Responsabilidad proactiva en los tratamientos masivos de datos

Pedro Alberto González
Agencia Vasca de Protección de Datos
paGonzalez@avpd.eus

Accountability in Massive Data Processing

Resumen: El tratamiento masivo de datos está suponiendo ya, hoy en día, un gran valor añadido para las personas, las empresas y la sociedad en su conjunto en áreas tan diversas como el marketing, finanzas, salud o planificación pública. Grandes oportunidades están esperando a ser aprovechadas. Pero cuando se tratan datos personales, es necesario prever los riesgos y actuar dentro de los límites que garanticen los derechos y libertades de las personas. Límites que deben ir más allá de lo estrictamente legal, dibujando un marco ético para el tratamiento masivo de datos personales.

Palabras clave: Privacidad, Protección de Datos, Big Data, Macrodatos, Responsabilidad Proactiva, Ética de los Datos

Abstract: Big data is delivering nowadays a great added value for people, business and society as a whole, in areas as diverse as marketing, finance, and health or public planning. Great opportunities are waiting to be seized. But when dealing with personal data, it is necessary to foresee the risks and act within limits that guarantee the rights and freedoms of individuals. Limits that must go beyond strictly legal issues, setting an ethical framework for big data processing of personal data.

Keywords: Privacy, Data Protection, Big Data, Accountability, Data Ethics

ISSN 1989-7022

DILEMATA año 9 (2017), nº 24, 115-129

*"Iván os ha planteado un enigma —exclamó Rakitine—. Un enigma estúpido, ridículo y necio en el que no hay nada que adivinar: «**Si no hay inmortalidad del alma, no hay virtud, lo que quiere decir que todo está permitido**.» Es una teoría seductora para los bribones. Por lo demás, aunque no crea en la inmortalidad del alma, la humanidad hallará en sí misma el vigor necesario para vivir virtuosamente. Esa fuerza se la proporcionará su amor a la libertad, a la igualdad y a la fraternidad"*

Fiodor Dostoievski,
"Los Hermanos Karamazov"

1. En tierra incógnita

Las grandes conquistas de nuevos territorios siempre han estado precedidas por la oportunidad, los medios y la motivación para emprender su exploración y explotación. Desde las migraciones africanas del paleolítico, pasando por las exploraciones americanas de españoles, portugueses y británicos, hasta llegar a la exploración espacial contemporánea, todas ellas han supuesto grandes oportunidades y han aportado grandes beneficios, pero también han supuesto grandes impactos.

Received: 30/04/2017
Accepted: 15/05/2017

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

Impactos dramáticos en ocasiones, como fue, por ejemplo, la conquista de América en cuanto a sus consecuencias para los pobladores originarios, ya fuesen estas la devastación causada por las enfermedades, el genocidio de los rebeldes o la limpieza étnica de los desplazados. Este es un claro ejemplo de cómo y cuándo la existencia de "grandes oportunidades" ni justifica ni debe dar pie a la conculcación de los derechos de *los otros*.

*Mutatis mutandi*s, la existencia de nuevos servicios, o nuevas formas de prestar los servicios, caracterizados por el registro sistemático de datos que marcan nuestra huella digital en las más diversas dimensiones de nuestra actividad, también supone una "gran oportunidad", no solamente por los datos en sí mismos, sino por las propiedades emergentes que arrojan tales datos cuando son tratados a gran escala. Es lo que viene siendo conocido como "Big Data", "Macrodatos" (a no confundir con los "metadatos") o "tratamientos masivos de datos". Cada día nos vemos sorprendidos con nuevos resultados atribuidos al tratamiento masivo de datos, los cuales estimulan nuevas iniciativas *creativas* de aplicación de tales macrodatos. Pero, no nos engañemos, también en este caso habrá damnificados por los efectos colaterales, cuando no por causa directa, de tales tratamientos masivos de datos, cuando se trate de datos de carácter personal. Y esto es algo que no debemos permitirnos.

Aplicando la terminología del mundo de la gestión de riesgos, puede afirmarse que el tratamiento masivo de datos personales tiene, por su propia naturaleza y según la forma en que se lleve a cabo, un *impacto* sobre los derechos de las personas afectadas y puede suponer un *riesgo* para las mismas, en el caso de que dicho tratamiento masivo de datos no cuente con *medidas* adecuadas para evitar o mitigar dichos riesgos. Tales medidas, dicho de una forma muy general, pueden pertenecer a diferentes categorías, como por ejemplo el establecimiento de límites legales, directrices organizativas o condiciones técnicas. Estas medidas suponen una delimitación, más o menos clara, de lo que se *puede* y lo que no se puede hacer. Pero, además, resulta necesario establecer también un *marco ético* de referencia respecto del tratamiento masivo de datos personales, que llegue *un poco más allá* de donde lleguen las medidas legales, organizativas y técnicas, estableciendo unos límites adicionales sobre los que *se debe* o no se debe hacer.

Por lo tanto, nos encontramos ante el escenario, por otra parte habitual, de necesidad de ponderación entre los beneficios conseguidos y los riesgos que supone la aplicación de los tratamientos masivos de datos.

ISSN 1989-7022

DILEMATA, *año 9 (2017), nº 24, 115-129*

2. La búsqueda del equilibrio

Es claro que el juicio de ponderación entre los beneficios y los riesgos que suponen los tratamientos masivos de datos ha de hacerse, en primer lugar, desde el punto de vista de cómo afecte a los derechos y libertades de las personas, ya sea individualmente consideradas, en cuanto que afectados por el hecho de que su información forme parte del conjunto de datos tratados, o bien porque, como ciudadanos, formen parte del colectivo de personas que, de una u otra manera, se vean afectadas por las consecuencias de los resultados obtenidos del tratamiento "Big Data". Y el marco adecuado para ello no es otro que la legislación sobre protección de datos personales. En función de este marco legal habrá que adecuar los tratamientos masivos de datos.

Sin embargo, no todos los actores que intervienen comparten este principio. Por ejemplo, uno de los documentos elaborados durante la administración Obama analizando el fenómeno Big Data, "*Big Data: seizing opportunities, preserving values*" (2014) [1] decía, en la primera de sus conclusiones:

> *"Las tecnologías de Big Data están impulsando una enorme innovación al tiempo que aumentan las nuevas implicaciones de privacidad que se extienden mucho más allá del enfoque actual en la publicidad online. Estas implicaciones hacen urgente un examen nacional más amplio del futuro de la protección de privacidad, (…). Será especialmente importante* ***reexaminar el marco tradicional de información y consentimiento****, que se enfoca en la obtención del permiso del usuario antes de recoger los datos. Si bien la información y el consentimiento siguen siendo fundamentales en muchos contextos, ahora es necesario examinar si un mayor enfoque en cómo se usan y reutilizan los datos* ***sería una base más productiva*** *para administrar los derechos de privacidad en un entorno de Big Data (…).* ***La protección de la privacidad también debe evolucionar de una manera que dé cabida al bien social que puede venir del uso de Big Data****."*

Es decir, se promovía el cambio del marco normativo (en este caso, el de los EEUU) para que se acomodase a las necesidades de los tratamientos masivos de datos.

Afortunadamente, a las pocas semanas el Grupo del Artículo 29[2] hizo público su posición ("*Declaración del WP29 sobre el impacto de Big Data sobre la protección*

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 115-129

de las personas", 2014)[3] que, si bien no citaba expresamente al documento anterior, fijaba una posición firme ante la pretensión de revisar el principio de consentimiento:

> *"Algunas partes interesadas afirman que la aplicación de algunos principios y obligaciones de protección de datos en virtud de la legislación de la UE debe revisarse sustancialmente para permitir que se produzcan avances prometedores en las operaciones de Big Data"*
>
> *"Sin embargo, en este momento no tiene ninguna razón para creer que los principios de la UE en materia de protección de datos (...) ya no son válidos y adecuados para el desarrollo de grandes datos (...)*
>
> *"También debe quedar claro que las reglas y principios son aplicables a* ***todas las operaciones de procesamiento, comenzando con la recolección*** *para garantizar un alto nivel de protección de datos".*

Y ¿cuáles son estos principios de la protección de datos que con tanta firmeza se defendieron?

En el tiempo transcurrido desde 2014, la unión europea procedió, efectivamente, a revisar su legislación, culminando un largo proceso que había dado comienzo en 2012 y concluido en la primavera de 2016, con la aprobación del *Reglamento General de Protección de Datos* de la UE[4] (RGPD - REGLAMENTO (UE) 2016/679). Y si bien el RGPD introdujo algunos elementos verdaderamente novedosos, los principios esenciales se mantuvieron, en líneas generales.

3. Comencemos por los principios

La protección de datos personales persigue, como objetivo general, garantizar los derechos y libertades de las personas y, en particular, el respeto de la vida privada y familiar, de las comunicaciones, la libertad de pensamiento, de expresión y de información, y la diversidad cultural, religiosa y lingüística. Para ello, la protección de datos personales se ha dotado de unos principios, consagrados en el RGPD, que son los siguientes:

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

- Exactitud y vigencia
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

De estos, destacaremos aquellos que tienen una especial incidencia en el caso de los tratamientos masivos de datos.

El primero de los principios, ***licitud***, establece que el tratamiento de los datos sólo será legítimo si éste se efectúa en virtud de determinados supuestos como son, en primer lugar, el *consentimiento* del interesado. Por supuesto que hay otros supuestos, como es la existencia de un contrato que implica la necesidad del tratamiento, cuando se trata de dar cumplimiento a *obligaciones legales* aplicables al responsable del tratamiento, o en el ejercicio de intereses o *poderes públicos* conferidos al citado responsable. También cuando se trate de preservar *intereses vitales* del interesado, pero tal supuesto tiene un carácter de urgencia y excepcionalidad. En estos grupos de supuestos no hay ninguna tensión respecto de la licitud del tratamiento.

Existe otro supuesto que abre una puerta cuyos límites no está siempre claro si se deben traspasar, y este es el supuesto de la existencia de un "*interés legítimo*" perseguido por quien pretenda tratar datos personales o, incluso, de un tercero. Este supuesto del interés legítimo constituye un concepto jurídico indeterminado que, en cualquier caso, debe interpretarse siempre de forma restrictiva y nunca constituir una "habilitación genérica" para justificar cualquier tratamiento. De las diferentes casuísticas que pueden presentarse se ha ocupado el Grupo de Artículo 29 en su "*Dictamen 6/2014*[5]*, sobre el concepto de interés legítimo del responsable del tratamiento*", cuya lectura complementaria puede resultar de sumo interés.

También son relevantes los principios de *lealtad* y *transparencia*, pero sobre ellos volveremos más adelante.

El segundo principio relevante es el de la ***limitación de la finalidad***, el cual está relacionado con las causas que, en origen, hayan legitimado el tratamiento. Es decir, los tratamientos de datos deberán tener unos fines *determinados, explícitos y legítimos*, y no deberán tratarse ulteriormente con otros fines, a excepción de determinadas finalidades declaradas compatibles, como son su archivo en interés público, la investigación científica e histórica o finalidades estadísticas. También,

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 115-129

en este caso, el ya citado Grupo del Artículo 29 elaboró un dictamen, la "*Opinion 3/2013*[6] *on purpose limitation*", en el que analiza profusamente las circunstancias en las que la reutilización `puede ser considerada, o no, compatible.

Un tercer bloque lo constituyen los principios de ***minimización*** de datos y de ***limitación del plazo*** de conservación, es decir, los datos tratados habrán de ser los adecuados, pertinentes y limitados a lo estrictamente necesario para la finalidad legitimada, incluida la limitación del plazo de conservación al tiempo estrictamente necesario para su tratamiento. También aquí, respecto del plazo de conservación, se reconocen las mismas excepciones anteriormente apuntadas como compatibles.

Finalmente y sin perjuicio de los demás principios, destacamos el principio de "***responsabilidad proactiva***", que es la trasposición elegida para el término anglosajón de *accountability*. Genéricamente, este principio se enuncia como la asunción de la responsabilidad, por parte quien trate datos personales, de *dar cumplimiento* a los principios anteriormente citados, así como de ser *capaz de demostrarlo*. Pero este principio tiene una concreción y un desarrollo en los cuales nos extenderemos un poco más adelante.

No haremos un especial análisis de los restantes principios, como son en de *exactitud y vigencia*, o el de *integridad y confidencialidad*, y no porque sean menos importantes, sino porque, de cara a la incidencia que el tratamiento masivo de datos tiene sobre ellos no presenta tantas aristas como los restantes.

A la vista de esto, ¿cuál es el resultado de la confrontación de los tratamientos masivos de datos frente a los principios de la protección de datos enumerados? Pues bien, podemos adelantar que no se trata de una convivencia pacífica.

4. Impacto de los tratamientos masivos de datos

Las Autoridades de Protección de Datos han tenido oportunidad de pronunciarse acerca del impacto que previsiblemente tendrán los tratamientos masivos de datos sobre los principios de la protección de datos. Así, y además de la Declaración del WP29 anteriormente mencionada, el "Grupo de Berlín [7]" elaboró un documento de trabajo, "*Working Paper on Big Data and Privacy - Privacy principles under pressure in the age of Big Data analytics*", el cual dio lugar, posteriormente, a una resolución

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

de la 36 Conferencia Internacional de Autoridades de Protección de Datos[8], celebrada en 2014 en Mauritius.

También el Supervisor Europeo de Protección de Datos[9] ha analizado las implicaciones del tratamiento masivo de datos personales en varios dictámenes, desde 2014 hasta el presente[10]

Sin necesidad de analizar individualmente cada uno de los documentos, podemos sintetizar las conclusiones de los diferentes análisis efectuados, los cuales identifican claramente los siguientes puntos de confrontación:

Legitimidad de la reutilización: Una de las características de algunos tratamientos masivos de datos consiste, precisamente, en la reutilización de datos que inicialmente habían sido recogidos para otra finalidad, o bien con una legitimación diferente. Pensemos en los casos en que se tratan datos personales que son necesarios para la ejecución de un contrato, en sentido estricto, y luego son reutilizados por el responsable de tratamiento para otros fines como, por ejemplo, en el caso de los pagos efectuados mediante tarjeta de crédito. En el caso de que el emisor de la tarjeta considerase efectuar un tratamiento adicional para, digamos, ofrecer a sus clientes sus propios productos financieros, puede entenderse que se trata de una finalidad conexa y compatible con la original. Sin embargo, una reutilización consistente en cruzar la información detallada de las compras efectuadas, con el fin de elaborar perfiles de consumo para luego ser ofertados a terceros resulta ajena a la relación contractual inicial. Esto constituye una desviación de la finalidad, para la cual se necesitaría una nueva legitimación en base al consentimiento.

En ocasiones, los tratamientos masivos de datos personales argumentan que su finalidad es la "investigación" o el mero "análisis estadístico". Hay que añadir que cuando la legislación sobre protección de datos contempla excepciones a la limitación de finalidad, como en el archivo, la investigación científica e histórica o finalidades estadísticas, tales finalidades deben ser establecidas "oficialmente" y en interés público, de acuerdo con las previsiones de cada estado miembro de la UE. Es decir, no basta una declaración de parte de que el tratamiento pertenece a tales categorías.

Incluso en estos casos, en el análisis efectuado por el Grupo del Artículo 29 se introduce el concepto de "separación funcional", que implica que cuando se haga

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

un tratamiento de datos con fines de investigación científica, histórica o estadística, deben de adoptarse medidas que garanticen dicha separación funcional, de forma que los datos de los sujetos afectados no deben estar disponibles para cualesquiera medidas o decisiones de apoyo que se tomen en su procesamiento. Es decir, hace necesario el uso de una disociación irreversible (anonimización), disociación reversible (pseudonimización) o el manejo de datos agregados. Aun así, estas medidas tienen otros efectos colaterales que veremos más adelante.

También interviene aquí el principio de *lealtad*, puesto que los interesados han facilitado sus datos en base a unas determinadas expectativas que no pueden verse defraudadas ni excedidas unilateralmente. El concepto de "expectativas razonables de privacidad" por parte de las personas afectadas debe respetarse siempre

Tratamiento excesivo de datos: Los tratamientos masivos de datos suelen incluir datos adicionales, ya sea como metadatos básicos, como pueden ser la localización temporal (fechas, horas) o espacial (geolocalización) o como otros atributos obtenidos del contexto en que se generaron los datos. Su conservación durante largos periodos de tiempo forma parte de la propia concepción del tratamiento masivo de datos, a la espera de la oportunidad de una potencial explotación ulterior, y de hecho la acumulación de datos está llegando a constituir un valor intrínseco. Esto excede el principio de limitación del plazo de conservación, según el cual los datos debieran cancelarse una vez que dejasen de ser necesarios para la finalidad que justificó su recogida.

Falta de transparencia: Gran parte de los datos recolectados para su tratamiento masivo son recogidos como consecuencia de la actividad ordinaria de los usuarios, aunque sin su participación consciente. Pensemos, por ejemplo, en los datos derivados de las búsquedas que lanzamos en los motores de búsqueda y nuestro historial de navegación a través de las páginas de internet, que luego sirven para alimentar la publicidad comportamental que se nos dirige. Con la generalización del uso de los dispositivos móviles de comunicación, la geolocalización se añade como metadato prácticamente en cualquier circunstancia.

Muchos de los datos que son tratados proceden de *sensores*, es decir, dispositivos que captan información de su entorno, como ocurre, por ejemplo, en la "Internet de las cosas" (IoT, Internet of Things) y que, en definitiva, no es más que un universo

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

de *aparatos identificables intercomunicados*. En su origen, estos sensores tenían una utilidad circunscrita a los entornos industriales y, como tales, no contenían información que pudiera considerarse "datos de carácter personal". Pero una vez que tales sensores aparecen vinculados a una persona, o pueden llegar a vincularse mediante datos adicionales, se constituyen en *monitores del comportamiento* y adquieren la consideración de *dato personal*.

Todos esto contextos tienen en común que la recogida de datos se efectúan de forma inadvertida o al menos poco transparente para el interesado, sin que éste sea informado no ya solo del hecho de su recopilación, sino de la finalidad de su tratamiento posterior, los derechos que le asisten al respecto, o las consecuencias que pudieran llegar a afectarle derivadas de tal tratamiento.

Difícil gestión del consentimiento: como consecuencia del hecho de que muchos tratamientos masivos de datos personales están basados en la reutilización, la cual necesitaría en muchos casos de un nuevo consentimiento, o bien en datos recogidos de forma poco transparente, aun cuando el interesado pueda ser consciente de que su actividad está generando datos, que son capturados, se haría necesario contar con el consentimiento del interesado. Pero, dadas las circunstancias en las que se produce la recopilación, resulta difícil gestionar el consentimiento, tanto en la información previa que debe ofrecerse como en la propia materialización de la "clara acción positiva" que exige el RGPD.

5. Efectos colaterales de los tratamientos masivos de datos

Además de los impactos sobre los principios de la protección de datos que se han enumerado, existen otras características intrínsecas al tipo de tratamientos efectuados con datos masivos que también les hacen suponer un riesgo para la protección de datos de los afectados, como son:

Reidentificación: A pesar de que entre las medidas recomendadas para el tratamiento masivo de datos es aplicar técnicas de disociación apropiadas, tales datos ya anonimizados pueden ser susceptibles de reidentificación. No estamos hablando, en este caso, de reidentificaciones casuales, debidas a errores o falta de calidad en los métodos de disociación empleados, sino del hecho de que se

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 115-129

ha demostrando que, aplicando técnicas, ingenio y esfuerzos adecuados muchos procesos de disociación `pueden llegar a revertirse.

Consecuencias discriminatorias: La finalidad de la mayor parte de los tratamientos masivos de datos persigue la búsqueda de patrones, tendencias o perfiles que permiten sacar conclusiones y tomas decisiones en consecuencia. En ocasiones, estas consecuencias afectan directamente a los individuos que han aportado la información y, si ésta contuviese cualquier inexactitud, puede acarrear consecuencias negativas para los afectados, por el hecho de ser signados a perfiles sobre los cuales se tomarán decisiones automáticamente. Pero también pueden llegar a afectar a individuos que ni siquiera han participado en la aportación de datos, por el hecho de pertenecer a colectivos extrapolados a partir de los patrones o perfiles obtenidos. Pensemos en los residentes en un barrio o zona residencial que sobre la que se han obtenido cualquier tipo de perfil en base a la geolocalización de otros afectados y que se verán afectados por estereotipos o prejuicios.

Correlaciones espurias: La propia naturaleza de los análisis masivos de datos introducen sesgos en las conclusiones debido a la confusión que induce en los conceptos de "correlación" y de "causalidad": Debido al enorme número de datos analizados, pueden aparecer determinadas correlaciones espurias, es decir hechos o comportamientos que, aparentemente, están relacionados, cuando de hecho no existe ninguna causalidad entre ellos y únicamente se trata de una correlación casual, sin ninguna causa subyacente. Los algoritmos utilizados en el análisis masivo de datos no son neutrales y pueden ser la causa de las consecuencias discriminatorias antes apuntadas.

6. Medidas correctoras y recomendaciones

Los anteriormente citados documentos y recomendaciones de las Autoridades de Protección de Datos coincidían tanto en el diagnóstico como en los tratamientos más eficaces para lograr un balance entre los riesgos que pudiera suponer el tratamiento masivo de datos, con el respeto a los derechos y libertades de las personas. En particular, se identificaba la necesidad de

- Respetar el principio de "limitación de finalidad"
- Limitarla cantidad de datos recopilada según el "principio de minimización"

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

- Obtener, siempre que sea posible, un consentimiento válido y de calidad
- Ser transparente respecto de:
  - Qué datos se recogen
  - Cómo serán tratados
  - Para qué finalidad serán usados y
  - Si serán cedidos a terceras partes
- Facilitar información sobre los criterios/algoritmos usados para establecer sus perfiles

Además de estas recomendaciones generales, también se identificaba la necesidad de reforzar el marco legal de protección de datos, si bien no en el sentido apuntado por el informe de la Casa Blanca de 2014 ("*…evolucionar para dar cabida al uso del Big Data…*"), sino para reforzar las garantías para las personas interesadas. Ello ha tenido su concreción en el *Reglamento General de Protección de Datos* de la UE.

El RGPD recoge el principio general, ya apuntado, de "*responsabilidad proactiva*", el cual sirve de paraguas para un conjunto de medidas que, aplicadas en su conjunto, contribuirán a mitigar los impactos identificados.

7. El papel decisivo de la responsabilidad proactiva

La responsabilidad proactiva, además del principio de "cumplir y demostrar que se cumple", engloba a varias medidas específicamente previstas en el RGPD, como son:

Evaluación de Impacto: El RGPD establece la necesidad de efectuar una evaluación de impacto sobre la protección de datos con carácter previo al inicio del tratamiento cuando se traten datos personales utilizando nuevas tecnologías que, por su naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas, como ocurre cuando se efectúa una evaluación sistemática y exhaustiva de aspectos personales de personas físicas, en base a en un tratamiento automatizado, como ocurre con la elaboración de perfiles, con todas las consecuencias antes apuntadas. Lo mismo ocurre cuando se tratan *a gran escala*, categorías especiales de datos, como son los datos de salud, o se produce una observación sistemática *a gran escala* de una zona de acceso público. El término "*gran escala*" puede tener unos límites de aplicación quizás difusos para otros tratamientos, pero forma parte intrínseca de los tratamientos masivos que aquí estamos considerando.

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 115-129

El RGPD establece el contenido básico de una evaluación en los siguientes detalles:

- una *descripción* sistemática de las operaciones de tratamiento previstas, así como de los fines del tratamiento, estableciendo el interés legítimo perseguido por el responsable del tratamiento;
- una evaluación de la *necesidad y la proporcionalidad* de las operaciones de tratamiento con respecto a su finalidad;
- una *evaluación de los riesgos* para los derechos y libertades de los interesados, y
- las *medidas* previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

La realización de evaluaciones de impacto implica una cierta metodología y sistematización a la hora de abordarlas. Diferentes Autoridades de Protección de Datos han adoptado sus propias aproximaciones y el concepto se ha consolidado hasta el punto de existir un estándar, actualmente en fase de desarrollo, sobre la realización de tales evaluaciones, ISO/IEC 29134 ("Guidelines for privacy impact assessment")[11].

Privacidad desde el diseño y por defecto: Frente a un planteamiento tradicionalmente reactivo frente a las implicaciones de la protección de datos en los tratamientos, el RGPD propugna la adopción de un enfoque proactivo y preventivo, de forma que la concepción de las implicaciones y consecuencias se tengan en cuenta desde el primer momento del ciclo de vida del tratamiento. Si bien el concepto de "privacidad desde el diseño" tuvo en sus primeros momentos una aproximación quizás un poco vaga y voluntarista, con el tiempo ha tenido una concreción en una serie de principios comúnmente admitidos, como son:

1. Diseño Proactivo, no Reactivo; Preventivo, no Correctivo
2. La Privacidad, como configuración por defecto del tratamiento
3. La Privacidad incrustada en el diseño del tratamiento
4. Funcionalidad total: "Suma-Positiva", no "Suma-Zero"
5. Seguridad en todo el ciclo de vida del tratamiento
6. Visibilidad y transparencia del tratamiento
7. Respeto a la privacidad personal ("tratamiento centrada en el usuario")

Respecto del carácter voluntarista que pudo tener en sus inicios, podemos afirmar que la privacidad desde el diseño está completamente afianzada a partir de su inclusión en el RGPD. Es de esperar que en los próximos tiempos surjan mecanismos de certificación que contribuyan a establecer de una forma más sólida este principio.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129

Anonimización y pseudonimización: Una de las medidas concretas que el RGPD recomienda aplicar, como mitigación de los riesgos de los tratamientos, es la ya antes apuntada de la disociación, ya sea con el fin de reconducir el tratamiento hacia un tratamiento de *datos anonimizados* (mediante una disociación irreversible) o bien aplicar la *pseudonimización* (mediante una disociación reversible). Aún así, habrán de tenerse en cuenta los riesgos ya apuntados de *reidentificación* de los datos personales. El Grupo del Artículo 29 emitió en 2014 unas directrices sobre técnicas de anonimización[12] ("Opinion 05/2014 on Anonymisation Techniques") que pueden resultar de utilidad.

8. Conclusión: hacia una "ética de los datos"

Tal como insinuábamos al comienzo, puede haber quien tenga la tentación de pensar que "***todo nos está permitido***", sin más límites que la mera posibilidad. Es, en efecto una teoría seductora para los bribones, para quienes no existe la virtud.

El uso de tecnologías emergentes, como pueden ser los tratamientos masivos de datos personales, puede suponer un riesgo latente para los derechos y libertades de las personas en su concreta aplicación a, digamos, datos especialmente sensibles como los datos de salud y, más en particular, los datos genéticos. Por su propia naturaleza, estos datos van más allá de los propios individuos, sino también a su grupo familiar, incluso de colectivos más amplios relacionados social, cultural o étnicamente. Por las técnicas necesarias para su procesamiento solo unos pocos y grandes operadores están en condiciones de su tratamiento, lo cual puede generar una concentración de conocimiento y, por tanto, poder, que acentuará el desequilibrio no solo entre estos grandes operadores y los interesados, sino quizás también entre aquellos y la sociedad.

Es importante considerar a los interesados como ***personas***, sujetos de derechos, y no solo como usuarios o consumidores. Las tendencias actuales para favorecer el ***mercado único digital***, pueden conducir a aumentar los riesgos de los tratamientos masivos para las personas, precisamente por el carácter impredecible y disruptivo que tienen las tecnologías emergentes, lo cual hace que las protecciones legales pueden llegar a ser insuficientes si han de enfrentarse a nuevas situaciones y supuestos, para los cuales no estaban diseñadas.

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 115-129

"*La tecnología no debe dictar los valores y los derechos, pero tampoco debe reducirse su relación a una falsa dicotomía*". Por eso es importante, también, introducir un ***enfoque ético***, centrado en los tratamientos basados en tecnologías emergentes, que sitúe la ***dignidad humana*** en el centro de la ecuación. En este sentido, las Autoridades de Protección de datos deben jugar un decisivo papel, como ya ha empezado a hacer el Supervisor Europeo de Protección de Datos, con la adopción, en 2015, del Dictamen[13] "*Hacia una nueva ética digital - Datos, dignidad y tecnología*", en el que indica que "*En el entorno digital actual, no basta con respetar la ley sino que es preciso tener en cuenta la dimensión ética del tratamiento de datos*". Como desarrollo de tal declaración, el EDPD ha constituido[14] en 2016 un "Grupo Consultivo sobre Ética", cuyos resultados habrán de jugar un decisivo papel a medio plazo.

Finalizando con Dostoievski, "***hemos de hallar la fuerza para vivir virtuosamente. Esa fuerza nos la proporcionará el amor a la libertad, la igualdad y la fraternidad***".

Notas

1. https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

2. El conocido como "Grupo del Artículo 29" debe su particular nombre al hecho de ser un órgano consultivo independiente constituido al amparo del artículo 29 de la Directiva 95/46/CE, integrado por las Autoridades de Protección de Datos de los estados miembros de la UE, más el Supervisor Europeo de Protección de datos.
Más información en http://ec.europa.eu/justice/data-protection/index_en.htm

3. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

4. Disponible en https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807

5. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf

6. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

7. El grupo de Berlín es un grupo de trabajo creado en 1983 por la Conferencia Internacional de Autoridades de Protección de Datos, a quien reporta sus documentos de trabajo, con el fin de estudiar las implicaciones de las telecomunicaciones en la esfera privada de las personas.
https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

8. Privacy Conference 2014
http://www.privacyconference2014.org/English/aboutconference/Pages/RESOLUTIONS.aspx

9. EDPS, European Data Protection Supervisor - https://edps.europa.eu/

10. EDPS, 2014 - Preliminary Opinion on Privacy and competitiveness in the age of big data: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf
EDPS Opinion 7/2015, Meeting the Challenges of Big Data: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf
EDPS Opinion 8/2016 , Coherent Enforcement of Fundamental Rights in the Age of Big Data: https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

11. ISO-IEC-29134, https://www.iso.org/standard/62289.html

12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

13. EDPS, Dictamen 4/2015 - Hacia una nueva ética digital - Datos, dignidad y tecnología
https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf

14. EDPS, Decision establishing "the Ethics Advisory Group"
https://edps.europa.eu/sites/edp/files/publication/15-12-03_ethical_dimensions_en.pdf

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 115-129