derecom

ISSN: 1988-2629. Nº. 26. Nueva Época. Marzo 2019-Septiembre 2019

Cómo citar este texto:
Rafael del Real Rubio y María Luisa Sánchez Calero (2019). Las tecnologías cognitivas y el periodismo de datos: su impacto en la privacidad. *Derecom*, 26, 141-154. http://www.derecom.com/derecom/

LAS TECNOLOGÍAS COGNITIVAS Y EL PERIODISMO DE DATOS: SU IMPACTO EN LA PRIVACIDAD

KNOWLEDGE TECHNOLOGIES AND DATA JOURNALISM: THEIR IMPACT ON PRIVACY

©Rafael del Real Rubio
Instituto de Empresa (España)
rdelreal@coit.es

©María Luisa Sánchez Calero
Universidad Complutense de Madrid (España)
mlusaca@ucm.es

Resumen

Inmersos en la era de la información comprobamos como las tecnologías han cambiado nuestras vidas conectados permanentemente a través de todo tipo de dispositivos. Una situación que a diario genera un rastro de datos a nuestro paso creando una huella digital, que sin duda está siendo utilizada por agentes externos para conocer nuestros hábitos y gustos, lo que podría dar lugar a abusos y usos ilícitos de nuestra información.

El objeto de este trabajo es determinar aquellos riesgos legales que en materia de privacidad pueden originar la falta de transparencia en la captación y tratamiento de nuestros datos y cómo el legislador en materia de privacidad ha reaccionado ante dicho fenómeno.

Analizaremos como el Periodismo de Datos, actualmente en auge como consecuencia de la revolución tecnológica en la que estamos inmersos, al utilizar los datos abiertos puestos por el sector público a disposición de ciudadanos y de medios de comunicación, puede originar vulneraciones del derecho a la protección de datos - de carácter personal- como consecuencia de la reutilización de los mismos en la elaboración de noticias.

Siguiendo esta línea, en este trabajo se utilizará una metodología que analizará el Reglamento Europeo de Protección de Datos, lo que pondrá de manifiesto cómo se puede alcanzar el necesario equilibrio entre la innovación tecnológica y el respeto de los valores y derechos fundamentales que rigen nuestra sociedad.

Recibido: 09/12/2018 Revisado: 11/03/2019
Aceptado: 12/03/2019 Publicado: 15/03/2019

Como resultado del análisis, se deducirá la necesidad de potenciar la implantación del denominado "Gobierno de los Datos" como herramienta fundamental para asegurar la calidad, control y explotación de la información de carácter personal de los ciudadanos y como garantía del cumplimiento normativo sobre la materia, por parte de las organizaciones.

Summary

Immersed in the information age as we are, the technology has changed our lives and we are permanently connected through many types of devices. A situation that daily generates a trail of data. This digital fingerprint is undoubtedly being used by external agents to know our habits and choices, which could mean the unfair and illegal use of information about ourselves.

The purpose of this paper is to determine the legal risks that may arise in terms of privacy from the lack of transparency in the collection and processing of our data and how the legislative authority in the matter has reacted to this phenomenon.

We will analyze how Data Journalism, nowadays booming as a result of the technological revolution in which we are involved, by using the open data made available by the public sector to citizens and the media, can cause breaches of the right to protection of data as a result of the reuse of personal data in the preparation of news.

Following this line, through the analysis of the EU General Data Protection Regulation, it will become clear how the necessary balance between technological innovation in the field of Artificial Intelligence and respect for citizens values and rights can be achieved.

As a result of the analysis, the need to enhance the implementation of the so-called "Governance of Data" will be considered as a fundamental tool to ensure the quality, control and exploitation of citizen´s data and as a guarantee of the compliance of law by the organizations.

Palabras clave: Datos. Inteligencia artificial. Protección de datos. Periodismo de datos. RGPD (Reglamento General de Protección de Datos).

Keywords: Data. Artificial intelligence. Privacy. Data Journalism. GDPR (General Data Protection Regulation).

1. Introducción.

Cada vez que voluntariamente instalamos una aplicación, escribimos un tweet o utilizamos Facebook dejamos un rastro digital de nuestros datos y preferencias, pero, en general, no somos conscientes de las consecuencia presentes y futuras de estas acciones.

En una reciente entrevista en el diario *El País*, Jannis Kallinikos[1] afirmaba que *En la mayoría de los casos no conocemos donde acabarán los datos. Los usuarios se juegan más que la privacidad cuando ceden información personal*.

2.Riesgos y amenazas de las tecnologías cognitivas en la privacidad.

Los avances tecnológicos de los últimos años y la disponibilidad de datos personales en la red permiten a tecnologías cognitivas como Big Data e Inteligencia Artificial, hallar correlaciones y crear vínculos entre esos datos y ciertos aspectos de la personalidad, el comportamiento, los intereses o los hábitos de una persona.

La elaboración de perfiles y el tratamiento automatizado de los datos, es decir, sin participación humana, plantea importantes riesgos para los derechos y libertades de las personas, por lo que deviene necesario establecer garantías de protección de los mismos. Además, la existencia de sesgos en los datos o en su tratamiento puede llevar a predicciones inexactas, lo que podría originar la denegación de determinados bienes y servicios, así como generar situaciones de discriminación para determinadas personas o colectivos.

Asimismo, la falta de transparencia en el tratamiento y análisis de los datos que fueron obtenidos para una determinada finalidad, y que son tratados con otros fines incompatibles, supone no solo un riesgo para la protección de la privacidad de las personas, sino también una amenaza para el ejercicio de los derechos y libertades fundamentales de los ciudadanos.

Joseph Weizenbaum,[2] creador de Eliza, el primer Bot conversacional, así como uno de los promotores de la introducción de cuestiones éticas en el desarrollo tecnológico, afirmaba en su libro *Computer Power and Human Reason,* publicado en 1976:

> *Cuando la Inteligencia Artificial sea posible, no deberemos dejarle tomar decisiones importantes porque los ordenadores nunca tendrán cualidades humanas como la compasión y la sabiduría al no haber crecido en el entorno emocional de una familia humana.*

3.La elaboración de perfiles y el tratamiento automatizado de los datos de carácter personal

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 (en adelante RGPD), define la elaboración de perfiles como:[3]

> *Toda forma de tratamiento automatizado de datos personales consistente en utilizarlos 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.*

La elaboración de perfiles puede llevarse a cabo en cualquiera de las fases del ciclo de vida del dato, es decir, en la recogida de los mismos, en su análisis y procesamiento o en su aplicación.

Implica, por lo tanto, la recogida de información sobre una persona (o grupo de personas) y la evaluación de sus características o patrones de comportamiento con el fin de asignarla a una determinada categoría o grupo. A partir de la categorización se elaboran

predicciones sobre capacidades, intereses o comportamientos. Conviene aclarar que la simple clasificación de las personas basada en características conocidas como su edad, sexo y altura no da lugar necesariamente a una elaboración de perfil, ya que depende de la finalidad de la clasificación.

Por su parte, el tratamiento automatizado de los datos se refiere a la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano. Las decisiones automatizadas pueden basarse en: datos obtenidos directamente de los interesados, por ejemplo, mediante cuestionarios; datos observados acerca de las personas como, por ejemplo, la geolocalización mediante aplicaciones y los datos derivados o inferidos de otras fuentes como, por ejemplo, perfiles existentes de la persona.

Las decisiones que cuentan con intervención humana y, por tanto, no están basadas únicamente en el tratamiento automatizado, pueden incluir también la elaboración de perfiles. El RGPD incorpora disposiciones que abordan los riesgos derivados de la elaboración de perfiles y las decisiones automatizadas. Del contenido del artículo 22 del RGPD[4] relativo a "Decisiones individuales automatizadas, incluida la elaboración de perfiles", se deduce que existe una prohibición general sobre los tratamientos automatizados, lo que permite vislumbrar la existencia de riesgos potenciales para los derechos y libertades de las personas.

No obstante, el propio Reglamento establece excepciones, permitiendo a los responsables del tratamiento la elaboración de perfiles y adoptar decisiones automatizadas en los casos de necesidad para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento. Se admite una segunda excepción en el caso de estar autorizada por el Derecho de la Unión o de los Estados miembros cuando se apliquen medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Y por último se permite la excepción en el caso de consentimiento explícito del interesado.

4.Los principios que rigen el tratamiento de datos de carácter personal.

El RGPD enuncia en su artículo[5] los principios inspiradores del tratamiento de los datos, estableciendo que la licitud, la lealtad, la transparencia, la limitación de la finalidad, la minimización de los datos, la exactitud, la limitación del plazo de conservación, la integridad, la confidencialidad y la responsabilidad proactiva deben regir todas las actividades en las que los datos de carácter personal son objeto de tratamiento.

El Grupo de Trabajo del artículo 29 (GT29)[6] ha publicado una serie de directrices dirigidas a los responsables del tratamiento, a fin de que les sirva de guía para asegurar el cumplimiento de las obligaciones que vienen fijadas en el RGPD. Según las citadas directrices, el principio de transparencia en el tratamiento de datos de carácter personal reflejado en el apartado 1a del artículo 5, es de aplicación en tres ámbitos fundamentales: *en el suministro de información a los interesados en relación con el tratamiento equitativo; en la comunicación con los interesados en lo que respecta a sus derechos en virtud del RGPD y en los medios y posibilidades de que los interesados ejerzan sus derechos*.

La utilización de tecnologías cognitivas en la generación de perfiles a partir de datos derivados o inferidos de bases de datos para los que el interesado no ha dado su consentimiento expreso podría suponer una vulneración del principio de transparencia que informa del proceso de aseguramiento del consentimiento. Asimismo, la utilización de esta técnica puede comprometer el principio de lealtad si en la elaboración de perfiles o en la utilización de algoritmos en las decisiones automatizadas se emplean prácticas discriminatorias

que impidan o penalicen a determinadas personas o colectivos el acceso a oportunidades de empleo, a créditos o a la contratación de seguros.

El principio de limitación de la finalidad, del apartado 1b del artículo 5, es infringido cuando se realiza el tratamiento de datos personales que se recogieron originalmente para otra finalidad. El ejemplo más paradigmático es la utilización de los datos de geolocalización que utilizan las aplicaciones y que son tratados para el envío de publicidad, lo que claramente supone una práctica incompatible con la finalidad para la que se obtuvo el consentimiento.

Otra mala praxis muy extendida, es la recogida de una mayor variedad de datos personales de los que realmente se necesitan, cuyo fin es una posible utilización en el futuro. Los algoritmos de aprendizaje automático están diseñados para procesar grandes volúmenes de información y generar correlaciones que permiten a las organizaciones crear perfiles exhaustivos. En este caso la conservación de los datos presenta ventajas para las organizaciones que explotan estas tecnologías, dado que el algoritmo podrá aprender de un mayor número de datos. Los responsables del tratamiento deben garantizar que cumplen el principio de minimización de datos, así como los requisitos de los principios de limitación de la finalidad y limitación del plazo de conservación.

Por otro lado, si los datos utilizados en un proceso de decisión automatizada o de elaboración de perfiles son inexactos, cualquier decisión o perfil resultante podría originar dificultades e inconvenientes a los interesados. Las decisiones pueden tomarse sobre bases de datos desactualizados o sobre la incorrecta interpretación de datos externos. Las inexactitudes pueden provocar predicciones o afirmaciones inadecuadas sobre, por ejemplo, las posibilidades de obtener un crédito.

Especial mención merece el cumplimiento del principio de licitud. El responsable del tratamiento debe garantizar que dispone de una base jurídica para el tratamiento. El artículo 6.1 del RGPD[7] establece de manera tasada cuando un tratamiento es lícito.

En relación con el apartado a) del artículo 6.1, el consentimiento explícito es una de las excepciones de la prohibición sobre la elaboración de perfiles y decisiones automatizadas del artículo 22 del RGPD. En cualquier caso, los interesados deben tener la suficiente información sobre el uso y las consecuencias previstas del tratamiento que se va a efectuar de sus datos de carácter personal.

Por otro lado, el interés legítimo que el responsable de tratamiento puede alegar en el caso de utilizar procesos de elaboración de perfiles y decisiones automatizadas en el ámbito de una relación contractual o precontractual, con base en criterios de mejora de eficiencia o de reducción de riesgos, debe estar suficientemente justificado como para poder encuadrarlo dentro de las condiciones de licitud del apartado b del artículo 6.

La base del tratamiento soportada en las condiciones del cumplimiento bien de una obligación legal o bien de una misión de interés público o en el ejercicio de poderes públicos debe encontrarse establecida por el Derecho de la Unión o por el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

Si el tratamiento es para otro fin distinto de aquel para el que se recogieron los datos personales, el responsable del tratamiento debe analizar la compatibilidad de fines, considerando: la relación entre los fines inicial y ulterior; el contexto en que se hayan recogido

los datos personales; la naturaleza de los datos personales; las posibles consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización. Por lo tanto, el responsable del tratamiento debe realizar un *test de compatibilidad de finalidades* y acreditar que la reutilización de datos se ha realizado para una finalidad compatible.

Conviene recordar que la Ley Orgánica 3/2018, de Protección de Datos, considera como infracción muy grave la utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

Por último, como uno de los principios explícitos que recoge el RGPD nos encontramos *la responsabilidad proactiva* que tiene como elemento clave para su cumplimiento la denominada Evaluación de Impacto en la Protección de Datos (EIPD). Esta herramienta permite al responsable del tratamiento evaluar los riesgos que suponen la adopción de acciones que puedan impactar en la privacidad de las personas y entre las que se encuentra la utilización de tecnologías cognitivas en la elaboración de perfiles y en la toma de decisiones automatizadas.

El RGPD, en su artículo 35, prescribe la obligación de llevar a cabo un EIPD en el caso de realización de una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles. Y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

5.Ejemplo de vulneración de Derechos. El caso Cambridge Analytica

Por su especial interés, se expone en este apartado el caso de Cambridge Analytica, como ejemplo de vulneración de derechos por un uso ilícito de las tecnologías cognitivas. Siguiendo la investigación llevada a cabo por el profesor José Manuel López Zafra, publicada en el diario *El Confidencial*[8], el origen de la cuestión se encuentra en el lanzamiento de la aplicación MyPersonality diseñada para Facebook por Michal Kosinsky y David Stillwell.
La finalidad de los dos creadores del proyecto era obtener información de los rasgos de personalidad de los usuarios de Facebook, basándose en los denominados rasgos *big five* u OCEAN: *Openness* (apertura al cambio); *Conscientiousness* (responsabilidad); *Extraversion* (extraversión, sociabilidad); *Agreeableness* (cordialidad, afabilidad); *Neuroticism* (neurotismo, inestabilidad emocional).

Una vez puesta la aplicación a disposición de los usuarios, y para sorpresa de los dos investigadores, se encontraron con millones de respuestas. En 2012 Kosinski presenta unos sorprendentes resultados de su investigación, afirmando que *con menos de 70 'likes' de Facebook, podía predecir el color de la piel de las personas, su orientación sexual, y, lo que resultará determinante, su sensibilidad política hacia el partido Demócrata o el Republicano*. Con la combinación de *likes* y la encuesta OCEAN, desarrollaron un algoritmo que podía determinar los hábitos de vida, su religión o las tendencias políticas de los participantes.

En 2013 se funda, en Londres, Cambridge Analytics, como extensión de Strategic Communication Laboratories, SCL, y cuyo objeto era el uso de técnicas de las Ciencias de Datos para la comunicación y el análisis electoral. Mejoran sustancialmente las técnicas de

microtargeting que había desarrollado el equipo de Obama cuatro años antes y efectúan alrededor de 250 millones de perfiles de norteamericanos, más que votantes potenciales (unos 231 millones entonces) y casi el doble de los finalmente inscritos (alrededor de 137 millones). De cada perfil, entre 3.000 y 5.000 registros.

Esa es la potencia de la ciencia de datos: convertir esos datos en información, y esa información en conocimiento. El 8 de noviembre de 2016, Donald Trump se convertía en el 45º presidente de los EEUU, contra todos los pronósticos.

Como se puede comprobar, la utilización de estas técnicas ha supuesto un antes y un después en las estrategias electorales y en la ciencia demoscópica en general y su uso de manera ilícita conlleva una flagrante vulneración del derecho fundamental a la protección de datos de carácter personal.

6.Medidas de control en el despliegue de las tecnologías cognitivas

Uno de los principales retos a que la humanidad se va a enfrentar en un futuro próximo es cómo se puede controlar el diseño y desarrollo del Big Data y la Inteligencia Artificial y los cambios que en la vida de las personas van a introducir estas tecnologías. Los Estados ya han comenzado a reflexionar sobre la elaboración de normas jurídicas y la introducción de cambios legislativos en sus ordenamientos jurídicos que tengan en consideración el impacto de las tecnologías cognitivas.

En la Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión Europea sobre Normas de Derecho Civil sobre Robótica[9], se hace mención de la importancia que en un escenario en el que la Inteligencia Artificial va a desencadenar una nueva revolución industrial, el legislador pondere las consecuencias jurídicas y éticas, sin obstaculizar con ello la innovación.

En esta línea se constituyó, en el mes de Abril de 2018, un Grupo de Expertos en Inteligencia Artificial, compuesto por representantes del mundo académico, la sociedad civil y la industria. El Grupo (HLEG AI) tiene como objetivo apoyar la implementación de la estrategia europea en esta materia, contemplando la elaboración de recomendaciones sobre el desarrollo de políticas relacionadas con el futuro y sobre cuestiones éticas, legales y sociales. El pasado 18 de Diciembre de 2018 publicaron un borrador con las "Directrices éticas que debe seguir el desarrollo y utilización de la Inteligencia Artificial[10]" cuya publicación definitiva está prevista para el próximo 2019.

7.Periodismo de Datos, Inteligencia Artificial y Privacidad

El Periodismo de Datos (PD) es una nueva disciplina periodística que trae consigo nuevas narrativas periodísticas, nuevas presentaciones y otra forma de acceder a los datos públicos. Recabar, analizar y preguntar a los datos mediante una serie de herramientas especializadas para convertirla en información accesible para la audiencia es su principal referencia.

La puesta en marcha de nuevas investigaciones, análisis en profundidad, localizar temas no divulgados, y hacerlo de forma innovadora aprovechando los datos, las estadísticas, las fuentes documentales o gráficos es el objetivo principal que persigue esta nueva modalidad periodística.

Un periodismo cuya base es el manejo de grandes volúmenes de datos abiertos en la red *open data*, impulsados por el aumento de los mismos en la red de acceso libre y de forma gratuita que pueden ser utilizados o como fuente o como herramienta que permitirá narrar historias. Unas posibilidades que tenemos hoy gracias a la evolución que en los últimos años están teniendo las tecnologías Big Data e Inteligencia Artificial, esenciales en el procesamiento y extracción de información a partir de los datos.

Herramientas como *Scrapewiki, Google Forms, DataWrapper.Narrativa, Google Cloud, Qvest, UGiat* son utilizadas por cabeceras de referencia en el mundo del periodismo como *The Guardian, The New York Times* o *The Washington Post.*

Uno de los elementos esenciales para la utilización apropiada de estos datos es su verificación y el contraste con las distintas fuentes de información, una técnica habitual que ha existido siempre en el campo del periodismo, aunque desde hace relativamente pocos años han comenzado a surgir herramientas que exclusivamente se dedican a la verificación de datos (*fact-check*) en el discurso periodístico. Su objetivo, según los expertos, es implantar otra nueva forma de entender el periodismo, más allá de las conocidas declaraciones de las fuentes. El *fact-check* es una herramienta que permite utilizar ese análisis de los datos para informar, contextualizar o elaborar reportajes con historias más completas. Un nuevo método de trabajo que basado en el análisis de grandes volúmenes de información y con la ayuda de un equipo de trabajo multidisciplinar formado por analistas, informáticos, estadísticos o programadores someterán a examen la información encontrada y procesarán los datos.

Son muchos los medios de comunicación en el ámbito nacional e internacional que han apostado por una sección de trabajo en PD. En Estados Unidos cuentan con experiencias en *The Washington Post* o *Los Angeles Times*. Y en Latinoamérica se encuentran *El Tiempo* de Colombia, *La Nación* en Costa Rica y *Ojo Público* en Perú. Mientras en Europa hay otras experiencias como el diario alemán *Zeit Online*, o la del diario francés *Le Monde*. Y en España experiencias más recientes han creado proyectos o secciones tanto en medios de comunicación generalistas como *El Mundo, El Confidencial* o *ElDiario.es* como en plataformas o Fundaciones como *Civio* o *Datadistas*.

Todos, referencias de medios de comunicación que generan informaciones procedentes de datos abiertos y por las que existe una gran demanda e interés no sólo por parte de ellos, sino también por parte de diferentes organizaciones con el fin de reutilizarlos en sus análisis, explotación o tratamiento. Un desarrollo que ha alcanzado su plenitud en España tras la promulgación de la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTAIBG).

Pero también existen limitaciones ya que no todos los datos son accesibles y es a través de la normativa legal donde se establece la política de acceso a la información. En España, diferente legislación regula el acceso a la información pública y la transparencia en la actividad política. Además de la citada LTAIBG, destacamos las modificaciones en la Ley General Tributaria (Ley 58/2003) y la Ley Orgánica 10/2015, Modificación de la Ley Orgánica 6/1985, del Poder Judicial, donde se ha incluido articulado específico que regula el acceso a la información.

Ahora bien, los principios de transparencia y publicidad pueden colisionar en ocasiones con otros derechos constitucionalmente protegidos, como son los de intimidad y protección de

datos, por lo que deben ponderarse adecuadamente los distintos intereses que se pretenden salvaguardar. Por ello hay que tener en cuenta lo establecido en la normativa comunitaria y nacional en materia de Protección de Datos: el RGPD ya mencionado en apartados anteriores y la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Por otro lado, la Ley 37/2007 (modificada por la Ley 18/2015) supuso en España un salto cualitativo ya que obliga al sector público a ofrecer al público los documentos en cualquier formato o lengua y a ampliar su ámbito de aplicación a bibliotecas, museos y archivos. La Ley mejora la regulación de los formatos promoviendo ofrecerlos en formatos abiertos junto con sus metadatos. Sin embargo, la reutilización de los mismos no es automática cuando en ella se utilizan datos personales que pueden originar vulneraciones en el derecho a la protección de datos personales. Y así se establece cuando la propia Ley hace referencia a la normativa de protección de datos personales en la reutilización de la documentación.

Por otra parte, dicha Ley sienta un punto de conexión con la normativa reguladora de la transparencia y acceso a la información pública al señalar que existen restricciones en cuanto al tratamiento de documentos sobre los que aparecen prohibiciones o limitaciones en el derecho de acceso en virtud de lo previsto en la LTAIBG. Esta última es una ley que, en España, contempla dos modalidades para la obtención de información pública: la publicidad activa y el ejercicio individual del derecho de acceso a la información pública. Y es en este caso donde el ejercicio profesional de los Periodistas de Datos puede originar un conflicto entre dos derechos fundamentales: por una parte, el derecho a la información reconocido y garantizado en el artículo 20 de la Constitución Española y, por la otra, el derecho a la protección de datos personales, reconocido en el artículo 18.4 de la Constitución.

Según doctrina y jurisprudencia, ¿qué derecho debe predominar sobre el otro para dar la información cuando existen datos sensibles y personales? ¿Cómo y cuándo puede reutilizarse la información del sector público para no interferir con la normativa de protección de datos?

La Agencia Española de Protección de Datos publicó en 2016 la guía con las orientaciones sobre protección de datos en la reutilización de la información del sector público. ¿Cuáles son esos supuestos/licencias que recomienda como buenas prácticas la AEPD?

La importancia de la elaboración de evaluaciones de impacto en los casos de reutilización de la información del sector público ha sido destacada en el Dictamen 06/2013 del Grupo de Trabajo del Artículo 29. Este documento dedica varios apartados a la evaluación de los riesgos en donde además hace referencia a las tecnologías que pueden ser útiles para llevar a cabo la anonimización de los datos de carácter personal. Una anonimización que, cada vez, es más difícil y, sobre todo, para los medios de comunicación cuyos sistemas de información, uso de tecnologías cognitivas y la diversidad de fuentes disponibles les permiten revertir el proceso.

Conclusiones

La implantación de las tecnologías cognitivas como Big Data e Inteligencia Artificial deben llevarse a cabo manteniendo el equilibrio necesario entre los grandes avances que van a traer estas tecnologías en el desarrollo humano y el respeto por los derechos fundamentales de los ciudadanos entre los cuales se encuentra el derecho a la protección de datos.

Los principios introducidos por el RGPD: licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva son de obligado cumplimiento en el tratamiento de los datos de carácter personal. Y especialmente deben ser observados y garantizados en el desarrollo y la implantación de las tecnologías cognitivas sin menoscabar los derechos de las personas.

La aplicación del principio *Privacy by Design*, el cual obliga a tener en cuenta el posible impacto en la privacidad desde el mismo momento del diseño de cualquier solución tecnológica, debe ser tenido en cuenta desde la génesis de las soluciones basadas en tecnologías cognitivas.

Deviene fundamental la utilización las estrategias de *gobierno de los datos*, estableciendo metodologías, políticas y herramientas que permiten la gestión de los datos personales y de la información para asegurar su calidad, control y explotación según los objetivos estratégicos y el cumplimiento normativo sobre la materia.

El Periodismo de Datos, impulsado en los últimos tiempos por el avance de las tecnologías cognitivas y favorecido por el principio de transparencia que debe estar presente en toda actividad pública, obtiene sus fuentes de las instituciones públicas quienes cada vez ponen a disposición del público una mayor cantidad de datos abiertos, *open data.* Esta forma de hacer periodismo basada en la reutilización de los datos apoyándose en la tecnología tiene el reto de conjugar el ejercicio del derecho a la información con la no vulneración del derecho a la protección de los datos de carácter personal, ambos reconocidos como derechos fundamentales en la Constitución en España.

El descubrimiento de las actividades de Cambridge Analytica en la elaboración de perfiles ideológicos con los datos obtenidos de Facebook ha supuesto un antes y un después en el modo en que los ciudadanos perciben la utilización de la información que comparten en redes sociales. La utilización de las tecnologías cognitivas para influenciar en las decisiones políticas pone de manifiesto la necesidad de implantar unas garantías normativas efectivas que controlen el tratamiento de los datos personales por empresas y organizaciones.

Lejos de ese objetivo, el legislador español ha introducido en la Disposición Final Tercera de la Ley Orgánica 3/2018 de Protección de Datos Personales la autorización para que los partidos políticos españoles puedan recopilar información de las opiniones políticas de las personas. Esta disposición modifica el artículo 58 de la Ley Orgánica 5/1985, y permite a los partidos rastrear información sobre ideología política en redes sociales, páginas web y otras fuentes de acceso público, de modo que se puedan enviar *anuncios personalizados* a los ciudadanos.

El pasado mes de marzo de 2019, el Defensor del Pueblo ha interpuesto recurso de inconstitucionalidad, por estimar que vulnera los artículos 9.3, 16, 18.4, 23.1 y 53.1 de la Constitución de 1978. Este recurso ha sido admitido a trámite por unanimidad por el Pleno del Tribunal Constitucional.

[1] KALLINIKOS, J. (2018). "En la mayoría de los casos, no tienes ni idea de dónde acabarán tus datos", entrevista, El País, 10 de diciembre.
https://elpais.com/tecnologia/2018/11/30/actualidad/1543597535_915372.html
(consultado el 13 de marzo de 2018)

[2] WEIZENBAUM, J. (08/01/1923 -05/03/2008), Profesor emérito de Informática, Instituto Tecnológico de Massachusetts.

[3] Art. 4.4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES
(consultado el 13 de marzo de 2018)

[4] Artículo 22 RGPD. 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. 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. 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.*

[5] Artículo 5 RGPD. Principios relativos al tratamiento:

> *1. Los datos personales serán:*
> *a) tratados de manera lícita, leal y transparente en relación con el interesado. 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. c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado. f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo* ("responsabilidad proactiva").

[6] Este Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

[7] Artículo 6 RGPD. Licitud del tratamiento:

> *1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan*

los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

[8] No son los rusos, es el Big Data. El Confidencial 20/03/2018 - Juan Manuel López Zafra profesor titular de Estadística en el CUNEF. https://blogs.elconfidencial.com/economia/big-data/2018-03-20/rusos-big-data-cambridge-analytica_1538043/

[9] P8_TA(2017)0051 Resolución del Parlamento Europeo de 16 de Febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre robótica (2015/2013(INL))

[10] Digital Single Market Report / Study|18 December 2018|. Draft Ethics Guidelines for Trustworthy AI https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai (consultado el 10 de marzo de 2019).

Documentación

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2016). Orientaciones sobre Protección de Datos en la Reutilización de la Información del Sector Público. Informe.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 WP251rev.01. (2017)Directrices sobre Decisiones Individuales Automatizadas y Elaboración de Perfiles a los Efectos del Reglamento 2016/679 (adoptadas el 3 de octubre) (revisadas por última vez y adoptadas el 6 de febrero de 2018)

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 WP260rev.01. (2017). Directrices sobre la Transparencia en Virtud del Reglamento (UE) 2016/679 (adoptadas el 29 de noviembre) (revisadas por última vez y adoptadas el 11 de abril de 2018)

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 WP248rev.01. (2017). Directrices sobre la Evaluación de Impacto relativa a la Protección de Datos (EIPD) y para Determinar si el Tratamiento "entraña probablemente un alto riesgo" a Efectos del Reglamento (UE) 2016/679 (adoptadas el 4 de abril)(revisadas por última vez y adoptadas el 4 de octubre de 2017)

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 WP229rev.01. (2017). Directrices sobre el Consentimiento en el Sentido del Reglamento (UE) 2016/679 (adoptadas el 28 de noviembre)(revisadas por última vez y adoptadas el 10 de abril de 2018)

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 WP207 rev.01 (2013). Opinion 06/2013 on Open Data and Public Sector Information ('PSI') Reuse (Adopted on 5 June 2013)