lleguen al mercado teniendo en cuenta la alta inversión con fondos públicos de le robótica.

Partamos desde el inicio, desde la base de nuestra filosofía moral, y la propia idea de ética aristotélica. Como decía Ortega y Gasset, *"la ética es el arte de elegir la mejor conducta* [45] *"*.

Existe en España un foro creado por académicos de distintas universidades, instituciones privadas y públicas que a través de su web site www.bioéticaweb.com debaten sobre la bioética y donde se definen los conceptos[46] de" *principio de autonomía"*, *"principio de beneficiencia"*, *y "principio de no malificiencia"*, creados por la bioética norteamericana junto el *"principio de justicia"*. Creo que es importante empezar a relacionar la Inteligencia Artificial con cuestiones de bioética, con la pretensión de desarrollar un debate lo más amplio posible sobre la idea misma de llegar a concebir la Inteligencia Artificial como una forma de vida, y lo que esto supondría.

Pero antes veamos el propio concepto de Bioética que según la "Encyclopedia of Bioethics" (New York, 1978) la define como:

> *" el estudio sistemático de la conducta humana en el ámbito de las ciencias de la vida y del cuidado de la salud, examinada a la luz de los valores y de los principios"* .

Bioética[47] (según www.bioéticaweb.com) es *aquella parte de la Ética o filosofía moral que estudia la licitud de las intervenciones sobre la vida del hombre y de su entorno, especialmente, pero no sólo, en el campo de la Medicina y de las ciencias biológicas.*

El borrador de proyecto propone, además, la creación de una agencia europea, con su propio presupuesto que aborde a través de comisiones interdisciplinares, todas estas cuestiones incluyendo el aspecto ético. Inteligencia artificial y aprendizaje autónomo (machine learning) es la parte de la IA donde más se está actualmente investigando, entiendo el aprendizaje autónomo como la habilidad computacional para aprender sin estar expresamente programado.

Como adelanta el informe, con recomendaciones a la comisión de normas de derecho civil sobre robótica (2015/2103)), la robótica sacude principios universales y fundamentales del ser humano, como su dignidad, seguridad, libertad y propiedad, y por eso propone un código de conducta en su anexo, destacando que la guía ética debe basarse en los principios de ***autonomía, beneficiencia,* y *no malificiencia***.

8.1 Principio de autonomía:

Según los filósofos Tom L. Beauchamp[48] y James F. Childress[49]

Autonomía personal:

> *"Regulación personal de uno mismo, libre, sin interferencias externas que puedan controlar, y sin limitaciones personales que impidan hacer una elección. Una persona actúa libremente de acuerdo con un plan elegido."*

Acciones autónomas:

> *"Las acciones autónomas se analizan en función de sus agentes, los cuales actuarán: a) intencionadamente; b) con conocimiento; y c) con ausencia de influencias externas que pretendan controlar y determinar el acto."*

Principio de respeto a la autonomía:

"Ser autónomo no es lo mismo que ser respetado como agente autónomo. Respetar a un agente autónomo implica, como mínimo, asumir su derecho a tener opiniones propias, a elegir y a realizar acciones basadas tanto en sus valores como en sus creencias personales. Este respeto debe ser activo, y no simplemente una actitud. Implica no sólo la obligación de no intervenir en los asuntos de otras personas, sino también la de asegurar las condiciones necesarias para que su elección sea autónoma."

"El principio de respeto a la autonomía se puede formular negativamente: las acciones autónomas no deben ser controladas ni limitadas por otros. Este principio plantea una obligación amplia y abstracta que no permite cláusulas de excepción, como por ejemplo "debemos respetar los puntos de vista y derechos del resto de las personas, siempre que sus ideas y acciones no supongan un grave perjuicio para otros." […] Podemos ahora considerar las exigencias afirmativas del principio, concretamente la obligación positiva de ser respetuoso ofreciendo información y favoreciendo la toma de decisiones autónomas. (…) Muchos actos autónomos no serían posibles sin la cooperación activa de otros que permita que las opciones sean viables. Respetar la autonomía obliga los profesionales a informar, a buscar y asegurar la comprensión y la voluntariedad y a fomentar la toma de decisiones adecuada."

Según el psiquiatra Diego Gracia[50]

Autonomía:

"Por autonomía se entiende en bioética la capacidad de realizar actos con conocimiento de causa y sin coacción."

Según el filósofo H. Tristram Engelhardt [51]

Principio de autonomía como principio de permiso:

"El principio de permiso fundamenta la moralidad del respeto mutuo, ya que exige que sólo se utilice a otras personas si éstas dan previamente su

consentimiento (…) El principio de permiso muestra que no se debe utilizar a los pacientes como simples medios para un fin."

8.2 Principio de beneficiencia [52]:

Según los folósofos Tom L. Beauchamp y James F. Childress:

> *"El principio de beneficencia se refiere a la obligación moral de actuar en beneficio de otros. Muchos actos de beneficencia son obligatorios, pero un principio de beneficencia, tal y como nosotros lo entendemos, impone una obligación de ayudar a otros a promover sus importantes y legítimos intereses."*

Según el psiquiatra Diego Gracia:

Beneficencia no paternalista:

> *"Una beneficencia no paternalista es aquella que intenta hacer el bien o ayudar a los demás en sus necesidades, siempre que ellos voluntariamente lo pidan o lo acepten. Por tanto, en las personas adultas y responsables este principio nunca permite hacer el bien o ayudar sin el "consentimiento informado".*

Beneficencia y autonomía:

> *"El principio de beneficencia es inseparable del de autonomía. […] Lo beneficioso lo es siempre para mí y en esta situación concreta, razón, por la cual es incomprensible separado de la autonomía. No se puede hacer el bien a otro en contra de su voluntad, aunque sí estamos obligados a no hacerle mal."*

Según el filósofo H. Tristram Engelhardt:

"El principio de beneficencia es el que pretende hacer, producir, o realizar el bien. Como tal, la beneficencia es el principio cardinal de las éticas teleológicas y consecuencialistas, siendo destinado a asegurar la realización del bien, así como el equilibrio positivo de los beneficios sobre los perjuicios".

"Se debería formular el principio de beneficencia en los siguientes términos positivos: haz el bien a los demás. Sin embargo, en la medida en que se intenta hacer a los demás lo que ellos consideran que sería su bien –y no lo que nosotros mismos o nuestra comunidad moral consideramos que es su bien– el sentido de la obligación se debilita."

8.3 Principio de no maleficiencia:

Su formulación clásica, **primum non nocere**[53], ha sido traducida como «*en primer lugar, no hacer daño*», y un ejemplo es el juramento hipocrático.

En conclusión se propone la adopción de principios éticos que sirvan de base para regular la IA, aunque también podían haberse basado en las tres leyes de la robótica de Asimov, pero sin embargo la tecnología de guerra actual, a través por ejemplo de Drones, no se para en cuestiones éticas, y viendo la escalada mundial por dotarse de sistemas inteligentes para la guerra no parece vayan a tenerse en cuenta, salvo que como siempre, suceda una catástrofe.

9. PROPUESTA DE INCIATIVAS LEGALES.

Trataremos de responder a las propuestas que se plantean en el borrador de proyecto:

- Establecer un sistema obligatorio de seguros para todos aquellos que tengan robots.

Parece lógico, teniendo en cuenta que actualmente es obligatorio para todos les vehículos. Pero hay que considerar que la idea misma de propiedad también sufra un proceso de cambio, porque en muchos casos la posesión de IA no será material ni exclusiva, pero en cualquier caso si es importante que exista un sistema de seguros que cubran los posibles daños de un sistema de IA. Pensemos que el concepto de propiedad actual de muchos bienes se va diluyendo, por ejemplo, no compramos música si no que nos suscribimos a servicios de *streaming* como Spotify, no compramos libros si no que adquirimos licencias de uso de libros electrónicos, aumenta la demanda de alquilar

vehículos por horas en grandes ciudades frente a la compra de los mismos, y así sucesivamente con nuevos modelos de negocio.

- Crear un fondo de compensación para cubrir los daños producidos por robots cuando allí donde los seguros habituales no llegan para cubrir.

Consecuencia de la reflexión anterior, aunque supongo que la cobertura podría no ser ilimitada, porque el daño de un sistema de IA global puede ser *infinito*.

- Crear un registro de robots individualizados que sirva para definir el tipo de responsabilidad y su cobertura, dependiendo del tipo o la capacidad autómata.

Lógico, siempre y cuando podamos individualizarlos.

- Crear un nuevo estatus de personas electrónicas dependiendo de la complejidad del robot que debería ser gestionado por la Agencia Europea de Robótica e Inteligencia Artificial.

Aquí se abre un debate apasionante, se habla de *personas electrónicas,* supongo que en un futuro cuando el sistema sea complejo, como el de un ser humano, se planteará si les otorga personalidad jurídica, con derechos sobre la privacidad como un ser humano. Recordemos que la singularidad tecnológica implica que un sistema de IA podrían ser capaz de auto-mejorarse en su programación llegando a diseñar nuevas máquinas más inteligentes que el propio ser humano. Para Ray Kurzweil (director de ingeniería de Google) esto sucederá en el 2045, mientras que para Vernor Vinge (escritor y matemático) será en el 2030*.

Singularidad tecnológica ***https://es.wikipedia.org/wiki/Singularidad_tecnol%C3%B3gica***

- Se debe acceder al código fuente de cualquier robot, como por ejemplo para la investigación de accidentes o cuestiones de responsabilidad

Este último punto es muy sensible por el carácter de secretismo y ventaja competitiva que tiene preservar el código fuente del acceso de terceros, para eso están las leyes de propiedad intelectual a las que las empresas tecnológicas se aferran para mantener conductas monopololísticas (legales), como son por ejemplo las patentes. No es que esté en contra de la propiedad intelectual, ni me considere un activista de la cultura libre, pero me llama la atención que las grandes tecnológicas consideren a la privacidad como *una carga del viejo orden*, y sin embargo se aferran a la propiedad intelectual para consolidar sus posiciones dominantes. El acceso a ese código fuente será también requerido por los propios gobiernos, bajo el principio de seguridad por lo que parece poco probable que las empresas o los gobiernos de estas empresas lo permitan. En cualquier caso este tema promete un apasionado debate.

- Los usuarios de los robots deberían revelar:

El número de robots autónomos que utilizan.
Cuánto le supone en ahorro en cotizaciones a la seguridad social.
Una evaluación de los beneficios que le supone el uso de la IA.

Todo ello con el objeto de completar las cotizaciones de la seguridad social y los ingresos fiscales de los estados, teniendo en cuenta que es probable que haya que financiar una renta básica para muchos ciudadanos que son apartados por la automatización masiva. Quizás este planteamiento de imposición fiscal directa sea fruto de un visión simple de lo que significa la IA, y su presencia en los modelos de negocio que están por venir.

10. CÓDIGO DE CONDUCTA ÉTICA PARA INGENIEROS ROBÓTICOS.

10.1Principios.

La primera llamada que se hace a los ingenieros en robótica (*pag 15*) en el borrador de informe 2015/2103(INL) es que tengan presentes los principios de dignidad, privacidad y seguridad de los seres humanos.

El código es voluntario y los investigadores en robótica deben tener la máxima profesionalidad y ética siguiendo los siguientes principios:

- Beneficiencia: actuando en beneficio de los seres humanos.

- No maleficiencia: no hacer daño a un ser humano.

- Autonomía: Tener capacidad de decisión e información sobre los términos de interacción con un robot.

- Justicia: Distribución de los beneficios de la robótica, y acceso a robots domésticos y relacionados con la salud y cuidado.

- Precaución: anticipando posibles impactos de seguridad.

- Inclusión: transparencia respecto al derecho de acceso de todas las partes interesadas en participar en los procesos de desarrollo.

- Responsabilidad (*Accountability):* efecto en la sociedad y en el ser humano.

- Seguridad: se debe preservar el bien estar humano.

- Reversibilidad: como condición indispensable del control, supone devolver al robot estado anterior de un acto indeseable.

- Privacidad: manteniendo segura la información y evitando el seguimiento de individuos sin su consentimiento.
  Los diseñadores de robótica tienen la responsabilidad de desarrollar procedimientos para otorgar el consentimiento, la confidencialidad, el anonimato.
  Los diseñadores cumplirán con cualquiera que solicita que cualquier dato relacionado sea destruido y eliminado de cualquier conjunto de datos.

- Maximizar los beneficios y minorizar los daños. No deben hacerse pruebas con seres humanos que supongan un riesgo mayor que en su vida cotidiana.

10.2 Observaciones para desarrolladores de IA.

A modo de resumen, y según el borrador de proyecto con recomendaciones a la comisión de normas de derecho civil sobre robótica (2015/2103), estas son las ideas que los desarrolladores deben tener en mente a la hora de programar IA

- ✓ ***"Deben tener en cuenta los principios europeos de dignidad, libertad y justicia durante todo el proceso de desarrollo, incluyendo el derecho de los usuarios de no ser dañados".***

Me parece que es la base correcta para el desarrollo de IA.

- ✓ ***"Se deben diseñar sistemas fiables desde el punto de vista de seguridad".***

Indudablemente para garantizar la dignidad y libertad de las personas.

- ✓ ***"Se deben introducir sistemas de privacidad en el diseño".***

El sistema de IA se basa en muchas ocasiones en el Big Data, y como ya hemos visto esto es incompatible con el sistema actual de privacidad.

- ✓ ***"Se debe introducir mecanismos fiables de opt-out".***

Es difícil salirse de un sistema que puede ser incontrolable, el sistema de opt-out puede servir para casos puntuales.

- ✓ ***"Debe asegurarse que un rotot actúa conforme a las normas locales, nacionales o internacionales".***

En principio esa es la lógica para cualquier sistema autómata, sin embargo este principio debería empezar aplicándose en los propios seres humanos y en especial en la política internacional.

- ✓ ***"Debe asegurarse que la decisión del robot es susceptible de reconstrucción y trazabilidad".***

Es conveniente reforzar la capacidad de control sobre los mismos.

- ✓ ***"Debe asegurarse máxima transparencia en el diseño de la IA".***

De dudosa aplicación por el secretismo imperante, tanto por razones de seguridad como comerciales.

- ✓ ***"Debe crearse un protocolo de evaluación de riesgos con todas las partes implicadas incluyendo los usuarios".***

Imprescindible, aunque puede ser en muchos casos impredecible.

- ✓ ***"Debe asegurarse que los robots son identificados como robots cuando interactúan con humanos".***

Necesario, por salud mental.

- ✓ ***"Se debe salvaguardar la seguridad y salud de quienes interactúan con los robots".***

La seguridad será otro elemento fundamental.

- ✓ ***"Deberá tenerse la aprobación del Comité Ético de Desarrollo antes de probar un robot".***

Lo importante será ver el contenido del código ético, aunque sí parece conveniente un control previo.

11. IDEAS BÁSICAS PARA UN MODELO DE PRIVACIDAD EN LA IA.

A continuación expongo una serie de ideas, de las que parto, para tratar de entender el alcance de la privacidad en el IA.

i) Principios universales.
ii) Repensar el propio concepto de privacidad.

11.1 Principios universales:

Debemos partir de una de una serie de principios irrenunciables que deberán estar por encima de cualquier interés o ventaja económica:

1- DIGNIDAD.

Entendida como que las personas no sean *"cosificadas"*, es decir entendidas como cosas, que se traducen en simples datos que les condiciona su vida.

2- LIBERTAD.

Para poder elegir, evitando los oligopolios.
Para poder desconectarse.

3- CONTROL.

Sobre la IA, y que garanticen la igualdad de oportunidades.

4- SEGURIDAD.

Física y económica de las personas.

11.2 Repensar el propio concepto de privacidad.

El profesor de **Alan Westin's**[54], pionero y precursor de los movimientos sociales a favor de la privacidad, definía como privacidad:

> *"El alegato de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida la información sobre ellos se comunica a otros".*

Irwin Altman profesor de Sicología social en la Universidad de Utha, Estados Unidos, desarrolló en 1975 lo que se conoce como ***"Teoría de la regulación de la privacidad"*** *("Privacy regulation theory")*[55] entendiendo la privacidad como *un "proceso de límites interpersonales" mediante el cual los individuos se vuelven más o menos accesibles y se abren a los demás en función de mecanismos de comportamiento".*

Definición de privacidad, desde el punto de vista de Psicología, es en definitiva *la forma que tenemos de relacionarnos con nuestros semejantes,* como así se recoge en los manuales académicos de los departamentos de Psicología[56].

En tales textos académicos, siguiendo el modelo de privacidad de Altman, se establecen cuatro tipos de mecanismos que permiten la consecución de privacidad:

a) *Verbales (la pronunciación, entonación, ritmo o latencia sirven para expresar discrepancias entre la privacidad real y la deseada).*
b) *No verbales, (la postura del cuerpo, la expresión facial o el contacto visual como formas de comunicar inclusión, exclusión, acercamiento o evitación de otras personas).*
c) *Ambientales, (vestimenta y adornos, el espacio personal o distancia interpersonal mantenida durante la interacción, así como elementos espaciales relacionados con la demarcación y defensa de un determinado entorno, manifestaciones en definitiva de territorialidad.*
d) *Socioculturales, (normas sociales y modos culturalmente aprendidos y aceptados de regular la interacción con los demás).*

Por ejemplo, si estamos manteniendo una conversación íntima en un lugar público, alcanzamos el nivel deseado de privacidad confiando en mecanismos como hablar en voz baja para evitar intrusiones, y aquí la relevancia de su modelo de privacidad porque destierra la idea que la privacidad se circunscribe al ámbito de lo privado. De forma natural, su teoría concebida en un mundo analógico podría estar más presente que nunca en el actual mundo digital y sus redes sociales, de ahí la idea también remarcada por Ira S. Rubinstein & Nathaniel Good [57], sobre la privacidad:

> *" Privacidad es un proceso de regulación de los límites por los cuales la gente se hace más o menos accesible y abierta a los demás".*

Para Helen Nissenbaum[58], su teoría de la privacidad se limita a la "**integridad contextual·** *("integrity contextual"),* basándose en la observancia de normas según el contexto, como podría ser un contexto familiar, profesional, amistad, entre otros, donde cada uno de ellos se regula por sus propias normas de carácter formal o informal.

O como en 1890, los juristas estadounidenses **Samuel D. Warren** y **Louis Brandeis** en su libro*"The Right to Privacy"* lo definieron como el derecho de estar solo, *("Right to be let alone").*

Actualmente impera en el mundo tecnológico una idea preconcebida, y es que la privacidad es cosa del pasado, como dijo Mark Zuckerberg *"la privacidad ya no será una norma social"* [59]. La verdad que no tiene mucha credibilidad si tales afirmaciones provienen de compañías donde la materia prima de su negocio es el dato, y cuantas menos restricciones mejor, y sin embargo, nunca se les oye decir que la propiedad intelectual está muerta o que es cosa del pasado. En cualquier caso esto no implica que no haya que repensar la idea de privacidad, quizás cambiando *"el derecho de estar solo"* de Samuel D. Warren y Louis Brandeis, por el *"derecho a que me dejen en paz"*, es decir la capacidad de un usuario a no ser obligado, socialmente o a través de una norma, de adoptar determinadas tecnologías.

Y por otra parte dado que el dato es un gran activo económico deberían ser sus titulares los primeros beneficiados por el tratamiento de los mismos por parte de terceros. Cabe

destacar un estudio[60] , realizado en el año 2012 por la **Agencia Europea de Seguridad de la Información ("ENISA")**, sobre el impacto económico de la privacidad.

El estudio se basó en un experimento de laboratorio que se complementó con un experimento híbrido y de campo con más de 2.300 participantes y 139 transacciones, donde los usuarios deberían realizar una serie de compras online sobre un mismo producto, pero los precios variaban en función del volumen de los datos personales aportados y la mayor personalización de los productos.

Destacamos la siguientes conclusiones:

- ✓ **Personalización de productos.**

Cuantos más datos de un comprador se capten más alta es la tasa de personalización para ofrecer productos y servicios a la medida. Sin embargo el estudio recuerda lo siguiente:

"la personalización también conlleva un riesgo de privacidad, es decir, que los datos pueden verse comprometidos una vez revelados a un proveedor de servicios."

- ✓ **Mayor ventaja competitiva con menos captación de datos (*"privacy friendly systems"*).**

Si frente a precios y productos similares con la competencia se captan menos datos personales se produce una ventaja competitiva:

"El experimento de campo confirmó las tendencias observadas en el laboratorio; La única diferencia observada es que en caso de que no hubiera diferencia de precio, los proveedores de servicios respetuosos con la privacidad que solicitaran menos datos personales obtuvieron una mayor cuota de mercado".

"Si hay poca o ninguna diferencia en los precios ofrecidos por los proveedores de servicios sobre los bienes homogéneos, un competidor que tiene un requisito de datos reducido ("privacy friendly") puede obtener una ventaja competitiva siempre y cuando este tipo de diferenciación sea evidente para el consumidor".

"La razón es que los consumidores pueden - al elegir el proveedor de servicios con un menor requerimiento de datos - reducir sus costos de divulgación de datos personales."

- ✓ **El precio es determinante.**

"El experimento de laboratorio también muestra que la mayoría de los consumidores compran a un proveedor más invasor de la privacidad si el proveedor de servicios cobra un precio más bajo."

"La mayoría de los participantes en el estudio expresan su preocupación por la privacidad (sección 6.3.1). Sin embargo, los resultados de los experimentos muestran que cuando existe una diferenciación de precios, los consumidores muestran una tendencia a elegir servicios / bienes más baratos".

Aunque…

"Una proporción no despreciable de los participantes del experimento, sin embargo, optó por pagar una "prima" por la privacidad. Lo hicieron con el fin de evitar la divulgación de más datos personales o porque el proveedor de servicios amigable con la privacidad prometió no utilizar sus datos con fines de marketing".

- ✓ **Transparencia en la información**.

Las conclusiones del estudio concluyen con elemento fundamental como es la transparencia. Idea que viene desarrollándose a través de estas páginas con la idea de la privacidad en el diseño y la usabilidad de las aplicaciones, su sencillez y comprensión.

"El aumento de la transparencia de las prácticas de información de las empresas debe ir acompañado de un aumento de la transparencia de los precios. Los precios deben anunciarse excluyendo los descuentos para los cuales los consumidores sólo son elegibles proporcionando datos personales adicionales. Además, si se utilizan datos

personales para discriminar los precios, se debe informar al consumidor sobre el hecho de que se está produciendo y sobre qué tipo de discriminación se utiliza".

Propuestas:

He aquí por lo tanto una de las claves, la TRANSPARENCIA:

1. Transparencia en el uso de los datos por parte de las tecnológicas:

Si como es visto una solución puede ser que el titular de los datos obtenga un beneficio por el tratamiento de los mismos por parte de terceros, lo primero que debemos es saber exactamente qué es lo que se hace con nuestros datos, es decir que las tecnológicas informen de todos los usos y no sigan bajo un régimen de ocultación, siendo ésta la única alternativa para poder *intentar* ejercer un control sobre los datos y si es posible ejercer derechos como de oposición.

2. Transparencia por parte de los empresas en los precios de los productos y servicios:

Si los datos personales aportados son lo que compensan la reducción del precio o que sean gratuitos. Se debe cuantificar el valor de los datos personales para evaluar si el intercambio comercial de producto o servicio por datos es justo.

3. Transparencia por pate de los gobiernos del uso y límites en el espionaje masivo:

Importante que exista un control judicial efectivo sobre el espionaje y seguimiento de las personas, pero de nada sirve si EEUU no toma esa iniciativa porque son prácticamente sus compañías, a través de las tecnológicas, quien en mayor medida recopila y trata nuestros datos.

12. CONCLUSIONES

Sin duda, introducir la idea de privacidad en el diseño en el nuevo Reglamento Europeo de protección de datos es positivo. No sólo porque confirma el compromiso de la Unión

Europea con la privacidad, si no porque traslada esta idea como una obligación al mismo momento de concepción del software.

El cambio por lo tanto es sustancial y muy significativo, porque no deja ninguna duda de la idea que tiene la Unión Europea sobre la privacidad, entendida como un derecho fundamental recogido en el art 8 de la Carta de Derechos Fundamentales de la Unión Europea, pero como he venido explicando a los largo de estas páginas, esto colisiona directamente con la realidad.

Primero, porque el uso del Big Data es incompatible con el *"principio de minimización de datos",* entendido como la obligación de un responsable de tratamiento de limitar la recopilación de información personal a lo que es directamente relevante y necesario para lograr un propósito específico, conservando los datos sólo durante el tiempo que sea necesario para cumplir con dicho propósito. *La recolección de datos basados en el Big Data, además de captar datos masivos e indiscriminados, no puede informar a los usuarios de la finalidad del tratamiento porque realmente se desconoce qué es lo que se va a extraer de la recolección de datos, es decir, el Big Data es impredecible porque recopila información pero no se sabe para qué, hasta que no se produce un análisis de conclusiones. Si no podemos informar de lo que no sabemos, el consentimiento, otro pilar en la protección de datos de carácter personal es imperfecto, al no ser libre, específico e informado, siendo por lo tanto inválido.*

En definitiva, un principio de información en un mundo de Big Data donde no se sabe para qué se capta el dato, porque las predicciones se realizan *a posteriori*; un principio de consentimiento que si no está basado en la información es incompleto y por lo tanto inválido; un principio de acceso donde la diseminación de la información es imprevisible; y un principio de seguridad en amenaza constante.

Y como se está comprobando, ni los gobiernos ni las compañías van a renunciar al uso del Big Data.

Segundo, es necesario desarrollar un modelo práctico de privacidad en el diseño, basado en el *"Privacy & Securicy Engineering"*, donde se aporten soluciones técnicas por

equipos técnicos, porque de lo contrario nos encontramos con un modelo teórico sin referencias prácticas para aquellos que vayan a desarrollar la privacidad en el diseño.

Tercero, la privacidad en el diseño en la IA es prácticamente imposible dado que los algoritmos se nutren de Big Data, pero eso no quiere decir que no haya que desarrollar un código ético de obligado cumplimiento junto con un control de los resultados de las predicciones de la IA.

Cuarto, las grandes tecnológicas tratan de eliminar la idea de privacidad en el mundo digital, y en parte lo están consiguiendo teniendo en cuenta que los consumidores prefieren menos precio (o gratis) a cambio de sus datos. Quizás, al igual que la privacidad en el diseño, que se dirige al origen mismo del software, hay que dirigirse a la fuente misma de la educación, y formar a los menores sobre el valor de nuestras libertades, y en concreto sobre la privacidad. Seguramente reformulándola.

Sin embargo soy optimista, y creo que la misma Inteligencia Artificial puede ser la solución, ya que se podrán diseñar sistemas inteligentes que preserven nuestra propia privacidad, pero si queremos que esto suceda, antes tenemos que creer y defender la privacidad, que es lo que nos mantendrá libres.

Eduardo Riestra Herrera.

13. REFERENCIAS

1- United States. Privacy Protection Study Commission. https://epic.org/privacy/ppsc1977report/

2- "Cambridge dictionary". Definición de *product design*. http://dictionary.cambridge.org/dictionary/english/product-design.

3- "Cambridge dictionary". Definición de *fron end y back en design.* http://dictionary.cambridge.org/dictionary/english/back-end.

4- Diccionario de la lengua española. Definición de interface. *Del ingl. interface 'superficie de contacto'. 1. f. Conexión o frontera común entre dos aparatos o sistemas independientes. 2. f. Inform. Conexión, física o lógica, entre una computadora y el usuario, un dispositivo periférico o un enlace de comunicaciones.*

5- Rubinstein Ira y Good Nathaniel." Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents". Ira S. Rubinstein &. New York University School of law. 2012. Pag 1352. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2007&context=btlj

6- Cavoukian Dr. Ann; Information & Privacy Commissioner Ontario, Canada. "Privacy by Design The 7 Foundational Principles". https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf-

7- Google compra la compañía de publicidad 'on line' DoubleClick por más de 2.300 millones de euros. El mundo 14 de julio de 2007. http://www.elmundo.es/mundodinero/2007/04/14/economia/1176509049.html (Accedido en diciembre 2016).

8- Steel Emily y Geoffrey A. Fowler. "Facebook in Privacy Breach. Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds". 2010. http://www.wsj.com/articles/SB10001424052702304772804575558484075236968. (Accedido en diciembre 2016).

9- Delgado Cristina. "EE UU concentra las 10 mayores empresas cotizadas del mundo". El País 2 enero de 2016. http://economia.elpais.com/economia/2016/01/01/actualidad/1451681862_633046.html. (Accedido en diciembre 2016).

10- Rubinstein Ira y Good Nathaniel. "Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents". Ira S. Rubinstein &. New York Berkeley Technology Law Journal. 12 de enero de 2013. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2007&context=btlj

11- Rubinstein Ira. Miembro del Instituto de Derecho de la Información. Universidad de Nueva York. Sus investigaciones incluyen privacidad de Internet, ley de vigilancia electrónica, Big Data, y la privacidad de los votantes. Rubinstein da conferencias y publica ampliamente sobre temas de privacidad y seguridad y ha testificado ante el Congreso sobre estos temas.

12- La Fundación OWASP ("*the OWASP Foundation*") es una organización internacional y comunidad abierta dedicada a capacitar a las organizaciones para concebir, desarrollar, adquirir, operar y mantener aplicaciones seguras. https://www.owasp.org/index.php/Security_by_Design_Principles.

13- "Privacy-enhancing Technologies: the path to anonymity". The Hague, 2000, Revised edition of: Rossum, H. van, e.a. (1995). Privacy-enhancing Technologies: the path to anonymity. Den Haag: Registratiekamer. ISBN 90 346 32 024. https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/av/av11.pdf

14- Enciclopedia Britannica https://global.britannica.com/topic/information-system

15- Angwin Julia and Singer-Vine Selling Jeremy. "You on Facebook". http://www.wsj.com/articles/SB10001424052702303302504577327744009046230 . Wall Street Journal.7 de abril de 2012. (Accedido en diciembre 2016).

16- Human Rights Council creates mandate of Special Rapporteur on the right to privacy – 2015. http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15763&LangID=E

17- https://www.iab.org.

18- Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015. De Maximillian Schrems contra Data Protection Commissioner. Petición de decisión prejudicial por la High Court de Irlanda con objeto de interpretar los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, de los artículos 25, apartado 6, y 28 de la Directiva 95/46/CE, así

como la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000.

19- https://letsencrypt.org/

20- Opinión del Grupo de Trabajo del art 29, 8/2014 sobre el desarrollo de Internet de las cosas. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf . pag 22.

21- Opinión del Grupo de Trabajo del art 29, sobre geolocalización y aparatos inteligentes. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf. pag 13.

22- Yadron Danny. "Facebook, Google and WhatsApp Plan to increase Encryption of User Data" The Guardian. 14 de marzo de 2016. http://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple. (Accedido en diciembre 2016).

23- Charta for Strengthening Confidential Communication. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2015/charta-vertrauenswuerdige-kommunikation.html .

24- Privacy Considerations for Internet Protocols. 2013.Internet Architecture Board (IAB). https://tools.ietf.org/html/rfc6973#ref-PbD. Pags 12, 13 y 14.

25- https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/

26- Definición de "*Machine Learning*". Universidad de Stanford. http://robotics.stanford.edu/~ronnyk/glossary.html

27- Definición de "*Machine Learning*" en wikipedia. (Accedido en diciembre 2016).

28- Big Data. A tool for inclusion or exclusion? Federal Trade Commission 2016. https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

29- http://www.intel.com/content/www/us/en/internet-of things/infographics/guide-to-iot.html

30- Rubinstein. Ira S. Big Data: The End of Privacy or a New Beginning? pag. 3 http://idpl.oxfordjournals.org/content/3/2/74.full.pdf

31- Agencia Española de Protección de Datos. " Procedimientos y garantías en los procesos de anonimización de datos personales"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf 2016

32- Yves-Alexandre de Montjoye, Radaelli Laura, Kumar Singh Vivek, Pentland Alex ."Unique in the shopping mall: On the reidentifiability of credit card metadata". 30 de enero de 2015. http://science.sciencemag.org/content/347/6221/536

33- Sweeney Latanya, Akua Abu, Winn Julia. "Identifying Participants in the Personal Genome Project by Name". Harvard University. 29 de abril de 2013. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257732

34- González Enric. "IBM y el holocausto". Edwin Black. Edit. Atlántida. http://elpais.com/diario/2001/02/13/ultima/982018801_850215.html 13 de febrero de 2001. (Accedido en diciembre 2016).

35- Polonetsky Jules & Tene Omer. https://www.stanfordlawreview.org/online/privacy-and-big-data-privacy-and-big-data/ 2013.

36- Searls (n 54); Ctrl-Shift (n 53); Andrieu (n 55); World Economic Forum (n 56); and Mydex, 'The Case for Personal Information Empowerment: The Rise of the Personal Data Store', September 2010. http://mydex.org/wp-content/uploads/2010/09/The-Case-for-Personal-Information-Empowerment-The-rise-of-the-personaldata-store-A-Mydex-White-paper-September-2010-Final-web.pdf.

37- Muñoz Ramón. "Telefónica quiere que sus clientes cobren a Google y Facebook por usar sus datos". http://economia.elpais.com/economia/2016/09/05/actualidad/1473067092_839315.html. 5 de sept 2016. (Accedido en diciembre 2016).

38- "Bringing big data to the enterprise".IBM. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

39- Liem Cassandra y Petropoulos Georgios. "The economic value of personal data for online platforms, firms and consumers". http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/ 14 de enero de 2016.

40- Thompson Cadie. “Here's how much thieves make by selling your personal data online”. May 27, 2015. http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5
Dell. Secure Works. “Underground Hacker Markets”: http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf

41- Federal Trade Commission 2016. “Big Data. A tool for inclusion or exclusion?” https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

42- Artificial Intelligence, Robotics, Privacy and Data Protection room document for the 38th international conference of Data Protection and Privacy Commissioners. octubre 2016.
https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Intconference

43- http://www.bbc.com/mundo/noticias-37837377

44- Popper Nathaniel http://www.nytimes.com/2016/02/28/magazine/the-robots-are-coming-for-wall-street.html?_r=0 FEB. 25, 2016. (Accedido en diciembre 2016).

45- Salmon Felix y Stokes Jon. https://www.wired.com/2010/12/ff_ai_flashtrading/. (Accedido en diciembre 2016).

46- Proyecto de informe con recomendaciones a la comisión de normas de derecho civil sobre robótica. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN

47- Ortega y Gasset: Origen y epílogo de la filosofía, 1943. Obras Completas, IX, página 349.

48- Principio de autonomia y beneficiencia. Dos principios en tensión . Publicado en la Universitat Ramon LLull, Càtedra Ethos.
http://www.bioeticaweb.com/autonomasa-y-beneficiencia-dos-principios-en-tensiasn/

49- Definicion de Bioética.
http://www.bioeticawiki.com/Que_es_la_Bio%C3%A9tica_(definici%C3%B3n)

50- Beauchamp Tom L. (n. Austin, 1939) es un filósofo estadounidense especializado en la filosofía moral, la bioética y la ética animal. Es profesor de Filosofía en la Universidad de Georgetown, y es el investigador principal en el

Instituto de Ética de la Universidad Kennedy. https://es.wikipedia.org/wiki/Tom_Beauchamp.

51- Childress James Franklin. También conocido como J. F. Childress, (n. 4 de octubre de 1940) es un filósofo y teólogo estadounidense, que se ha ocupado principalmente de la ética, en especial de la bioética médica. Es profesor de ética en la cátedra John Allen Hollingsworth del Departamento de Estudios Religiosos en la Universidad de Virginia. Además, es profesor de Educación Médica en dicha universidad, donde también dirige el Instituto de Ética Práctica. Ha obtenido un B.A. del Guilford College, un título de Grado de la Yale Divinity School, una maestría y un doctorado de la Universidad de Yale. https://es.wikipedia.org/wiki/James_Franklin_Childress.

52- Gracia Guillén, Diego. (1941) es un médico, escritor y filósofo español, especialista en Psicología y Psiquiatría, que ha trabajado como investigador para el CSIC, y al que se considera uno de los grandes expertos españoles en bioética. https://es.wikipedia.org/wiki/Diego_Gracia_Guill%C3%A9n

53- Tristram Engelhardt jr. Hugo (1941) es un filósofo estadounidense, que obtuvo un doctorado en filosofía en la Universidad de Texas (Austin) así como un doctorado en medicina en la Universidad Tulane (en Nueva Orleans). Es profesor de filosofía en la Universidad William Marsh Rice (en Houston), especialidad historia y filosofía de la medicina. https://es.wikipedia.org/wiki/Hugo_Tristram_Engelhardt_jr

54- "Principio de autonomia y beneficiencia. Dos principios en tensión". http://www.bioeticaweb.com/autonomasa-y-beneficiencia-dos-principios-en-tensiasn . Publicado en la Universitat Ramon LLull, Cátedra Ethos.

55- Gracia, D (1990). "*Primum non nocere*. El principio de no-maleficencia como fundamento de la Ética Médica". Madrid: Instituto de España. Real Academia Nacional de Medicina. pp. 25.

56- Singularidad tecnológica. Wikipedia. https://es.wikipedia.org/wiki/Singularidad_tecnol%C3%B3gica. . (Accedido en diciembre 2016).

57- *Westin, Alan (1967). Privacy and Freedom. New York: Atheneum. p. 7.*

58- Altman, I (1975). The environment and social behavior. Monterey, CA: Brooks/Cole.

59- Psicología ambiental. Elementos básicos. Tema 3. Entorno físico e interacción social. Asignatura de psicología ambiental, del segundo ciclo de licenciatura de psicología de la Universidad de Barcelona. http://www.ub.edu/psicologia_ambiental/uni3/index.htm.

60- Rubinstein Ira y Good Nathaniel. "Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents". Ira S. Rubinstein &. New York University School of law. Pag 1369. 2013. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2007&context=btlj

61- Nissenbaum Helen. Profesora de la Universidad de Nueva York, de Media, Culture and Communication y directora del Information Law Institut. Autora de "Privacy in Context, Technology, Policy, and the Integrity of Social Life". 2009. http://www.elmundo.es/mundodinero/2007/04/14/economia/1176509049.html

62- Bobbie Jhonson."Privacy no longer a social norm, says Facebook founder". The Guardian 11 de enero de 2010. https://www.theguardian.com/technology/2010/jan/11/facebook-privacy .

63- ENISA. European Network and Information Security Agency. "Study on monetising privacy. An economic model for pricing personal information". 2012. https://www.enisa.europa.eu/publications/monetising-privacy

14. BIBLIOGRAFÍA

1- Agencia Española de Protección de Datos. 2016. *" Procedimientos y garantías en los procesos de anonimización de datos personales"*.

2- Altman, I. 1975. *"The environment and social behavior"*. Monterey, CA: Brooks/Cole.

3- Angwin Julia and Singer-Vine Selling Jeremy. 7 de abril de 2012. Wall Street Journal. *"You on Facebook"*.

4- Artificial Intelligence, Robotics, Privacy and Data Protection room document for the 38th international conference of Data Protection and Privacy Commissioners. octubre de 2016.

5- Cavoukian Dr. Ann; 2009. *"Privacy by Design The 7 Foundational Principles"*. Information & Privacy Commissioner Ontario, Canada.

6- Charta for Strengthening Confidential Communication. Ministerio Federal del Interior. Alemania. 18 de noviembre de 2015.

7- Delgado Cristina. El País. 2 enero de 2016. *"EE UU concentra las 10 mayores empresas cotizadas del mundo"*.

8- El mundo. 14 de julio de 2007. *"Google compra la compañía de publicidad 'on line' DoubleClick por más de 2.300 millones de euros"*.

9- ENISA. 2012. European Network and Information Security Agency. *"Study on monetising privacy. An economic model for pricing"*

10-Federal Trade Commission. 2016. *"Big Data. A tool for inclusion or exclusion?"*

11- González Enric. *"IBM y el holocausto"*. 2001. Edwin Black. Edit. Atlántida.

13- Gracia, D. 1990. *"Primum non nocere. El principio de no-maleficencia como fundamento de la Ética Médica"*. Madrid: Instituto de España. Real Academia Nacional de Medicina. pp. 25.

14- Grupo de Trabajo del art 29, 8/2014. Opinión sobre el desarrollo de Internet de las cosas (pag 22), y sobre geolocalización y aparatos inteligentes (pag 13).

15- Internet Architecture Board (IAB). Julio de 2013. *"Privacy Considerations for Internet Protocols"*.

16- Liem Cassandra y Petropoulos Georgios. 14 de enero de 2016. *"The economic value of personal data for online platforms, firms and consumers"*.

17- Muñoz Ramón. El país. 5 de sept 2016. *"Telefónica quiere que sus clientes cobren a Google y Facebook por usar sus datos"*.
18- Nissenbaum Helen. 2009. *"Privacy in Context, Technology, Policy, and the Integrity of Social Life"*.
19- Ortega y Gasset: Origen y epílogo de la filosofía, 1943. Obras Completas, IX, página 349.
20- Polonetsky Jules & Tene Omer. 2013. *"Privacy and Big Data"*.
21- Privacy Protection Study Commission. United States.
22- Proyecto de informe con recomendaciones a la comisión de normas de derecho civil sobre robótica. 31 de mayo de 2016. Parlamento Europeo.
23- Rossum, H. van. *"Privacy-enhancing Technologies: the path to anonymity"*. The Hague, 2000, Revised edition. Privacy-enhancing Technologies: the path to anonymity. Den Haag: Registratiekamer. ISBN 90 346 32 024.
24- Rubinstein Ira y Good Nathaniel. 2012.*" Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents"*. Ira S. Rubinstein &. New York University School of law. Pag 1352; "The End of Privacy or a New Beginning?" pag. 3.
25- Searls (n 54); Ctrl-Shift (n 53); Andrieu (n 55); World Economic Forum (n 56); and Mydex, September 2010.*'The Case for Personal Information Empowerment: The Rise of the Personal Data Store'*.
26- Steel Emily y Geoffrey A. Fowler. 2010. *"Facebook in Privacy Breach. Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds"*.
27- Sweeney Latanya, Akua Abu, Winn Julia. 29 de abril de 2013. *"Identifying Participants in the Personal Genome Project by Name"*. Harvard University.
28- Thompson Cadie. May 27, 2015. *"Here's how much thieves make by selling your personal data online"*.
29- Universitat Ramon LLull, Càtedra Ethos. 2008. *"Principio de autonomi¬a y beneficiencia. Dos principios en tensión"*.
30- Valera, Sergi, Pol Enric, Tomeu Vidal. Psicología ambiental. Elementos básicos. Tema 3. Entorno físico e interacción social. Asignatura de psicología ambiental, del segundo ciclo de licenciatura de psicología de la Universidad de Barcelona.
31- Westin, Alan. 1967. Privacy and Freedom. New York: Atheneum. p. 7.

Yadron Danny. 14 de marzo de 2016. The Guardian. *"Facebook, Google and WhatsApp. Plan to increase Encryption of User Data"*.

32- Yves-Alexandre de Montjoye, Radaelli Laura, Kumar Singh Vivek, Pentland Alex . 30 de enero de 2015. *"Unique in the shopping mall: On the reidentifiability of credit card metadata"*.