

Martes, 14 de marzo de 2017

P8_TA(2017)0076

Implicaciones de los macrodatos en los derechos fundamentales

Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI))

(2018/C 263/10)

El Parlamento Europeo,

- Visto el artículo 16 del Tratado de Funcionamiento de la Unión Europea,
- Vistos los artículos 1, 7, 8, 11, 14, 21, 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea,
- Vistas las Directrices para la regulación de los archivos de datos personales informatizados recogidas en la Resolución 45/95 de 14 de diciembre de 1990 de la Asamblea General de las Naciones Unidas,
- Vistos el 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) ⁽¹⁾, y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo ⁽²⁾,
- Vista la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 6 de mayo de 2015, titulada «Una Estrategia para el Mercado Único Digital de Europa» (COM(2015)0192),
- Vistos el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (ETS n.º 108), y su Protocolo adicional, de 8 de noviembre de 2001 (ETS n.º 181) ⁽³⁾,
- Vista la Recomendación CM/Rec(2010)13, de 23 de noviembre de 2010, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre la protección de las personas con respecto al tratamiento automático de datos de carácter personal en el contexto de perfiles ⁽⁴⁾,
- Visto el Dictamen 7/2015, de 19 de noviembre de 2015, del Supervisor Europeo de Protección de Datos titulado «Meeting the challenges of big data; A call for transparency, user control, data protection by design and accountability» (Afrontar los desafíos de los macrodatos — Llamamiento en favor de la transparencia, el control por los usuarios, la protección de los datos desde la fase de diseño y la rendición de cuentas) ⁽⁵⁾,
- Visto el Dictamen 8/2016, de 23 de septiembre de 2016, del Supervisor Europeo de Protección de datos titulado «EDPS Opinion on coherent enforcement of fundamental rights in the age of big data» (Dictamen del SEPD sobre la aplicación coherente de los derechos fundamentales en la era de los macrodatos) ⁽⁶⁾,

⁽¹⁾ DO L 119 de 4.5.2016, p. 1.

⁽²⁾ DO L 119 de 4.5.2016, p. 89.

⁽³⁾ <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>

⁽⁴⁾ https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00

⁽⁵⁾ https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

⁽⁶⁾ https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-23_BigData_opinion_EN.pdf

Martes, 14 de marzo de 2017

- Vista la declaración, de 16 de septiembre de 2014, del Grupo de Trabajo del artículo 29 relativo a la Protección de Datos, sobre el impacto del desarrollo de los macrodatos en la protección de las personas por lo que respecta al tratamiento de sus datos personales en la UE ⁽¹⁾,
 - Visto el artículo 52 de su Reglamento,
 - Visto el informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (A8-0044/2017),
- A. Considerando que el concepto de macrodato se refiere a la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos);
- B. Considerando que algunos casos de utilización de macrodatos implican la capacitación de dispositivos de inteligencia artificial como redes neuronales y modelos estadísticos con el fin de predecir algunos acontecimientos y comportamientos; y que los datos de capacitación a menudo son de una calidad cuestionable y no son neutrales;
- C. Considerando que el avance de las tecnologías de la comunicación y la utilización generalizada de dispositivos electrónicos, aparatos de seguimiento, medios sociales, redes e interacciones en internet, incluidos dispositivos que comunican informaciones sin intervención humana, han dado lugar a la aparición de grandes conjuntos de datos cada vez mayores que, a través de técnicas avanzadas de tratamiento y análisis, permiten tener una visión sin precedentes del comportamiento humano, de la vida privada y de nuestras sociedades;
- D. Considerando que los servicios de inteligencia de los terceros países y de los Estados miembros se han estado apoyando cada vez en mayor medida en el tratamiento y la analítica de este tipo de conjuntos de datos que, o bien no están cubiertos por ningún marco jurídico o, más recientemente, han sido objeto de medidas legislativas cuya compatibilidad con el Derecho primario y el Derecho derivado de la Unión suscita preocupación y todavía debe determinarse;
- E. Considerando que el recrudecimiento del acoso y de la violencia contra las mujeres, así como de la vulnerabilidad de los menores, también se está produciendo en internet; y que la Comisión y los Estados miembros deben adoptar todas las medidas jurídicas necesarias para luchar contra estos fenómenos;
- F. Considerando que un número creciente de empresas, sociedades, órganos y agencias, organizaciones gubernamentales y ONG (además de los sectores público y privado en general), dirigentes políticos, la sociedad civil, el mundo académico y la comunidad científica y los ciudadanos en su conjunto han aprovechado esos conjuntos de datos y la analítica de macrodatos para estimular la competitividad, la innovación, la prospección del mercado, las campañas políticas, la publicidad selectiva, la investigación científica y la elaboración de políticas en los ámbitos del transporte, la fiscalidad, los servicios financieros, las «ciudades inteligentes», la aplicación de la ley, la transparencia, la salud pública y la respuesta a las catástrofes, así como para influenciar las elecciones y los resultados políticos, por ejemplo mediante comunicaciones específicas;
- G. Considerando que el mercado de macrodatos crece ya que cada vez se reconoce en mayor medida que la tecnología y el proceso de toma de decisiones con base empírica ofrecen soluciones; que todavía no existe la metodología para llevar a cabo una evaluación del impacto total de los macrodatos con base empírica pero que sí existen pruebas que sugieren que la analítica de macrodatos posee el potencial de ejercer un considerable impacto transversal en los sectores público y privado; y que la Estrategia para el Mercado Único Digital de Europa de la Comisión reconoce el potencial de las tecnologías, los servicios y los macrodatos con base empírica como catalizadores del crecimiento económico, la innovación y la digitalización en la Unión;
- H. Considerando que la analítica de macrodatos genera valor añadido de diversas maneras y que son muchos los ejemplos positivos de ello, ya que generan importantes oportunidades para los ciudadanos, por ejemplo en los ámbitos de la asistencia sanitaria, la lucha contra el cambio climático, la reducción del consumo energético, la mejora de la seguridad en el transporte y la posibilidad de establecer ciudades inteligentes, mejorando, así, la optimización y eficiencia de las

⁽¹⁾ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Martes, 14 de marzo de 2017

empresas y contribuyendo a una mejora de las condiciones laborales y a la detección y la lucha contra el fraude; y que los macrodatos pueden ofrecer una ventaja competitiva para los procesos de toma de decisiones de las empresas europeas, al mismo tiempo que el sector público puede beneficiarse de una mayor eficacia gracias a un mejor conocimiento de los distintos niveles de desarrollo socioeconómico;

- I. Considerando que los macrodatos presentan el potencial mencionado anteriormente para los ciudadanos, el mundo académico y la comunidad científica y los sectores público y privado, pero que también conllevan riesgos significativos, concretamente en lo que se refiere a la protección de derechos fundamentales como el derecho a la privacidad, la protección y la seguridad de los datos, además de la libertad de expresión y la no discriminación, garantizados por la Carta de los Derechos Fundamentales y la legislación de la Unión; que las técnicas de seudonimización y cifrado pueden atenuar los riesgos anejos a la analítica de macrodatos y, por ello, desempeñar un papel importante en la garantía de la privacidad del interesado y fomentar, asimismo, la innovación y el crecimiento económico; y que estos elementos deben considerarse parte de la revisión que se está realizando en la actualidad de la Directiva sobre privacidad electrónica;
- J. Considerando que la generalización de los sensores, la producción rutinaria y extensiva de datos y las actividades actuales de tratamiento de datos no siempre tienen un grado de transparencia suficiente, plantean desafíos a la capacidad de los ciudadanos y de las autoridades de evaluar los procesos y la finalidad de la recopilación, la compilación, el análisis y el uso de datos personales; y que puede observarse la aparición de una difuminación entre datos personales y no personales derivada del uso de la analítica de macrodatos, que puede generar la creación de nuevos datos personales;
- K. Considerando que el sector de los macrodatos está creciendo a un ritmo del 40 % anual, siete veces más rápidamente que el del mercado de las tecnologías de la información; que la concentración de grandes conjuntos de datos generados por las nuevas tecnologías ofrece información fundamental para las grandes empresas, lo que desencadena cambios sin precedentes en el equilibrio de poderes entre los ciudadanos, los gobiernos y los agentes privados; que tal concentración de poder en manos de las empresas podría consolidar monopolios y prácticas abusivas y tener un efecto perjudicial en los derechos de los consumidores y en la competencia justa en el mercado; y que deberían seguir analizándose en mayor medida los intereses de las personas y la protección de los derechos fundamentales en el contexto de las concentraciones de macrodatos;
- L. Considerando que los macrodatos poseen un enorme potencial sin aprovechar como motores de productividad y como medio para ofrecer mejores productos y servicios a los ciudadanos; y haciendo hincapié, no obstante, en que el uso generalizado por parte de los ciudadanos de dispositivos, redes y aplicaciones digitales inteligentes no refleja necesariamente satisfacción con los productos ofrecidos sino, más bien, un reconocimiento general de que estos servicios se han convertido en indispensables para vivir, comunicarse y trabajar, a pesar de la falta de conocimiento de los riesgos que pueden entrañar para nuestro bienestar, seguridad y derechos;
- M. Considerando que debe hacerse una distinción entre cantidad y calidad de los datos a fin de facilitar la utilización eficaz de los macrodatos (algoritmos y otras herramientas analíticas); y que los datos y/o los procedimientos de baja calidad en los que se basan los procesos de toma de decisiones y las herramientas analíticas podrían dar lugar a algoritmos sesgados, correlaciones falsas, errores, una subestimación de las repercusiones éticas, sociales y legales, el riesgo de utilización de los datos con fines discriminatorios o fraudulentos y la marginación del papel de los seres humanos en esos procesos, lo que puede traducirse en procedimientos deficientes de toma de decisiones con repercusiones negativas en las vidas y oportunidades de los ciudadanos, en particular los grupos marginalizados, así como generar un impacto negativo en las sociedades y empresas;
- N. Considerando que la responsabilidad algorítmica y la transparencia deben implicar la aplicación de medidas técnicas y operativas que garanticen la transparencia, la no discriminación de la toma de decisiones automatizadas y el cálculo de probabilidades de comportamiento individual; que la transparencia debe facilitar a las personas información fiable sobre la lógica aplicada, el significado y las consecuencias previstas; y que debe incluir información sobre los datos utilizados para la formación en materia de análisis de macrodatos y permitir a las personas comprender y controlar las decisiones que los afectan;

Martes, 14 de marzo de 2017

- O. Considerando que el análisis de datos y los algoritmos tienen cada vez más repercusión en la información que se facilita a los ciudadanos; que dichas técnicas, en caso de utilizarse indebidamente, podrían poner en peligro los derechos fundamentales a la información, así como la libertad de los medios de comunicación y el pluralismo; y que el sistema de radiodifusión pública en los Estados miembros está directamente relacionado con las necesidades democráticas, sociales y culturales de cada sociedad y con la necesidad de preservar el pluralismo de los medios de comunicación, según contempla el Protocolo sobre el sistema de radiodifusión pública de los Estados miembros anejo al Tratado de Ámsterdam (11997D/PRO/09);
- P. Considerando que la proliferación del tratamiento y la analítica de datos, la infinidad de agentes que intervienen en la recopilación, la conservación, el tratamiento y el intercambio de datos, así como la combinación de grandes conjuntos de datos que contienen datos personales y no personales procedentes de distintas fuentes, si bien brindan oportunidades significativas, todos ellos han generado una gran inseguridad tanto para los ciudadanos como para los sectores público y privado en lo que se refiere a los requisitos específicos para el cumplimiento de la legislación vigente en la Unión en materia de protección de datos;
- Q. Considerando que existen numerosos sistemas legados no estructurados que contienen volúmenes enormes de datos recopilados por las empresas desde hace años con sistemas de gobernanza de datos dudosos que deberían adecuarse sistemáticamente;
- R. Considerando que debe impulsarse una mayor cooperación y coherencia entre los reguladores y las autoridades de supervisión, y las autoridades encargadas de la protección del consumidor y de la protección de datos a escala nacional y de la Unión con el fin de velar por un enfoque coherente y la comprensión en relación con las implicaciones de los macrodatos en relación con los derechos fundamentales; y que la creación y el desarrollo de una cámara de compensación digital ⁽¹⁾ como red voluntaria de los órganos de control puede contribuir a reforzar sus trabajos y sus actividades respectivas en materia de aplicación de la ley, además de poder contribuir a profundizar las sinergias y la protección de los derechos e intereses de las personas;

Consideraciones generales

1. Subraya que los ciudadanos, los sectores público y privado, el mundo académico y la comunidad científica solo podrán aprovechar plenamente las perspectivas y oportunidades que brindan los macrodatos si la confianza pública en esas tecnologías se garantiza mediante la estricta observancia de los derechos fundamentales y el cumplimiento de la legislación vigente de la Unión en materia de protección de datos, así como la seguridad jurídica en relación con todas las partes interesadas; pone de relieve que el tratamiento de los datos personales solo puede realizarse de conformidad con alguno de los fundamentos jurídicos recogidos en el artículo 6 del Reglamento (UE) 2016/679; considera fundamental que la transparencia y la correcta información al público afectado son fundamentales para generar la confianza de la opinión pública y la protección de los derechos individuales;
2. Hace hincapié en que el cumplimiento de la legislación vigente en materia de protección de datos, así como la existencia de unas normas científicas y éticas estrictas, son fundamentales para generar confianza en las soluciones basadas en los macrodatos y para que sean fiables; subraya, asimismo, que la información revelada por los análisis de los macrodatos no ofrece una visión general objetiva e imparcial de ninguna materia y que es tan fiable como lo permitan los datos subyacentes; resalta que los análisis predictivos basados en macrodatos únicamente pueden ofrecer una probabilidad estadística y que, por ello, no pueden predecir siempre con precisión la conducta individual; resalta, por ello, que son fundamentales normas científicas y éticas estrictas para gestionar la recopilación de datos y valorar los resultados de esos análisis;
3. Señala que puede inferirse información delicada sobre las personas de datos que no sean de carácter sensible, lo que desdibuja la línea entre la información delicada y la que no es de carácter sensible;
4. Destaca que el escaso conocimiento y comprensión por parte de los ciudadanos sobre la naturaleza de los macrodatos posibilita que la información personal se utilice de formas indebidas; señala que la educación y la concienciación sobre los derechos fundamentales reviste una importancia de primer orden en la Unión; insta a las instituciones de la Unión y a los Estados miembros a que inviertan en la alfabetización digital y la sensibilización en relación con los derechos digitales, la privacidad y la protección de datos entre los ciudadanos, incluidos los menores; subraya que este tipo de educación debe abordar la comprensión de los principios y la lógica de cómo funcionan los algoritmos y los procesos de toma de decisiones automatizadas y cómo interpretarlos de forma significativa; subraya, asimismo, la necesidad de educar con vistas a fomentar

⁽¹⁾ Dictamen 8/2016, de 23 de septiembre de 2016, del Supervisor Europeo de Protección de datos, p. 15.

Martes, 14 de marzo de 2017

la comprensión de dónde y cómo se recaban los flujos de datos (es decir, la extracción de información de sitios web, *web scraping*, combinando los flujos de datos con datos de las redes sociales y los dispositivos conectados e incorporándolos a un nuevo flujo continuo de datos);

Los macrodatos para fines comerciales y en el sector público

Privacidad y protección de datos

5. Señala que el Derecho de la Unión sobre la protección de la privacidad y los datos personales, el derecho a la igualdad y a la no discriminación, el derecho de las personas a recibir información sobre la lógica que subyace en relación con la toma de decisiones automatizada y la elaboración de perfiles y el derecho a interponer un recurso por vía judicial son aplicables al tratamiento de datos incluso cuando dicho tratamiento esté precedido de técnicas de seudonimización o, en cualquier caso, cuando el uso de datos no personales pueda repercutir en la vida privada de las personas o en otros derechos y libertades, lo que conduciría a estigmatizar a grupos completos de la población;

6. Subraya que el mercado único digital debe construirse sobre la base de redes de alta velocidad fiables y de confianza y de servicios que protejan los derechos fundamentales de la persona interesada en relación con la protección de los datos y la privacidad, alentando a la vez la innovación y las analíticas de macrodatos a fin de crear las condiciones idóneas y unas condiciones de competencia equitativas para impulsar la economía digital europea;

7. Pone de relieve, asimismo, la posibilidad de reidentificar individuos mediante la correlación de distintos tipos de datos anonimizados; subraya que el Derecho de la Unión sobre la protección de la privacidad y los datos personales solo se aplica al tratamiento de estos datos correlacionados cuando un individuo es realmente reidentificable;

8. Hace hincapié en que los principios mencionados anteriormente deben servir de marco para los procedimientos de toma de decisiones de los sectores público y privado y de otros agentes que utilizan los datos; hace hincapié en la necesidad de un grado de transparencia y de una responsabilidad algorítmica mucho mayor por lo que respecta al tratamiento y la analítica de datos por los sectores público y privado y cualquier otro agente que utilice la analítica de datos como herramienta de base para garantizar que el individuo esté informado adecuadamente sobre el tratamiento de sus datos personales;

9. Destaca el papel fundamental que la Comisión, el Comité Europeo de Protección de Datos, las autoridades nacionales de protección de datos y otras autoridades de supervisión independientes deberían desempeñar en el futuro para promover la transparencia y un tratamiento adecuado, la seguridad jurídica en términos generales y, más concretamente, normas concretas de protección de las garantías y los derechos fundamentales asociadas al uso del tratamiento y la analítica de datos por los sectores público y privado; pide que se intensifique la colaboración entre los reguladores de la conducta en el entorno digital para reforzar las sinergias entre los marcos reguladores de los consumidores y las autoridades en materia de competencia y de protección de datos; pide que se dote con recursos financieros y humanos adecuados a dichas autoridades; reconoce, por otra parte, la necesidad de crear una cámara de compensación digital;

10. Subraya que el objetivo intrínseco de los macrodatos debe ser lograr correlaciones comparables con la menor cantidad posible de datos personales; destaca, en ese sentido, que la ciencia, las empresas y los organismos públicos deben centrarse en la investigación y la innovación en el ámbito de la anonimización;

11. Reconoce que la aplicación de la seudonimización, la anonimización o el cifrado de los datos personales puede reducir los riesgos para los interesados cuando se utilizan datos personales en aplicaciones de macrodatos; pone de relieve, asimismo, las ventajas de la seudonimización previstas en el Reglamento general de protección de datos como salvaguardia apropiada; recuerda que la anonimización es un proceso irreversible según el cual no puede seguir utilizándose solamente ningún dato personal para identificar o seleccionar a una persona física; considera que las obligaciones contractuales deben garantizar que los datos anonimizados no se reidentificarán mediante la utilización de correlaciones adicionales mediante la combinación de distintas fuentes de datos; pide a los sectores público y privado y a los demás agentes implicados en el análisis de macrodatos que revisen periódicamente esos riesgos teniendo en cuenta las nuevas tecnologías y que documenten la idoneidad de las medidas adoptadas, pide a la Comisión, al Comité Europeo de Protección de Datos y a las demás autoridades independientes de supervisión que elaboren directrices sobre la manera de anonimizar adecuadamente

Martes, 14 de marzo de 2017

los datos para evitar abusos futuros de estas medidas y que hagan un seguimiento de estas prácticas;

12. Insta a los sectores público y privado y a otros responsables del tratamiento de datos que utilicen los instrumentos previstos en el Reglamento general de protección de datos como, por ejemplo, los códigos de conducta y los sistemas de certificación, en aras de una mayor seguridad sobre sus obligaciones específicas en virtud del Derecho de la Unión, y a que ajusten sus prácticas y actividades a las salvaguardias y normas jurídicas de la Unión que corresponda;

13. Pide a la Comisión y a los Estados miembros que velen por que las tecnologías basadas en los datos no limiten o discriminen el acceso a un entorno mediático pluralista sino que fomenten la libertad de los medios de información y el pluralismo; hace hincapié en que la cooperación entre gobiernos, instituciones educativas y organizaciones de los medios de comunicación desempeñará un papel primordial a la hora de garantizar que se respalda la alfabetización mediática digital para habilitar a los ciudadanos y proteger sus derechos a la información y a la libertad de expresión;

14. Considera que la publicación de datos personales por autoridades públicas por razones de interés público, como la prevención de la corrupción, los conflictos de interés, el fraude fiscal y el blanqueo de capitales, puede ser admisible en una sociedad democrática siempre que la información se revele en las condiciones establecidas por ley, que existan las salvaguardias adecuadas y que dicha publicación sea necesaria y proporcional en relación con el fin perseguido;

Seguridad

15. Reconoce el valor añadido del desarrollo tecnológico, que contribuirá a mejorar la seguridad; reconoce que algunos de los riesgos más acuciantes asociados a las actividades de tratamiento de datos, como las técnicas en materia de macrodatos (en particular en el contexto de la «internet de las Cosas»), que son fuente de preocupación para las personas, incluyen infracciones de seguridad de los datos, acceso no autorizado a los datos y la vigilancia ilegal; estima que para luchar contra esas amenazas sin violar los derechos fundamentales es necesaria una auténtica cooperación concertada entre el sector privado y el sector público, las fuerzas y cuerpos de seguridad y las autoridades de supervisión independientes; pone de relieve, a este respecto, que debe prestarse una atención especial a la seguridad de los sistemas de e-gobierno, así como a medidas adicionales de carácter jurídico como la responsabilidad por el software;

16. Considera que debe fomentarse y, cuando resulte necesario, exigirse, la utilización del cifrado de extremo a extremo, de acuerdo con el principio de protección de datos desde el diseño; recomienda que el futuro marco legislativo para este fin prohíba de manera concreta a los proveedores de servicios de cifrado, a los proveedores de servicios de comunicaciones y al resto de organizaciones (en todos los niveles de la cadena de suministro) que permitan o faciliten las «puertas traseras»;

17. Pone de relieve que un aumento de la generación de datos y de los flujos de datos implica más vulnerabilidades y nuevos retos en materia de ciberseguridad; pide, en este contexto, que se recurra a la protección de la privacidad desde el diseño y por defecto, si procede, a técnicas de anonimización, de cifrado, y a la realización de evaluaciones de impacto preceptivas de la privacidad; pone de relieve que estas dichas medidas deben aplicarlas todos los agentes involucrados en la analítica de macrodatos en los sectores público y privado y los demás agentes que trabajan con datos sensibles, como los abogados, los periodistas y las personas que trabajan en el sector sanitario, de modo que los macrodatos no supongan un incremento del grado de exposición a los riesgos en materia de ciberseguridad;

18. Recuerda que, con arreglo al artículo 15 de la Directiva 2000/31/CE, «los Estados miembros no impondrán a los prestadores de servicios, para la prestación de servicios de transporte, almacenamiento y alojamiento, una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas»; recuerda, en particular, que el Tribunal de Justicia de la Unión Europea, en los casos C-360/10 y C-70/10, desestimó las medidas de «supervisión activa» de la práctica totalidad de los usuarios de los servicios afectados (proveedores de acceso a Internet en un caso, red social en el otro) y precisó que está prohibida cualquier medida que imponga a dicho prestador de servicios de alojamiento de datos una supervisión general;

No discriminación

19. Hace hincapié en que, como consecuencia de los conjuntos de datos y sistemas de algoritmos que se utilizan al hacer evaluaciones y predicciones en las distintas fases del tratamiento de datos, los macrodatos no solo pueden resultar en violaciones de los derechos fundamentales de los individuos sino, también, en un tratamiento diferenciado y en una discriminación indirecta de grupos de personas con características similares, en particular en lo que se refiere a la justicia

Martes, 14 de marzo de 2017

e igualdad de oportunidades en relación con el acceso a la educación y al empleo, al contratar o evaluar a las personas o al determinar los nuevos hábitos de consumo de los usuarios de los medios sociales;

20. Insta a la Comisión, a los Estados miembros y a las autoridades encargadas de la protección de datos a que definan y adopten las medidas que se impongan para minimizar la discriminación y el sesgo algorítmicos y a que desarrollen un marco ético común sólido para el tratamiento transparente de los datos personales y la toma de decisiones automatizada que sirva de guía para la utilización de los datos y la aplicación en curso del Derecho de la Unión;

21. Pide a la Comisión, a los Estados miembros y a las autoridades de protección de datos que evalúen de manera específica la necesidad, no solo de transparencia algorítmica, sino también de transparencia en relación con posibles sesgos en los datos de capacitación utilizados para hacer inferencias sobre la base de los macrodatos;

22. Recomienda que las empresas lleven a cabo evaluaciones periódicas sobre la representatividad de los conjuntos de datos, que consideren si los conjuntos de datos se ven afectados por elementos sesgados, y que desarrollen estrategias para superarlos; pone de relieve la necesidad de examinar la exactitud e importancia de las predicciones basadas en el análisis de los datos teniendo presente las preocupaciones de carácter ético y la equidad;

Los macrodatos para fines científicos

23. Destaca que las analíticas de macrodatos pueden resultar beneficiosas para el desarrollo y la investigación en el ámbito científico; considera que el desarrollo y la utilización de la analítica de macrodatos con fines científicos debe llevarse a cabo teniendo debidamente en cuenta los valores fundamentales consagrados en la Carta de los Derechos Fundamentales y conforme a la actual legislación en materia de protección de datos de la Unión;

24. Recuerda que en el marco del Reglamento general de protección de datos el tratamiento ulterior de los datos personales con fines estadísticos solo puede generar datos agregados que no pueden volver a aplicarse a las personas;

Los macrodatos con fines coercitivos

Privacidad y protección de datos

25. Recuerda a todos los agentes de las fuerzas y cuerpos de seguridad que utilizan el tratamiento y la analítica de datos que la Directiva (UE) 2016/680: regula el tratamiento de datos personales efectuado por los Estados miembros con fines coercitivos; establece que la recopilación y el tratamiento de datos personales con fines coercitivos siempre deben ser adecuados, pertinentes y no excesivos en relación con los propósitos específicos, explícitos y legítimos para los que se tratan; señala que debe probarse claramente la finalidad y los motivos la recopilación de dichos datos; indica que se prohíben 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; pide a la Comisión, al Comité Europeo de Protección de Datos y a las demás autoridades independientes de supervisión que emitan directrices, recomendaciones y buenas prácticas para definir mejor los criterios y condiciones de las decisiones basadas en la elaboración de perfiles y la utilización de macrodatos con fines coercitivos;

26. Destaca la importancia que reviste el cumplimiento de la Directiva (UE) 2016/680 en lo que se refiere a la realización de evaluaciones de impacto previas y auditorías que tengan en cuenta las preocupaciones de carácter ético, a fin de evaluar el carácter integrador, la exactitud y la calidad de los datos y de garantizar que las personas a las que se refieren las decisiones y/o los agentes que intervienen en los procesos de toma de decisiones son capaces de entender e impugnar la recopilación o el análisis, los patrones y las correlaciones y evitar cualesquiera efectos perjudiciales para determinados grupos de personas;

27. Señala que la confianza de los ciudadanos en los servicios digitales puede verse gravemente mermada por las actividades gubernamentales de vigilancia masiva y el acceso injustificado a datos comerciales y otros datos personales de las autoridades encargadas de la aplicación de la ley;

Martes, 14 de marzo de 2017

28. Recuerda que debe considerarse que la legislación que permite a las autoridades públicas tener acceso al contenido de las comunicaciones electrónicas de forma generalizada compromete la esencia del derecho fundamental al respeto de la vida privada, garantizado en el artículo 7 de la Carta;

29. Hace hincapié en la necesidad de que se incorporen directrices y sistemas en las licitaciones públicas para los modelos, herramientas y programas de tratamiento de datos basados en macrodatos en materia de aplicación de la ley con el fin de garantizar que las autoridades encargadas de la aplicación de la ley puedan comprobar el código subyacente y así lo hagan antes de la adquisición final, y que pueda verificarse su adecuación, corrección y seguridad teniendo en cuenta que la transparencia y la responsabilidad están limitadas por el software propio; señala que algunos modelos de actuación policial predictiva son más respetuosos con la privacidad que otros, por ejemplo, cuando se realizan predicciones probabilísticas sobre lugares o acontecimientos y no sobre personas particulares;

Seguridad

30. Subraya la absoluta necesidad de proteger las bases de datos policiales de infracciones en términos de seguridad y del acceso no autorizado ya que se trata de una cuestión que preocupa a las personas; opina, por lo tanto, que para atajar esos problemas se requiere una cooperación concertada y eficaz entre las autoridades encargadas de la aplicación de la ley, el sector privado, los gobiernos y las autoridades independientes de supervisión de la protección de datos; insiste en la necesidad de garantizar una seguridad adecuada de los datos personales con arreglo al Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, así como de minimizar las vulnerabilidades mediante arquitecturas de bases de datos seguras y descentralizadas;

No discriminación

31. Advierte de que, debido al efecto intrusivo de las decisiones y medidas adoptadas por las autoridades encargadas de la aplicación de la ley, también sobre la base del tratamiento de datos y la analítica de datos, en la vida de los ciudadanos y en sus derechos, se requiere la máxima prudencia para evitar la discriminación ilícita y la selección de determinadas personas o grupos de personas, definidos en relación con la raza, el color, el origen étnico o social, las características genéticas, la lengua, la religión o creencia, las opiniones políticas o de otra índole, la propiedad, el nacimiento, la discapacidad, la edad, el género, la expresión o la identidad de género, la orientación sexual, la situación en materia de residencia, la salud o la pertenencia a una minoría nacional, que a menudo es objeto de elaboración de perfiles en función de la etnia o de una actuación policial más intensa, además de las personas que pueden definirse por características particulares; pide que se forme de manera adecuada a quienes recopilan los datos en primera línea y a los usuarios de las informaciones obtenidas del análisis de datos;

32. Pide a las autoridades encargadas de la aplicación de la ley de los Estados miembros que utilizan la analítica de datos en apoyo de las normas éticas más elevadas en el análisis de datos y que garanticen la intervención humana y la rendición de cuentas a lo largo de las distintas etapas de la toma de decisiones para evaluar no solo la representatividad, la exactitud y la calidad de los datos sino también la idoneidad de cada una de las decisiones que vayan a adoptarse sobre la base de dicha información;

o

o o

33. Encarga a su presidente que transmita la presente Resolución al Consejo y a la Comisión.
