Usar webs oficiales y contraseñas "robustas", y no utilizar redes Wifi públicas, consejos para la compra segura '*online*'

MADRID, 19 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD), la Dirección General de Política Comercial y Competitividad, y la Dirección General de Consumo han presentado este lunes una serie de consejos para realizar compras seguras *online*, recomendaciones que pasan por utilizar páginas oficiales y/o de confianza, usar contraseñas robustas y no comprar utilizando redes WiFi públicas.

La presentación ha tenido lugar en vísperas de que se celebre el Black Friday y el Cyber Monday -23 y 26 de noviembre, respectivamente-, fechas elegida por millones de personas para adquirir productos de todo tipo y, en muchos casos, para anticipar sus compras navideñas.

De este modo, los organismos públicos aconsejan cerrar siempre la sesión al finalizar la compra; emplear una tarjeta de uso exclusivo para realizar pagos *online*, no enviar dinero en efectivo o ignorar los correos en los que nos solicitan datos bancarios.

Asimismo, se recomienda revisar la política de privacidad de webs y aplicaciones y no dar más datos de los necesarios para completar la compra. Además, se recuerda que las tiendas no pueden tratar los datos de los menores de 14 años sin el consentimiento de sus padres o tutores.

Por otro lado, en el caso de los juguetes conectados, se aconseja comprobar aspectos como qué datos recoge el juguete; quién y para qué los va a utilizar; qué opciones ofrece para configurar la privacidad o ante quién y cómo se puede interponer una reclamación en caso de querer ejercer nuestros derechos. También es aconsejable optar por productos que ofrezcan información completa e identifiquen de forma clara, por ejemplo, cuándo están grabando la voz del niño/a.

CIUDADANOS "BIEN" INFORMADOS

"Desde la Agencia queremos promover acciones que favorezcan la confianza de los ciudadanos y que posibiliten, al mismo tiempo, el desarrollo de la economía digital, ya que un ciudadano bien informado es clave para el crecimiento de los negocios *online*, donde la confianza es una base fundamental", ha señalado durante la presentación la directora de la AEPD, Mar España.

El director general de Política Comercial y Competitividad de la Secretaría de Estado de Comercio, José Luis Kaiser, ha afirmado que "la Secretaría de Estado de Comercio acompaña tanto a empresas digitales como retailers tradicionales en la transición hacia un modelo de futuro que garantice la elección del consumidor en un marco de comercio seguro".

"En paralelo al perfeccionamiento de los mecanismos de pago *online*, el consumidor ha incrementado su confianza en la seguridad del sistema, precondición para el desarrollo saludable del comercio. Una mayor información sobre los elementos de riesgo en la red unido a la adopción de sistemas de pago seguro y a la protección de los datos que configuran la identidad del usuario en sentido amplio son elementos que determinan la consolidación y crecimiento ordenado del negocio *online*", ha recalcado.

En su intervención, el director general de Consumo del Ministerio de Sanidad, Consumo y Bienestar Social, Nelson Castro, ha destacado la importancia de realizar

una compra reflexiva, en páginas webs seguras y que a los consumidores les asisten los mismos derechos que si hicieran una compra o contratación en un establecimiento físico.

Los materiales presentados este lunes y forman parte de las actuaciones preventivas y de colaboración puestas en marcha por la AEPD para impulsar que los ciudadanos conozcan los derechos que les asisten, en un escenario comercial en el que descuentos y ofertas llamativas pueden ser utilizadas por webs o aplicaciones fraudulentas. Por ello, la AEPD, Comercio y Consumo se han unido para promover que las compras *online* se realicen con seguridad y en sitios de confianza.

Estas recomendaciones y consejos complementan a la Guía de compra segura en internet, una iniciativa realizada por la Agencia, INCIBE, Consumo y la Policía Nacional con la finalidad de generar confianza y contribuir al crecimiento del comercio *online* en España.

https://www.europapress.es/sociedad/noticia-usar-webs-oficiales-contrasenas-robustas-no-utilizar-redes-wifi-publicas-consejos-compra-segura-*online*-20181119145642.html

---

La AEPD aclara que la futura ley de Protección de Datos no permite el tratamiento de datos para crear perfiles políticos

MADRID, 21 (EUROPA PRESS)

La modificación de la Ley Orgánica del Régimen Electoral General (LOREG) en el Proyecto de Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, que se vota este miércoles en el Pleno del Senado, "no permite el tratamiento de datos personales para la elaboración de perfiles basados en opiniones políticas".

Así lo ha indicado este miércoles la Agencia Española de Protección de Datos (AEPD), al tiempo que ha agregado que "tampoco permite el envío de información personalizada basada en perfiles ideológicos o políticos".

"El proyecto sólo permite, conforme al Considerando 56 del Reglamento Europeo de Protección de Datos, la recopilación por parte de los partidos políticos de datos personales relativos a opiniones políticas para obtener información que les permita pulsar las inquietudes de los ciudadanos con el fin de poder darles respuesta en sus propuestas electorales", ha manifestado.

El organismo estatal ha detallado que esta interpretación se fundamenta en la supresión del término "tratamiento" recogido en la enmienda 331 inicialmente presentada en el Congreso de los Diputados, y que este criterio se basa, asimismo, en la supresión del apartado 2 de dicha enmienda, que permitía la difusión de propaganda electoral basada en perfiles ideológicos con determinadas garantías.

Asimismo, la Agencia ha aclarado que el texto "permite el envío de propaganda electoral sin que su contenido pueda basarse en los perfiles antes citados, identificando en cualquier caso su naturaleza electoral y garantizando el ejercicio sencillo y gratuito del derecho de oposición".

"En todo caso, las previsiones del artículo recogido en el Proyecto de ley deben cumplir todas las garantías establecidas en el Reglamento Europeo de Protección de Datos", ha subrayado el organismo que preside Mar España.

En el texto del proyecto, recogido por Europa Press, se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente, en el que se establece que "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".

Además, el nuevo artículo indica que "los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral".

De este modo, indica que el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes "no tendrán la consideración de actividad o comunicación comercial".

"Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral", destaca el artículo, que establece también que se facilitará al destinatario "un modo sencillo y gratuito" de ejercicio del derecho de oposición.

Por su parte, la Confederación de Consumidores y Usuarios (CECU) ha pedido al Gobierno la retirada del artículo. "El problema no es sólo que se pueda realizar publicidad personalizada sin autorización, sino que se permite recopilar información por toda la Red sobre la ideología de los votantes para elaborar bases de datos sin su consentimiento, bases de datos que el Reglamento General de Protección de Datos prohíbe expresamente", ha argumentado.

Según critica la CECU, el Congreso de los Diputados "ha dado el consentimiento por todos los ciudadanos sin consultar ni informar a los interesados". "Pero, además, una vez finalizada la campaña electoral, ¿quién va a controlar qué se hace con esos datos o a quién se facilitan? ¿Quién y cómo se garantizará que esas bases de datos elaboradas por las empresas contratadas al efecto no harán un uso ilícito de las mismas?", ha cuestionado.

Finalmente, ha insistido en que "la creación de tales bases de datos no puede tener más que consecuencias negativas para los ciudadanos" y ha exigido que la creación de las mismas "sea a partir del consentimiento expreso e informado de cada ciudadano". "En caso de que el artículo se apruebe, pedimos a los partidos que, por ética política, se abstengan de realizar esas bases de datos", ha zanjado.

https://www.europapress.es/sociedad/noticia-aepd-aclara-futura-ley-proteccion-datos-no-permite-tratamiento-datos-crear-perfiles-politicos-20181121170736.html

---

Aprobada definitivamente la ley de Protección de Datos con la polémica del tratamiento por parte de los partidos

MADRID, 21 (EUROPA PRESS)

El Pleno del Senado ha aprobado este miércoles definitivamente el Proyecto de Ley Orgánica de protección de datos personales y garantía de los derechos digitales, con el voto en contra de Unidos Podemos, Compromís, Nueva Canarias y Bildu, en medio de la polémica por el artículo '58 bis' sobre utilización de medios tecnológicos y datos personales en las actividades electorales de los partidos políticos.

El texto del Proyecto de ley ha salido adelante en la Cámara Alta tal y como se aprobó en el Congreso de los Diputados ya que PSOE y PP han rechazado todas las enmiendas que habían sido presentadas por Compromís, Ciudadanos, PDeCAT y Unidos Podemos - En Comú Podem - En Marea. La iniciativa legislativa comenzó su tramitación con el PP en el Gobierno. De este modo, sale directamente para su publicación en el Boletín Oficial del Estado (BOE) y su aplicación.

La polémica de esta ley ha surgido a raíz del citado artículo '58 bis' que establece que "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".

Además, el nuevo artículo indica que "los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral".

En este contexto, Unidos Podemos - En Comú Podem - En Marea en el Senado ha elaborado una Propuesta de Modificación al dictamen del Proyecto de la Ley Orgánica de Protección de Datos para que el artículo se retirase, pero ha sido rechazada por todos los grupos parlamentarios.

"La aplicación de este texto que puede dar vía libre a los partidos políticos para elaborar perfiles ideológicos de los ciudadanos y ciudadanas. La actual legislación otorga a los datos ideológicos de la ciudadanía una protección de carácter especial. Sin embargo, la nueva LOPD supone una peligrosa involución en este sentido. Resultaría muy peligroso que los partidos políticos tuvieran vía libre, sin previa autorización, para contactar con los ciudadanos y ciudadanas de nuestro país, realizar perfiles ideológicos y, además, almacenarlos para fines distintos a los electorales", ha indicado la senadora Celia Cánovas.

Para la senadora de Unidos Podemos, la nueva norma "puede abrir la puerta a que sus opiniones políticas sean grabadas y almacenadas". "En un momento en el que grupos de extrema derecha utilizan las denominadas 'fake news' (noticias falsas) para difundir sus mensajes, es alarmante que esta ley deje un cauce abierto para que una información que pertenece a la propia ciudadanía pueda utilizarse para estos fines", ha apostillado.

PODEMOS ANUNCIA QUE LA RECURRIRÁ AL TC

Tras haber sido aprobada en los términos, la parlamentaria de Unidos ha anunciado que la formación impulsará su modificación mediante una Proposición de Ley Orgánica

y recurrirá al Tribunal Constitucional el redactado.

Por su parte, la senadora socialista Begoña Nasarre ha defendido que esta ley "no permite el tratamiento de datos personales para la elaboración de perfiles basados en opiniones políticas", pero, ante "las dudas" que ha despertado el polémico artículo, se ha mostrado partidaria de despejarlas en el desarrollo reglamentario y de que se pidan los informes jurídicos correspondientes, como ha planteado previamente el senador de ERC Miquel Ángel Estradé.

Finalmente, la parlamentaria 'popular' María Rosa Vindel ha puesto de manifiesto que es una ley "muy consensuada" en el Congreso, y que modifica otras diez leyes "muy trascendentes". "Es una buena ley, señorías a pensar de las alarmas que causa", ha subrayado.

https://www.europapress.es/sociedad/noticia-aprobada-definitivamente-ley-proteccion-datos-polemica-tratamiento-parte-partidos-20181121193623.html

---

Protección de Datos insiste en que es ilegal hacer perfiles ideológicos y estará vigilante a lo que hacen los partidos

MADRID, 22 (EUROPA PRESS)

La presidenta de la Agencia Española de Protección de Datos (AEPD), Mar España, ha advertido de que será "extremadamente vigilante" y "rigurosa" respecto al tratamiento de datos personales que lleven a cabo los partidos políticos y ha insistido en que es "ilegal" hacer perfiles ideológicos en base a las opiniones que viertan los ciudadanos en Internet y enviar propaganda segmentada en base a ese perfilado.

España se ha expresado así en un desayuno informativo, celebrado este jueves 22 de noviembre en la sede de la AEPD, y después de que el Pleno del Senado aprobara definitivamente el Proyecto de Ley Orgánica de protección de datos personales y garantía de los derechos digitales, en medio de la polémica por el artículo '58 bis' sobre utilización de medios tecnológicos y datos personales en las actividades electorales de los partidos políticos.

"La Agencia va a ser extremadamente vigilante y rigurosa en la aplicación de la normativa", ha afirmado España, para después aclarar que "entre sus funciones, la Agencia tiene la competencia de interpretar la normativa de protección de datos en base a las nuevas garantías establecidas en el Reglamento General de Protección de Datos", de obligado cumplimiento desde el pasado 25 de mayo.

En este sentido, la presidenta de la AEPD ha aclarado la interpretación que va a dar a la nueva ley es que "no se permite a los partidos políticos perfilar datos ideológicos, sexuales, de religión o de cualquier otro tipo, que los ciudadanos estén dando a través de su comportamiento en Internet o en las redes sociales".

Asimismo, Mar España ha avisado de que, según su interpretación, "tampoco se permite el envío de publicidad o propaganda electoral adaptada a un perfil ideológico". "No es la primera vez que la Agencia ha realizado actuaciones de investigación durante una campaña electoral y ha declarado una infracción, estableciendo la correspondiente sanción económica", ha asegurado.

DERECHO DE OPOSICIÓN

España ha aclarado que los ciudadanos pueden recibir propaganda electoral a través de medios tecnológicos como el correo electrónico o WhatsApp en periodo electoral de igual manera que en el buzón físico de un domicilio y sin que previamente tengan que dar su consentimiento. No obstante, ha apostillado que los partidos políticos "tienen que garantizar siempre el derecho de oposición de una forma clara, sencilla y accesible".

Según ha detallado Mar España, se podría permitir, por ejemplo, que los partidos políticos testen si en las redes sociales la preocupación por el cambio climático está siendo 'trending topic' y que puedan "adaptar sus programas electorales a esas preocupaciones" o "enviar a través de los datos que hayan obtenido en Internet publicidad o propaganda con el mismo carácter general" que lo enviarían a los domicilios, "y no personalizada" porque "no pueden hacer un seguimiento ideológico".

Además, la responsable de la AEPD ha concretado que después del periodo electoral "esa recopilación de datos que hayan hecho tendrán que destruirla" y ha asegurado que el incumplimiento de la normativa, de acuerdo con los criterios de Protección de Datos y los que establezca la Junta Electoral Central, pueden acarrear sanciones económicas para los partidos políticos que pueden alcanzar los 20 millones de euros en función de

las circunstancias de cada caso.

"Mi obligación a través de la interpretación de la normativa vigente es dar las mayores garantías a los ciudadanos y tienen mi compromiso de que así lo voy a hacer", ha subrayado la presidenta, que ha asegurado que la Agencia actuará "caso a caso" en base a denuncias que reciba, pero también en investigaciones que puede realizar de oficio.

En este contexto, España ha informado de que "ya hace unos días" ha contactado con el presidente de la Junta Electoral Central (JEC) con el objetivo de trabajar conjuntamente en la interpretación "de esas garantías" que, según ha detallado Mar España, el propio Reglamento General indica que "pueden establecerse en la ley o con posterioridad".

Por otro lado, la presidenta de la Agencia Española de Protección de Datos ha afirmado que el organismo no valora la redacción de un artículo de una ley y ha agregado que "respeta profundamente" el trabajo de los grupos parlamentarios.

"La Agencia no avala, la Agencia interpreta y aplica la normativa", ha subrayado, para después aclarar que lo que sí trasladó la AEPD cuando se puso este artículo sobre la mesa fue que "quizás el marco más adecuado para una modificación de una legislación electoral de ese calado no era el de la normativa de protección de datos".

Pese a la polémica generada por este artículo, Mar España ha destacado que esta norma ha tenido un "alto" consenso parlamentario y ha recabado el 93% de los votos favorables, "es un punto importante". "La ley tiene importantes mejoras para garantizar los derechos de los ciudadanos", ha subrayado la presidenta, que ha agregado que se introducen "novedades" y "mejoras", así como "se clarifica conceptos y se da seguridad jurídica".

Finalmente, Mar España ha resaltado que desde 2008 se ha multiplicado por cuatro el volumen de gestión de la AEPD y que desde el pasado 25 de mayo han aumentado un 35% las reclamaciones, mientras que la nueva ley le otorga la obligación de garantizar derechos nuevos. "Necesitamos el refuerzo de los medios personales y materiales", ha destacado, al tiempo que ha explicado que ha pedido un incremento presupuestario del 10% para el año que viene, "algo absolutamente moderado".

https://www.europapress.es/sociedad/noticia-proteccion-datos-insiste-ilegal-hacer-perfiles-ideologicos-estara-vigilante-hacen-partidos-20181122131122.html

---

La AEPD publica el registro de Delegados de Protección de Datos de cerca de 20.000 entidades

MADRID, 11 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD) ha publicado este martes el registro de Delegados de Protección de Datos (DPD), que contiene los datos de contacto de cerca de 20.000 entidades, de las cuales alrededor de 3.000 corresponden al sector público y las restantes al sector privado.

"Este espacio de consulta, disponible en la Sede electrónica de la Agencia, permite a cualquier interesado conocer el contacto de los delegados de protección de datos comunicados a la AEPD", ha explicado la Agencia.

Asimismo, ha indicado que los ciudadanos que quieran ejercitar sus derechos o presentar una reclamación ante una entidad pueden introducir el nombre, razón social o NIF de la organización para conocer los datos de contacto del DPD y dirigirle sus solicitudes.

Según ha explicado la Agencia, la información que figura en esta lista se actualiza diariamente y se corresponde con los datos de contacto que los responsables o encargados del tratamiento facilitan a la AEPD a través del formulario que se encuentra disponible en su Sede electrónica.

En este sentido, ha detallado que la comunicación relativa a las designaciones, nombramientos y ceses de los delegados de protección de datos debe realizarse en el plazo de diez días, tanto en los supuestos en que sea obligatoria su designación como en el caso en que sea voluntaria.

La comunicación de los datos del delegado de protección de datos a la AEPD es obligatoria para organismos públicos, así como para entidades que hagan tratamientos de datos que requieran una observación sistemática a gran escala o tratamientos masivos de categorías especiales de datos, como recoge el RGPD. Y, en todo caso, cuando se trate de las entidades incluidas en el artículo 34.1 de la Ley Orgánica 3/2018.

Con este registro la Agencia da cumplimiento a lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que en su artículo 34.4 señala que 'La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos'.

ESQUEMA DE CERTIFICACIÓN

La AEPD, en colaboración con la Entidad Nacional de Acreditación (ENAC), presentó en julio del año pasado su 'Esquema de certificación de Delegados de Protección de Datos' para ofrecer "seguridad y fiabilidad" a los profesionales de la privacidad y a las empresas y entidades que incorporen esta figura a sus organizaciones.

Según la AEPD, este Esquema permite certificar que los DPD reúnen la cualificación profesional y los conocimientos para ejercer la profesión, y las certificaciones se otorgan por entidades certificadoras debidamente acreditadas por ENAC.

Por el momento, tres entidades han sido acreditadas para poder certificar Delegados de Protección de Datos: IVAC Instituto de Certificación, Asociación para el Fomento de

la Seguridad de la Información (ISMS Fórum), y Asociación Española para la Calidad (AEC). Los DPD certificados pueden consultarse en las páginas web de cada una de estas entidades.

Finalmente, ha señalado que la certificación no es obligatoria y se puede ejercer la profesión sin estar certificado bajo este o cualquier otro esquema, si bien la Agencia ofrece así un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación como garantía para acreditar la cualificación y capacidad profesional de los candidatos a DPD.

https://www.europapress.es/sociedad/noticia-aepd-publica-registro-delegados-proteccion-datos-cerca-20000-entidades-20181211181316.html

---

AEPD avisa de que los partidos no pueden usar big data o inteligencia artificial para inferir la ideología de personas

MADRID, 19 (EUROPA PRESS)

Los partidos políticos, federaciones, coaliciones y agrupaciones de electores "sólo podrán tratar opiniones políticas cuando estas hayan sido libremente expresadas por las personas en el ejercicio de su derecho a la libertad de expresión y a su libertad ideológica".

"Este precepto no ampara aplicar tecnologías de big data o inteligencia artificial para inferir la ideología política de una persona, ya que esto supondría una vulneración de su derecho fundamental a no declarar su ideología", advierte la Agencia Española de Protección de Datos (AEPD) en un informe que acaba de publicar.

La Agencia ha analizado el tratamiento de datos personales en relación con la Disposición final tercera de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, que modifica la Ley Orgánica 5/1985 del Régimen Electoral General (LOREG) añadiendo el artículo 58 bis.

Así, la AEPD aclara que esta modificación fue introducida durante la tramitación parlamentaria de la LOPD y, al no encontrarse en el Proyecto de Ley remitido por el Gobierno, "no fue objeto de informe preceptivo" por parte de la Agencia.

En este sentido, la Agencia considera que la modificación de la LOREG, que aborda el tratamiento de datos relativos a opiniones políticas por los partidos, "debe ser objeto de una interpretación restrictiva".

Por una parte, argumenta que se trata de "una excepción a la regla general" recogida en el artículo 9 del Reglamento General de Protección de Datos (RGPD) y en el 9.1 de la LOPD, que prohíbe el tratamiento de categorías especiales de datos personales --entre las que se encuentran las opiniones políticas--. Además, añade que el artículo 58 bis debe ser interpretado conforme a lo establecido en la Constitución, de modo que no conculque derechos fundamentales como la protección de datos, el derecho a la libertad ideológica, la libertad de expresión e información o el derecho a la participación política.

En relación con la ausencia de definición en la Ley Orgánica 3/2018 de "fuentes de acceso público", la Agencia cree que puede seguir aplicándose como criterio interpretativo la derogada LOPD 15/1999 pero "debe tratarse de webs y fuentes en las que la consulta la pueda realizar cualquier persona, lo que excluiría aquellas en las que el acceso está restringido a un círculo determinado, ya sea como "amigo" u otro concepto similar".

Sobre la finalidad del tratamiento, la AEPD recoge en su informe que éste deberá ser "proporcional al objetivo perseguido" (artículo 9.2 g RGPD), lo que no ampara tratamientos no proporcionales como el microtargeting, ni tener por finalidad forzar o desviar la voluntad de los electores.

"Si bien el funcionamiento de un sistema democrático puede requerir la elaboración de perfiles generales, de modo que los partidos políticos puedan conocer las inquietudes políticas de la ciudadanía, incluso por categorías genéricas como la edad, sexo, población, etc., lo que no puede en ningún caso pretenderse es la realización de perfiles individuales o realizados atendiendo a categorías muy específicas que conculcarían los derechos fundamentales anteriormente citados", añade.

En este sentido, la AEPD recuerda que los tratamientos deben cumplir con todos los principios recogidos en el artículo 5 del RGPD (licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación de plazo de conservación; integridad y confidencialidad y responsabilidad proactiva).

En cuanto al envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de esta en redes sociales o medios equivalentes (artículo 58 bis LOREG), los datos que vayan a ser usados para el envío de la misma (números de teléfono, correo electrónico, etc.) deben haberse obtenido "lícitamente", amparados en alguna de las bases del artículo 6 del RGPD. Además, en los envíos que se realicen deberá constar su carácter electoral y facilitar el derecho de oposición por los destinatarios.

LAS GARANTÍAS

Por otro lado, la Agencia indica que el texto del artículo 58 bis "no detalla las garantías aplicables a este tipo de tratamientos". Por ello, la Agencia ha identificado esas garantías que pasan por que los responsables adopten medidas técnicas y organizativas apropiadas, como la seudonimización e incluso la agregación y anonimización.

Designar un delegado de protección de datos; elaborar el registro de actividades de tratamiento, debiendo ser precisos y claros, conforme a los principios de lealtad y transparencia; o realizar una evaluación de impacto relativa a la protección de datos, al realizar un tratamiento a gran escala de categorías especiales de datos son otras de las garantías identificadas por la Agencia.

Asimismo, se debe consultar a la AEPD antes de proceder al tratamiento cuando la evaluación de impacto muestre que el tratamiento entraña un alto riesgo. "Si esa evaluación de impacto se realiza adecuadamente será obligatorio consultar a la AEPD, salvo que el responsable garantice que el riesgo puede mitigarse", subraya.

Por otro lado, hay que adoptar medidas de seguridad, que deberán ser "lo más rigurosas que permita el estado de la técnica, teniendo en cuenta que se trata de datos referentes a opiniones políticas cuyo tratamiento es excepcional y que suponen un importante riesgo para los derechos y libertades de las personas".

Si el tratamiento va a ser realizado por un encargado en concreto, se debe elegir a uno que de "garantías suficientes" y suscribir con él un contrato en el que se garantice que actuará "sólo siguiendo instrucciones del responsable, debiendo contemplar dichas instrucciones las garantías definidas por la Agencia".

También se debe facilitar el ejercicio de los derechos de acceso, rectificación, supresión y oposición; y en caso de que se pretenda obtener datos de terceros (que no actúen como encargados del tratamiento) el responsable deberá comprobar que esos datos fueron obtenidos de manera lícita y cumpliendo con todos los requisitos del RGPD, especialmente que el tercero tenga una legitimación específica para obtener y tratar dichos datos y que haya informado expresamente a los afectados de la finalidad de cesión a los partidos políticos.

INFORMAR SOBRE EL TRATAMIENTO DE DATOS

Además de estas garantías, la Agencia destaca la obligación de informar sobre los tratamientos "teniendo en cuenta que nos encontramos ante un supuesto excepcional de legitimación de los datos relativos a la ideología política de los ciudadanos".

El informe detalla que, con anterioridad al inicio del periodo electoral, los sujetos legitimados y que vayan a presentar candidatura podrán desarrollar las actuaciones necesarias para preparar los tratamientos que vayan a desarrollar en el periodo electoral, conforme a las obligaciones anteriormente señaladas, pero sin poder iniciarlos.

En especial, las relativas al registro de actividades, evaluación de impacto, consulta previa, designación del delegado de protección de datos (si no lo hubiera designado con anterioridad) y la celebración, en su caso, del contrato de encargado del tratamiento. En periodo electoral podrán iniciar el tratamiento, debiendo en primer lugar cumplir con su obligación de información y velar por el cumplimiento de la normativa de protección de datos.

Por último, la Agencia explica que, "finalizado el periodo electoral, deberán garantizar la supresión de los datos personales conforme a lo establecido en la ISO 27001:2013 y la Norma UNE- EN15713:2010, sin que en ningún caso puedan ser objeto de tratamiento ulterior por los partidos políticos ni por ninguna otra entidad".

https://www.europapress.es/sociedad/noticia-aepd-avisa-partidos-no-pueden-usar-big-data-inteligencia-artificial-inferir-ideologia-personas-20181219115033.html

---

Internautas critican un 2018 marcado por la "falta de respeto" a su privacidad con la Ley de Protección de Datos

MADRID, 24 (EUROPA PRESS)

La Asociación de Internautas ha hecho balance del año 2018, destacando "una de las asignaturas pendientes no superadas" en el citado ejercicio, "la falta de respeto a la privacidad de los internautas" con casos como el Cambridge Analytica o la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El presidente de la asociación, Víctor Domingo, explica que esta circunstancia se ha significado en dos hechos. Por un lado, el "escándalo" del caso de la empresa de datos Cambridge Analytica, con la filtración y uso con fines de propaganda política de los datos de al menos 87 millones de usuarios de Facebook sin la debida autorización.

Según destaca Víctor Domingo, en una entrevista concedida a Europa Press, este hecho produjo que millones de datos fueran utilizados para "intereses espúreos", poniendo de relieve "lo endeble" de la privacidad de los ciudadanos "en estos momentos".

Asimismo, el presidente de la Asociación de Internautas sostiene que "esa sensación se ha agravado ostensiblemente" con la reciente entrada en vigor de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. "Bajo ese rimbombante título, los partidos políticos se han blindado para convertir a sus representados en 'ciudadanos de cristal'", critica.

Otro caso para lamentar desde esta organización ha sido la normativa europea sobre los derechos de autor en el mercado único digital, conocida como Directiva de 'Copyright' aprobada por el Parlamento Europeo el pasado mes de septiembre. "No satisface a los expertos ni a la sociedad civil que ven aún lagunas en su articulado", recalca.

Por otra parte, Víctor Domingo asegura que ha llamado la atención de los internautas "la falta de sensibilidad" de los dos Gobiernos tanto del PP como del PSOE, "en materia de Sociedad de la Información. "El actual, incluso, ha escondido la Secretaría de Estado para la Agenda Digital del título ministerial que ahora se llama Ministerio de Economía y Empresa", lamenta.

Durante el año 2018, según denuncia Domingo, se han producido también "repetidas subidas tarifarias unilaterales por parte de las operadoras telefónicas, principalmente de sus servicios convergentes, para acceder a Internet, obligando al conjunto de los clientes a subvencionar contenidos no deseados cómo el caso del fútbol".

De cara al año nuevo, la Asociación de Internautas pide la reactivación el Consejo Asesor de las Telecomunicaciones y para la Sociedad de la Información (CATSI), órgano asesor del Gobierno en materia de telecomunicaciones y sociedad de la información que tiene como cometido el estudio, deliberación y propuesta en materias relativas a las telecomunicaciones y a la sociedad de la información, sin perjuicio de las competencias que correspondan a los órganos colegiados interministeriales con competencias de informe al Gobierno en materia de política informática.

"Este Consejo no ha sido convocado desde 2016, a pesar de que el Gobierno ha hecho propuestas legislativas como la que proponía acabar con el anonimato en Internet, calificada desde la sociedad civil como un intento de recortar las libertades en

Internet, y un ataque "muy grave" contra derechos fundamentales, en particular la libertad de expresión e ideológica o la reciente Ley de Propiedad Intelectual", argumenta el presidente de la asociación.

También opina que el DNI electrónico "adolece de una Ley Orgánica que garantice la gestión, desarrollo y funcionamiento de este documento vital para la identificación de los ciudadanos ante la administración pública, así como facilitar su funcionamiento".

Según apunta Víctor Domingo, es necesario también el desarrollo de una Ley Orgánica sobre "la interceptación de las comunicaciones electrónicas que establezca las garantías necesarias para que el poder judicial vele y asegure la privacidad y la intimidad de las comunicaciones electrónicas y telefónicas de la ciudadanía".

Finalmente, Domingo avanza que en 2019 la Asociación de Internautas trabajará "en directrices universales para informar y mejorar el diseño y uso de la Inteligencia Artificial (AI)". "Los nuevos desarrollos en Inteligencia Artificial están transformando el mundo de la ciencia y la industria, a la administración gubernamental y las finanzas. El aumento de la toma de decisiones de AI también implica derechos fundamentales de imparcialidad, responsabilidad y transparencia", concluye.

https://www.europapress.es/sociedad/noticia-internautas-critican-2018-marcado-falta-respeto-privacidad-ley-proteccion-datos-20181224115834.html

La AEPD trabaja en un protocolo para que víctimas de violencia de género puedan pedir la retirada de vídeos vejatorios

MADRID, 25 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD) trabaja en un protocolo de actuación para que las víctimas de violencia de género puedan acudir a la Agencia en tutela de derechos y así lograr la retirada "en el menor tiempo posible" de vídeos vejatorios que atentan contra su imagen y su dignidad, y que están siendo difundidos a través de Internet y las redes sociales.

Así lo ha dado a conocer este viernes la presidenta de la Agencia, Mar España en un desayuno informativo, en el que ha detallado que el protocolo de actuación será presentado al Ministerio del Interior, a la Fiscalía General del Estado y al Consejo General del Poder Judicial.

Según ha detallado Mar España, este protocolo se dirige a las víctimas de violencia de género que "además de la violación, los abusos o la suplantación de identidad, están viendo cómo la grabación de esos hechos delictivos que son deleznables se están difundiendo en redes sociales o plataforma".

En este sentido, la presidenta de la AEPD ha asegurado que hasta este momento la Agencia no ha recibido "ni una sola" solicitud de tutela, lo que le parece "preocupante", y ha añadido que este protocolo "es compatible con la posible sanción penal y la instrucción que haga el juez en una fase posterior".

Además, Mar España ha advertido de que si se detecta que el agresor ha vulnerado la privacidad de la víctima será investigado por la Agencia Española de Protección de Datos y ha avisado de que la sanción puede llegar a los 20 millones de euros. "Tendremos tolerancia cero en este tipo de comportamientos que son deleznables", ha subrayado.

"Yo lo que pido es concienciación y advierto a los posibles agresores, que además pretendan seguir vejando a la víctima, porque eso hace imposible la reparación y que esa mujer pueda tener una vida normal si todo el mundo ha conocido los abusos, su identidad, dónde vive, dónde estudia", ha remachado.

Mar España ha asegurado que se puede "conseguir que ese vídeo sea retirado en 24 horas", pero ha aclarado que primero habría que recurrir a la plataforma de Internet y solicitar la retirada del vídeo. "Si la compañía no lo retirara, se acude a la Agencia. En esos casos daremos absoluta prioridad", ha zanjado.

https://www.europapress.es/epsocial/igualdad/noticia-trabajan-protocolo-victimas-violencia-genero-puedan-pedir-retirada-videos-vejatorios-20190125135008.html

---

Aumenta casi un 33% las reclamaciones planteadas ante la Agencia de Protección de Datos en 2018, hasta las 14.146

MADRID, 25 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD) ha recibido un total de 14.146 reclamaciones durante 2018, lo que representa un incremento del 32,8% respecto al año anterior cuando se plantearon 10.651 quejas ante el organismo.

Así lo ha dado a conocer este viernes la presidenta de la Agencia, Mar España en un desayuno informativo, que ha tenido lugar en la sede de la AEPD en Madrid, para presentar las cifras del ejercicio 2018, así como el grado de cumplimiento del Plan Estratégico de 2018 y avanzar algunas líneas de actuación para el presente 2019.

El 25 de mayo de 2018, el Reglamento General de Protección de Datos (RGPD) se hacía de obligado cumplimiento. Ante este hecho, las cifras presentadas por Mar España indican que entre el 1 de enero y el 24 de mayo las reclamaciones pasaron de las 4.550 del año 2017 a las 5.036 denuncias del citado periodo de 2018. Sin embargo, entre el 25 de mayo y el 31 de diciembre, las reclamaciones crecieron un 48,9%.

En relación con la temática de las reclamaciones, Mar España ha explicado que han estado relacionadas con ficheros de morosidad, videovigilancia, servicios de Internet, reclamación de deudas , administración pública, sanidad, publicidad (excepto spam), comercios, transporte y hostelería, entidades financieras (acreedoras), y publicidad a través de correo electrónico o teléfono móvil.

Respecto a las denuncias recibidas y resueltas con respuesta satisfactoria tras haberlas remitido al responsable o delegado de protección de datos (DPD), Mar España ha detallado que durante 2018 se ha producido 863.

No obstante, la presidenta de la AEPD ha explicado que el hecho de que la reclamación se presente ante el responsable del tratamiento de datos personales no implica que la Agencia no realice inspecciones a posteriori, y ha asegurado que un 13% de los 863 expedientes, es decir, 110 están siendo auditados.

Sobre los casos con otras autoridades europeas de protección de datos, de los 395 casos analizados, la Agencia se ha personado como interesada en un total de 237 de ellos, siendo la autoridad líder en 11 de ellos. Las reclamaciones sobre ejercicio de derechos, en 2018 se han recibido 1.784 peticiones, de las que 191 fueron por derecho al olvido.

Mar España ha explicado que Google y sus servicios suponen 125 de las 191 reclamaciones (65%), seguido de medios de comunicación, con 18 y el 9%; otros buscadores de Internet, con 14 y un 7%; las administraciones públicas y boletines, con 13 reclamaciones y un 6%. En este sentido, la presidenta de la AEPD considera "normal" que Google aglutine el mayor porcentaje, ya que cuenta con "30 millones de usuarios en España".

En 2018, se han dictado 907 resoluciones sancionadoras (434 con sanción económica, 96 con resolución de infracción a administraciones públicas, y 377 apercibimientos). Así, la morosidad y la contratación fraudulenta representaran 3.770.803 euros (29%) y 4.979.200 euros (38%), respectivamente, sobre el total del volumen de sanciones (12.824.454 euros).

Finalmente, la presidenta de la AEPD ha anunciado que prevé publicar el próximo mes

de febrero una instrucción o circular que recoja las conclusiones del informe de la Agencia sobre el tratamiento de datos personales que pueden hacer los partidos políticos de cara a las próximas elecciones. Así, ha apelado a la responsabilidad de las formaciones y ha aclarado que de momento no ha recibido ninguna denuncia por perfilado ideológico.

https://www.europapress.es/sociedad/noticia-aumenta-casi-33-reclamaciones-planteadas-agencia-proteccion-datos-2018-14146-20190125143326.html

---

La AEPD avisa de que la navegación privada o de incógnito no es efectiva para prevenir el seguimiento del dispositivo

MADRID, 7 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD) ha avisado de que la navegación privada o de incógnito no resulta efectiva para prevenir el seguimiento de los dispositivos (móvil, tableta, portátil u ordenador), "proyectando una falsa sensación de seguridad".

Así lo pone de manifiesto la Agencia en su estudio 'Fingerprinting o huella digital del dispositivo', donde aborda esta técnica de identificación y rastreo de los usuarios a través de sus dispositivos y para el que ha analizado más de 14.000 páginas web dirigidas al público español, describiendo las técnicas más utilizadas para realizar ese perfilado.

La huella digital del dispositivo es un conjunto de datos extraídos del dispositivo del usuario que permiten individualizar "de forma unívoca" dicho terminal. "Dado que lo habitual es que las personas no compartan sus equipos, individualizar el terminal supone individualizar a la persona que lo utiliza y, en consecuencia, poder realizar un perfil de la misma", añade.

En este sentido, advierte de que el perfilado no se limita a recopilar y analizar los hábitos de navegación o las búsquedas que realiza, sino a extraer geolocalización, datos de configuración del sistema y las aplicaciones, programas instalados, movimientos del ratón, etc. La combinación de esta y otra información permite confeccionar una huella digital única del dispositivo que lo singulariza y, por lo tanto, diferencia de forma unívoca a cada usuario en internet.

El informe publicado este jueves 7 de febrero, el organismo explica que muchos navegadores tienen la opción de navegación privada o de incógnito, una opción con la que los usuarios "tienen la sensación de que su navegación es segura y no será rastreable".

La AEPD explica en su informe que en esta opción el navegador no guarda información sobre páginas web, ni historial de navegación, caché web, contraseñas, información de formularios, cookies u otros datos de sitios web, y al cerrar la ventana borra del equipo del usuario toda esta información.

"Puede dar la sensación de que la navegación permite que el usuario esté protegido frente al uso de la huella digital, pero es una sensación de falsa seguridad, pues a las técnicas usadas en la confección de la huella les resulta transparente la navegación privada, ya que las características que chequea la huella son las mismas, con navegación privada o sin ella, y el equipo del usuario quedará igualmente individualizado. Así pues, en este sentido, la navegación privada no es efectiva", destaca.

NI INFORMACIÓN NI CONSENTIMIENTO

El informe concluye que "con mucha frecuencia" se emplean estas técnicas para recoger datos del equipo del usuario "sin ofrecerle información y sin solicitarle su consentimiento", y que el conjunto de datos recabados "puede ser tan extenso, o enriquecerse de tal forma, que puede llegar a recoger incluso categorías especiales de datos".

Asimismo, el documento advierte de que, "en la mayoría de los casos", al usuario no

se le proporcionan herramientas para poder evitar "de forma efectiva" la recogida de datos y no se le ofrecen medios para ejercer los derechos establecidos en el Reglamento General de Protección de Datos (RGPD) cuando se recogen o asocian a datos personales.

En este contexto, el organismo que lidera Mar España aconseja que los usuarios utilicen la opción 'Do not track' del navegador, que permite dejar constancia de que se quiere evitar el seguimiento; instalar bloqueadores que permiten eludir la publicidad y el rastreo; deshabilitar el uso de Javascript; alternar entre distintos navegadores o ejecutar el acceso a internet en máquinas virtuales.

En relación con los consejos para la industria, se ofrecen recomendaciones tanto para los desarrolladores de productos y servicios, como para aquellas entidades que explotan los datos obtenidos a partir de la huella del dispositivo.

De este modo, en el caso de fabricantes o desarrolladores, deberían incluir en sus productos las opciones necesarias para que el usuario disponga de capacidades para denegar o aceptar, de forma total o parcial, el uso de estas tecnologías. Además, deberían proporcionar al consumidor los equipos con las máximas opciones de privacidad activadas de forma predeterminada, y que sea el propio usuario quien reduzca esas opciones. Como buena práctica, los navegadores podrían tener activada por defecto la opción Do Not Track, según la AEPD.

Para las entidades que quieran explotar datos obtenidos a partir de la huella del dispositivo, la Agencia indica que el responsable del tratamiento debe abstenerse de recabar y tratar la huella y cualquier otro dato asociado a la misma si el usuario no ha dado su consentimiento. Además, agrega que toda aplicación de huella debería chequear el estado de la opción Do Not Track.

En términos generales, el estudio recomienda a las entidades que utilizan el fingerprinting contar con los servicios de un Delegado de Protección de Datos, y deberán realizar un análisis de riesgos de protección de datos relativos a los derechos y libertades de los afectados.

"Si de dicho análisis se deriva que el nivel de riesgo es elevado, será entonces obligada la realización de una Evaluación de Impacto para la Protección de Datos (EIPD) para establecer las medidas necesarias que garanticen la protección de los derechos de los usuarios", concluye.

https://www.europapress.es/sociedad/noticia-aepd-avisa-navegacion-privada-incognito-no-efectiva-prevenir-seguimiento-dispositivo-20190207130227.html

---

AEPD inicia el trámite de audiencia sobre la Circular del tratamiento de datos de opiniones políticas por los partidos

MADRID, 12 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD) ha iniciado el trámite de audiencia para recabar la opinión de los interesados acerca del proyecto de Circular sobre el tratamiento de datos relativos a opiniones políticas por parte de los partidos.

Así lo ha dado a conocer este martes 12 de febrero la Agencia, que ha explicado que el texto se realiza tras la aprobación de la Disposición final tercera de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, que modifica la Ley Orgánica del Régimen Electoral General añadiendo el artículo 58 bis.

En concreto, la elaboración y publicación de este proyecto de Circular, que consta de una parte expositiva, diez artículos y una disposición final, se lleva a cabo tras la publicación por parte de la AEPD de un informe jurídico en el que analizaba el tratamiento de datos personales relativos a opiniones políticas por los partidos.

"Dada la tipología de los datos que se tratarían y que existe un alto riesgo para los derechos y libertades de las personas, el borrador de Circular establece, entre otras garantías, la obligación de consultar a la AEPD antes de proceder al tratamiento de datos a no ser que el partido político justifique que ha adoptado medidas para mitigar los riesgos", ha indicado la Agencia.

En este caso, la AEPD ha detallado que se deberá remitir a la Agencia el análisis de riesgos y la evaluación de impacto realizada junto a la justificación de las medidas adoptadas. "Todo ello sin perjuicio de cualquier otra que estime el responsable del tratamiento y las que puedan exigir otros órganos en el ámbito de sus competencias, como la Junta Electoral Central, el Tribunal de Cuentas, el Ministerio del Interior y, en último término, el Tribunal Constitucional", ha recalcado.

El objetivo del proyecto de Circular es fijar los criterios a los que responderá la actuación de la AEPD en la aplicación de la normativa de protección de datos. En ese sentido, interpreta el citado artículo 58 bis conforme a lo establecido en la Constitución Española y en el Reglamento UE 2016/169, y de modo que no conculque derechos fundamentales como el derecho a la protección de datos de carácter personal reconocido en el artículo 18.4, el derecho a la libertad ideológica del artículo 16, la libertad de expresión e información del artículo 20 o el derecho a la participación política del artículo 23.

Finalmente, ha informado de que las contribuciones al texto publicado podrán remitirse hasta el día 5 de marzo de 2019 a través del correo electrónico **circularpartidos@aepd.es**.

https://www.europapress.es/sociedad/noticia-aepd-inicia-tramite-audiencia-circular-tratamiento-datos-opiniones-politicas-partidos-20190212130213.html

---

Facua denuncia a Epic Games ante Protección de Datos por una posible filtración de datos de usuarios de Fortnite

MADRID, 13 (EUROPA PRESS)

Facua-Consumidores en Acción ha presentado una denuncia contra la empresa estadounidense Epic Games ante la Agencia Española de Protección de Datos (AEPD) por una posible filtración de datos de usuarios de su videojuego Fortnite.

La empresa de ciberseguridad CheckPoint ha desvelado que existen una serie de vulnerabilidades en el sistema del videojuego que permiten que terceros puedan acceder a información personal de los usuarios, incluyendo datos bancarios, y escuchar conversaciones privadas que mantengan dentro del juego.

"De esta forma, habría sido suficiente con que el jugador hubiera sido víctima de phishing, es decir, que hubiera pinchado en un enlace fraudulento que simulaba ser del videojuego, para que toda su información estuviera expuesta, debido a un fallo relacionado con los tokens (identificadores únicos) de acceso de su cuenta", ha explicado la organización.

En este sentido, Facua ha recordado que el Reglamento Europeo 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, recoge que los datos personales deben ser "tratados de tal manera que se garantice una seguridad adecuada", incluyendo "la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental".

Asimismo, ha apuntado que el artículo 6 de la misma normativaestablece que dicho tratamiento sólo será lícito si "el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos", entre otros.

Igualmente, ha destacado que el artículo 32 del Reglamento recoge que "el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", entre otras, "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento".

La asociación también manifiesta que, "teniendo en cuenta el alto número de posibles afectados al ser Fortnite un videojuego de alcance mundial, la infracción de la normativa de protección de datos posee una gran envergadura, que la AEPD debería tener en cuenta a la hora de fijar una sanción".

El Reglamento 2016/679 establece que las multas se impondrán, entre otros factores, teniendo en cuenta "la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido", según recuerda Facua.

Finalmente, señala que recoge como cantidades a aplicar "20.000.000 de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".

https://www.europapress.es/sociedad/noticia-facua-denuncia-epic-games-proteccion-datos-posible-filtracion-datos-usuarios-fortnite-20190213124333.html

La OCU pide a Protección de Datos que investigue a Apple por el tratamiento de datos personales de sus aplicaciones

MADRID, 15 (EUROPA PRESS)

La Organización de Consumidores y Usuarios (OCU) ha solicitado formalmente a la Agencia Española de Protección de Datos (AEPD) la apertura de un procedimiento de investigación a Apple para comprobar si la compañía cumple con la normativa en vigor en materia de tratamiento de datos personales de sus aplicaciones, para que, en su caso, se le impongan las correspondientes sanciones.

"Según se ha sabido recientemente, algunas aplicaciones que Apple pone al servicio de los usuarios a través de App Store han estado utilizando una herramienta que permite registrar los movimientos y datos de los consumidores, incluyendo la captura de las pantallas de sus móviles", ha indicado la OCU.

En este sentido, la organización ha señalado que, "a pesar de que supuestamente todas las aplicaciones que se publican en la App Store deben seguir la política de privacidad de Apple, ninguna de las aplicaciones indicadas muestra claramente en sus políticas que grabaran la pantalla del usuario, ni contaban con el permiso explícito para hacer este tipo de registro".

A su juicio, Apple debería revisar "de manera más eficiente" el cumplimiento de la política de privacidad por parte de las aplicaciones que forman parte de su App Store, así como "controlar mejor" su cumplimiento.

Por último, la Organización de Consumidores cree que la compañía debería ser sancionada en caso de que se demuestre que alguna de sus aplicaciones ha recopilado y utilizado información de sus usuarios sin su consentimiento.

https://www.europapress.es/sociedad/noticia-ocu-pide-proteccion-datos-investigue-apple-tratamiento-datos-personales-aplicaciones-20190215125733.html

---

Juristas y usuarios de Internet piden al Defensor que recurra al TC el tratamiento de datos por parte de partidos

MADRID, 25 (EUROPA PRESS)

Un grupo de juristas y cuatro organizaciones de defensa de los derechos digitales han presentado este lunes 25 de febrero al Defensor del Pueblo una solicitud de interposición de recurso de inconstitucionalidad ante el Tribunal Constitucional (TC) contra la Ley de Protección de Datos que permite el tratamiento de datos personales obtenidos en webs y redes sociales por parte de los partidos políticos.

"Es una ley --la de Protección de Datos Personales-- que pretende proteger los datos personales se incorpora una reforma que hace todo lo contrario, que permite elaborar perfiles en base a opiniones políticas y que ha desdibujado totalmente la Ley Orgánica de Protección de Datos", ha explicado a los medios de comunicación José Luis Piñar Mañas, exdirector de la Agencia Española de Protección de Datos, que respalda la solicitud.

El Defensor del Pueblo tiene de plazo para decidir si plantea el recurso de inconstitucionalidad hasta el próximo 6 de marzo, es decir, tres meses después de la publicación de la ley en el Boletín Oficial del Estado y de la entrada en vigor de la norma. Las Cortes Generales deberán disolverse antes del 5 de marzo con motivo de la convocatoria de elecciones generales 28 de abril.

La Plataforma para la Defensa de la Libertad de Información (PDLI), que apoya e impulsar la petición, ha destacado que esta norma incorpora mediante su disposición final tercera, un artículo 58 bis en la Ley Electoral sobre el uso de tecnologías e Internet con fines de propaganda electoral.

Según dicho artículo, los "partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral". Además, prevé que "el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial".

Piñar Mañas, abogado y catedrático de Derecho Administrativo en la Universidad CEU San Pablo, ha tachado de "desafortunada" la reforma de la Ley Orgánica del Régimen Electoral General (LOREG) a través de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales aprobada con un 93% de apoyo parlamentario.

Asimismo, el jurista ha insistido en que "el artículo 58. Bis de la LOREG tal como está en la Ley dice lo que dice" y ha añadido que "permite recabar sin consentimiento de los ciudadanos sus opiniones políticas por parte de los partidos, con un alcance que va más allá del contenido esencial del derecho a la protección de datos que protege el artículo 18.4 de la Constitución". Para los impulsores de esta petición al Defensor del Pueblo, este precepto "viola" el artículo 18.4 de la Carta Marga.

Preguntado por el proceso parlamentario de la norma, Piñar Mañas ha criticado que "se ha evitado cualquier tramitación técnica más allá del debate mínimo que se ha llevado a cabo en las Cortes" y ha argumentado que "no hay dictamen del Consejo de Estado ni de la Agencia de Protección de Datos ni del Consejo del Poder Judicial".

"No ha participado nadie que tenga relevancia en el mundo de la Protección de datos

salvo, por su puesto, el legislador. Creemos que ha sido una norma que no sabemos si es que ha pasado desapercibida o se ha aprobado conscientemente lo que se estaba aprobando", ha recalcado.

De cara a los distintos procesos electorales que tendrán lugar en España, Piñar Mañas ha asegurado que serán distintas para los ciudadanos en función del "uso que hagan los partidos políticos", pero ha insistido que se trata de "una herramienta muy potente" para las formaciones para "tener muy fichados a los ciudadanos".

En este sentido, Piñar Mañas ha detallado que la campaña electoral podría desarrollarse con "perfilado de los ciudadanos, segmentación de las campañas, elaboración de listas negras". "Luego, puede condicionar", ha indicado, para después recordar que la ley permite ejercer el derecho de oposición.

LISTAS NEGRAS

Carlos Sánchez Almeida, abogado y director legal de la PDLI, ha señalado que con este proyecto, "más allá de la molestia que supone recibir propaganda electoral en WhatsApp", el problema es que posibilita que los partidos políticos "elaboren listas negras de los ciudadanos en razón de su ideología". "Este es el gran peligro y queremos que haya una declaración del TC anulando este precepto", ha zanjado.

"Creemos que es muy importante no solo que se presente el recurso por parte del Defensor del Pueblo, sino que el propio tribunal suspenda la ejecución de esta norma que se ha incrustado en la Ley de Protección de Datos para modificar la LOREG", ha recalcado Borja Adsuara Varela, abogado y profesor de Derecho Digital en el Centro Universitario Villanueva.

Han impulsado esta solicitud Borja Adsuara Varela, abogado y profesor de Derecho Digital en el Centro Universitario Villanueva; José Luis Piñar Mañas, abogado y catedrático de Derecho Administrativo en la Universidad CEU San Pablo; Jorge García Herrero y Elena Gil González, abogados de Secuoya Group; Víctor Domingo Prieto, presidente de la Asociación de Internautas; y Miguel Pérez Subías, presidente de la Asociación de Usuarios de Internet.

También han promovido esta petición Virginia Pérez Alonso, presidenta de la Plataforma en Defensa de la Libertad de Información (PDLI); Rodolfo Tesone Mendizábal, presidente de la Asociación de Expertos Nacionales de la Abogacía Digital (ENATIC); Ofelia Tejerina Rodríguez, abogada de la AI; Carlos Sánchez Almeida, abogado de la PDLI; Cecilia Álvarez Rigaudias, abogada y delegada de Protección de Datos; y Lorenzo Cotino Hueso, catedrático de Derecho Constitucional de la Universidad de Valencia.

https://www.abc.es/tecnologia/redes/abci-juristas-y-usuarios-internet-piden-defensor-recurra-tratamiento-datos-parte-partidos-201902252156_noticia.html

---

Asociación pro DD. HH. pide al Defensor que recurra al TC la norma que permite recoger opiniones políticas en Internet

MADRID, 4 (EUROPA PRESS)

La Asociación Española Pro Derechos Humanos (AEPDH) ha solicitado al Defensor del Pueblo a que recurra ante el Tribunal Constitucional la norma que permite la recopilación de datos personales relativos a las opiniones políticas de las personas por parte de los partidos políticos en el marco de sus actividades electorales.

La asociación ha celebrado este lunes 4 de marzo un desayuno informativo para informar sobre la solicitud que ha presentado ante el Defensor del Pueblo para que interponga un recurso de inconstitucionalidad contra el artículo 58 bis 1 de la Ley Orgánica de Régimen Electoral (LOREG), que se incluyó a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Disposición Final Tercera punto Dos).

Junto a la solicitud registrada el pasado 8 de febrero ante institución que dirige Francisco Fernández Marugán en funciones, la asociación presentó un dictamen jurídico sobre la constitucionalidad del artículo, elaborado por el catedrático emérito de Derecho Constitucional Diego López Garrido.

Según las conclusiones del dictamen, recogido por Europa Press, el nuevo artículo 58 bis.1 de la LOREG contempla la recopilación por los partidos políticos de datos sobre opiniones políticas de las personas, lo que "vacía de contenido en esta materia el derecho a la protección de datos (art. 18.4 de la Constitución española)".

Asimismo, indica que la recopilación de datos personales sobre opiniones políticas por las formaciones políticas "vulnera el derecho a la protección de datos, en cuanto desapodera a la persona del control sobre dichos datos, especialmente sensibles, cuyo tratamiento está prohibido en la legislación europea y española sobre protección de datos personales".

En este sentido, destaca que la recopilación de datos sobre opiniones políticas, "concepto de gran amplitud, es una amenaza para algo tan íntimo como la ideología, especialmente protegida por el art. 16.1 de la Constitución Española (CE), que 'garantiza la libertad ideológica'".

Por otro lado, advierte de que la tecnología informática y digital actual "permite aumentar la amenaza" al derecho a la intimidad y la protección de datos personales cuando se poseen datos sobre opiniones políticas. "El caso reciente de Facebook y Cambridge Analytica pone manifiesto la manipulación a que puede estar sometida la opinión ideológica de millones de personas", apostilla.

Además, critica que el art. 58 bis.1 de la LOREG no exige el consentimiento de la persona para la recopilación de sus datos por los partidos políticos, "lo que agrava la vulneración por dicho precepto del art. 18.4 Constitución".

"Según el Tribunal Constitucional, la Constitución (art. 18.4) ampara todos los datos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico (sentencia 292/2000, fto.jco. 6). Esto ocurre con la posesión y tratamiento por los partidos de las opiniones políticas de las personas a cuyos datos accedan", argumenta.

Por último, señala que permite la recopilación de datos cuando "se ofrezcan garantías

adecuadas", pero "no explicita qué se quiere decir con esa expresión". "Ello lesiona el contenido esencial del derecho a la protección de datos (STC.11/1981), que no puede rebasar el legislador (art. 53.1 CE), y también se opone al principio de Seguridad Jurídica que establece el art.9 de la CE", concluye.

https://www.europapress.es/sociedad/noticia-asociacion-pro-ddhh-pide-defensor-recurra-tc-norma-permite-recoger-opiniones-politicas-internet-20190304173213.html

---

El Defensor recurre al TC la norma que permite a los partidos recoger opiniones políticas en Internet

MADRID, 5 (EUROPA PRESS)

El Defensor del Pueblo ha interpuesto un recurso de inconstitucionalidad ante el Tribunal Constitucional (TC) contra la norma que permite la recopilación de datos personales relativos a las opiniones políticas de las personas en redes sociales por parte de los partidos políticos en el marco de sus actividades electorales.

De este modo, la institución ha recurrido al TC el artículo 58 bis.1 de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, incorporado a esta por la disposición final tercera, punto dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, una iniciativa legislativa que comenzó su tramitación con el PP en el Gobierno.

Desde la sociedad civil, un grupo de juristas y organizaciones de defensa de los derechos digitales han presentado en las últimas semanas al Defensor del Pueblo una solicitud de interposición de recurso ante el alto tribunal, que deberá decidir si paraliza esta disposición de cara a las elecciones generales del 28 de abril, las primeras en las que en principio estaría vigente esta medida.

"El Defensor del Pueblo (e.f.) ha hecho uso de la legitimación que le confiere el artículo 162.1 de la Constitución Española, y ha interpuesto recurso de inconstitucionalidad contra el precepto de la mencionada ley --por considerar que a través del mismo se vulneran los artículos 9.3, 16, 18.4, 23.1 y 53.1 de la Constitución--, en los términos que se concretan en la demanda que ha sido presentada ante el Tribunal Constitucional", comunica Francisco Fernández Marugán a los solicitantes en su escrito, al que ha tenido acceso Europa Press.

El polémico artículo '58 bis' establece que "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".

Asimismo, "los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral".

En este sentido, el Defensor del Pueblo considera que este precepto vulnera el artículo 16 de la Constitución por el que "se garantiza la libertad ideológica, religiosa y de culto de los individuos y las comunidades sin más limitación, en sus manifestaciones, que la necesaria para el mantenimiento del orden público protegido por la ley".

Entre otros preceptos, la institución cree que este artículo es contrario al artículo 18.4 que establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", así como el 23.1 que recoge que "los ciudadanos tienen el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal".

"Absténganse los partidos políticos de enviar publicidad electoral electrónica hasta que haya sentencia del TC. Cualquier envío ilícito será denunciado ante la Agencia de Protección de Datos y ante los Tribunales de Justicia, pidiendo indemnización", ha advertido en declaraciones a Europa Press el director legal de la Plataforma en Defensa

de la Libertad de Información (PDLI), Carlos Sánchez Almeida.

ENMIENDA DEL PSOE APOYADA POR TODOS LOS GRUPOS DEL CONGRESO

La reforma de la Ley Orgánica de Protección de Datos comenzó su andadura en noviembre de 2017 con el PP en el Gobierno y en su redacción inicial no aparecía la polémica disposición final tercera. Ésta fue introducida un año después, ya con el Ejecutivo de Pedro Sánchez, mediante una enmienda del PSOE que fue apoyada por todos los grupos del Congreso.

En noviembre de 2018, la ley fue aprobada definitivamente en el Pleno del Senado, con el voto en contra de Unidos Podemos, Compromís, Nueva Canarias y Bildu. Por su parte, PSOE y PP rechazaron todas las enmiendas presentadas por Compromís, Ciudadanos, PDeCAT y Unidos Podemos - En Comú Podem - En Marea.

Unidos Podemos - En Comú Podem - En Marea en el Senado había elaborado una Propuesta de Modificación al dictamen del Proyecto de la Ley Orgánica de Protección de Datos para que el artículo se retirase en la Cámara Alta, pero fue rechazada por el resto de grupos parlamentarios. La formación morada anunció entonces que impulsaría su modificación mediante una Proposición de Ley Orgánica y recurriría al Constitucional el redactado, pero no llegó a realizarlo.

https://www.europapress.es/sociedad/noticia-defensor-recurre-tc-norma-permite-partidos-recoger-opiniones-politicas-redes-sociales-20190305145049.html

---

La PDLI, satisfecha por el recurso del Defensor ante el TC contra la recogida de opiniones políticas en Internet

MADRID, 5 (EUROPA PRESS)

La Plataforma en Defensa de la Libertad de Información (PDLI) ha recibido con satisfacción la notificación del Defensor del Pueblo informando de que ha interpuesto recurso de inconstitucionalidad contra la norma que establece que "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".

La institución ha recurrido al TC el artículo 58 bis.1 de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, incorporado a esta por la disposición final tercera, punto dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. La PDLI, junto con juristas expertos en Protección de Datos y otras organizaciones de defensa de los derechos digitales, habían solicitado que lo recurriera.

Para la PDLI, esta decisión del Defensor del Pueblo confirma el "atropello que representa esta norma para los derechos fundamentales al permitir a los partidos recopilar, en páginas web y redes sociales, datos personales vinculados a las opiniones políticas de los ciudadanos para realizar 'perfiles ideológicos' y personalizar la propaganda electoral". "Es decir, acciones de 'microtargeting' análogas a las del escándalo de 'Cambridge Analytica'", ha subrayado.

El riesgo de estas prácticas "va más allá de la molestia del 'spam' político: el mayor peligro está en los usos ilícitos que se pueden hacer por el hecho de tener una lista de personas y sus pensamientos ideológicos en manos de un partido", según ha explicado el director legal de la Plataforma, Carlos Sánchez Almeida.

El Defensor del Pueblo corrobora este enfoque al considerar que esta ley vulnera los artículos de la Constitución 9.3 (principio de legalidad), 16 (derecho a la libertad ideológica), 18.4 (derecho a la protección de datos personales), 23.1 (derecho a la participación política) y 53.1 (los derechos fundamentales son vinculantes para todos los Poderes Públicos).

https://www.europapress.es/sociedad/noticia-pdli-satisfecha-recurso-defensor-tc-contra-recogida-opiniones-politicas-internet-20190305183025.html

---

El Defensor del Pueblo afirma que las "limitaciones legales" al spam electoral deben ser "contundentes" y "efectivas"

MADRID, 6 (EUROPA PRESS)

El Defensor del Pueblo considera que las "garantías normativas y las limitaciones legales" deben ser "contundentes, precisas y efectivas" cuando se trate de la recopilación o tratamiento de los datos personales relativos a opiniones políticas que puedan llevar a cabo los partidos políticos en el marco de sus actividades electorales.

Así lo expresa el Defensor del Pueblo en funciones, Francisco Fernández Marugán, en el recurso de inconstitucionalidad que ha presentado ante el Tribunal Constitucional (TC) contra el artículo 58 bis.1 de la de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, incorporado a esta por la disposición final tercera, punto dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Según establece el polémico artículo, "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".

"La posibilidad, o más bien la certeza como acredita el todavía reciente asunto de Cambridge Analytica, de la utilización de estas técnicas (Big Data) para modular, cuando no manipular, opiniones políticas evidencia la necesidad de que las garantías normativas y las limitaciones legales sean contundentes, precisas y efectivas", argumenta el Defensor.

En los fundamentos jurídicos de su recurso, Fernández Marugán pone el foco en las "indeterminadas garantías adecuadas" y en que el legislador "no establece" en el precepto ahora recurrido "cuáles sean esas garantías, ni siquiera los criterios para determinarlas, ni el vehículo normativo que deba contenerlas, ni la autoridad o poder público que deba establecerlas ni, menos aún, referencia alguna a los derechos de los titulares de los datos ni al modo y condiciones en que estos puedan ejercitarlos".

En este sentido, el Defensor del Pueblo en funciones advierte de que "de este modo cualquier dato personal relativo a opiniones políticas, aún siendo un dato sensible especialmente protegido, puede ser objeto de tratamiento sin que hubiera sido aportado para este fin, o sin que su titular lo consienta, o sin que tenga noticia de su tratamiento ni de su finalidad y sin que sepa en qué condiciones puede ejercer sus derechos de oposición y cancelación".

"Todo es posible al no haber precisado el legislador como debía, por mor del artículo 53.1 de la Constitución, en qué consisten y cuáles son esas 'garantías adecuadas'", recalca Fernández Marugán, para después añadir que ello propicia una situación de "evidente" inseguridad jurídica contraria al artículo 9.3 de la Constitución.

Asimismo, el Defensor del Pueblo señala que, en el contexto tecnológico actual, este precepto afecta también al derecho a la libertad ideológica (artículo 16) y al derecho a la participación política (artículo 23.1).

Fernández Marugán comienza su argumentación poniendo de relieve que la sociedad digital tiene como consecuencia que los ciudadanos están generando "continuamente" información personal (actividad, localización, contactos, contenido, intereses, consumo, etc), que se encuentra en "fuentes accesibles" como las redes sociales, o se recopilan

"directamente" en sus dispositivos.

Usando técnicas de Big Data, según destaca el Defensor, se puede recoger "todo ese gran volumen" de datos y tratarlo. "El objeto de dicho análisis puede ser el perfilado del individuo dentro de una categoría, es decir, como perteneciente a un colectivo y así ofrecer productos y servicios orientados a un grupo social o económico", apunta, para después agregar que "también puede ir más lejos, hasta perfilar a cada individuo como un elemento singular".

Este recurso de inconstitucionalidad es el fruto de varias quejas provenientes de la sociedad civil. Un grupo de juristas y organizaciones de defensa de los derechos humanos y también de los derechos digitales presentaron en las últimas semanas al Defensor del Pueblo una solicitud de interposición de recurso ante el alto tribunal.

Entre los solicitantes se halla la Asociación Pro Derechos Humanos de España (APDHE) que este miércoles ha ofrecido una rueda de prensa para valorar el recurso del Defensor. Así, el presidente de la organización, Hernán Hormazábal, ha explicado que el precepto "vulnera claramente la Constitución" y específicamente los artículos 16 (libertad ideológica) y 18 que limita el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos.

Por su parte, el vocal de la asociación Antoni Farriols ha recordado que este artículo 58 bis1. les produjo una "sorpresa increíblemente fuerte y desagradable", mientras que el catedrático de Derecho Constitucional Diego López Garrido ha afirmado que se trata de "un cuerpo extraño" dentro de una "muy buena ley". "Permite que pasen cosas como Cambridge Analytica", ha subrayado.

López Garrido, autor del dictamen que acompañaba a la solicitud que presentó la APDHE ante el Defensor, ha señalado que esperan que el TC "no tarde" en fallar al respecto ya que se trata de un tema que "está afectando de forma decisiva a los procesos electorales" y ha destacado que la Junta Electoral Central debería "tomar muy en consideración" el asunto.

https://www.europapress.es/sociedad/noticia-defensor-pueblo-afirma-limitaciones-legales-spam-electoral-deben-ser-contundentes-efectivas-20190306142445.html

---

Los partidos políticos deberán consultar a la AEPD con tres semanas de antelación si quieren usar 'spam político'

MADRID, 11 (EUROPA PRESS)

Los partidos políticos deberán consultar a la Agencia Española de Protección de Datos (AEPD), con una antelación mínima de tres semanas al inicio de la campaña electoral, antes de proceder al tratamiento de datos personales para el envío de propaganda electoral para los procesos del 28 de abril y el 26 de mayo.

Así se recoge en la Circular de la AEPD sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores, que ha sido publicada este lunes 11 de marzo en el Boletín Oficial del Estado (BOE) y entrará en vigor el día siguiente al de su publicación.

La Circular desarrolla el artículo 58 bis 1 de la LOREG, contra el que el Defensor del Pueblo ha interpuesto un recurso de inconstitucionalidad. El Alto Tribunal deberá decidir ahora si suspende cautelarmente esta aplicación ante las dudas sobre la constitucionalidad del precepto, mientras falla sobre la cuestión.

En cualquier caso, la Circular de la AEPD fija los criterios conforme a los que va a actuar la Agencia en la aplicación de la normativa de protección de datos respecto al tratamiento relativo a opiniones políticas por los partidos al amparo del artículo 58 bis de la LOREG, con el marco del Reglamento General de Protección de Datos (RGPD) y conforme a lo establecido en la Constitución Española.

En concreto, se establece la obligación de consultar a la AEPD antes de proceder al tratamiento de datos a no ser que el responsable justifique que ha adoptado medidas para mitigar los riesgos. En ese caso, deberá remitir el análisis de riesgos y la evaluación de impacto realizada junto a la justificación de las medidas adoptadas. La solicitud de consulta a la AEPD o, en su defecto, la remisión de esa documentación deberá realizarse al menos 14 semanas antes del inicio del periodo electoral.

No obstante, al no ser posible cumplir dicho plazo para los procesos electorales del 28 de abril y de 26 de mayo de 2019, se ha introducido una disposición transitoria que fija el plazo en tres semanas antes del comienzo de la campaña electoral.

En relación con el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y contratación de propaganda electoral en redes sociales, los datos personales que vayan a ser usados por los partidos políticos para el envío de propaganda electoral (números de teléfono, correo electrónico u otros similares) deberán haber sido obtenidos "lícitamente" y deberán corresponder a personas que puedan ejercer su derecho al voto en el ámbito de la circunscripción que se corresponda con el proceso electoral al que se presenten.

La Agencia señala que en los envíos que se realicen deberá constar su carácter electoral y la identidad del remitente. Asimismo, deberá facilitarse "de un modo sencillo y gratuito" el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición".

En caso de ejercicio del derecho de oposición, los datos personales dejarán de ser tratados para el envío de propaganda electoral mientras el afectado no preste su consentimiento expreso, según el texto de la Circular, recogido por Europa Press.

El texto mantiene que "sólo" podrán recopilarse las opiniones políticas que hayan sido "libremente expresadas" por ellas mismas en el ejercicio de sus derechos a la libertad ideológica y a la libertad de expresión reconocidos en los artículos 16 y 20 de la Constitución Española.

En este sentido, apunta que "en ningún caso" podrán tratarse otro tipo de datos personales a partir de los que, "aplicando tecnologías como las de tratamiento masivo de datos o las de inteligencia artificial, se puede llegar a inferir la ideología política de una persona".

Asimismo, las "únicas fuentes" de las que se pueden obtener los datos personales sobre opiniones políticas son las webs y otras fuentes que sean "de acceso público", aquellas cuya consulta puede ser realizada "por cualquier persona, quedando excluidas las fuentes en las que el acceso esté restringido a un círculo determinado de personas".

Por último, el texto limita la legitimación a los partidos políticos, en el ámbito de la circunscripción correspondiente al proceso electoral en la que se presenten, a la circunstancia de que resulten proclamados. En caso contrario, al no participar en el procedimiento electoral, perderían la legitimación para el tratamiento de los datos y deberán cesar "inmediatamente "el tratamiento de dichos datos y proceder a su destrucción, salvo que proceda la obligación de bloqueo.

https://www.europapress.es/sociedad/noticia-partidos-politicos-deberan-consultar-aepd-tres-semanas-antelacion-si-quieren-usar-spam-politico-20190311132456.html

---

Lanzan la 'Lista Viernes', una 'Lista Robinson' contra el 'spam electoral' por e-mail y teléfono

MADRID, 11 (EUROPA PRESS)

Secuoya Group, un grupo de profesionales expertos en privacidad y protección de datos ha puesto en marcha la 'Lista Viernes', una página web gratuita similar a la 'Lista Robinson' en la que los ciudadanos pueden inscribirse de forma anónima y manifestar su oposición al 'spam' electoral de los partidos políticos por correo electrónico y teléfono, de cara a los próximos procesos electorales del 28 de abril y el 26 de mayo.

Esta iniciativa ha sido lanzada a raíz de la aprobación del artículo 58 bis.1 de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG), incorporado a esta por la disposición final tercera, punto dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El polémico artículo señala que "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".

Asimismo, según este precepto, los partidos políticos podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral; y el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

Tras la aprobación de esta norma, asociaciones civiles y juristas presentaron al Defensor del Pueblo una solicitud para que interpusiera recurso de inconstitucionalidad contra la reforma de la Ley Orgánica del Régimen Electoral General (LOREG), y la institución que dirige Francisco Fernández Marugán interpuso el recurso el pasado 5 de marzo.

Entre los juristas que presentaron la referida solicitud de hallan dos de los abogados de Secuoya Group, Jorge García Herrero y Elena Gil González. "La 'Lista Viernes' sirve a todos los ciudadanos y sirve también a los partidos políticos. Los partidos tienen la oportunidad de demostrar que les importa nuestra privacidad", ha explicado García Herrero.

Según los impulsores de esta web, este proyecto tiene la "ventaja añadida" del anonimato de las personas que se apunten que "está garantizado por un sistema tecnológico 'doble ciego'". De este modo, los partidos pueden "tachar" de sus bases de datos a los votantes de la 'Lista Viernes', sin tener acceso directo a la base de datos.

Finalmente, Jorge García Herrero ha indicado que Fundación para la Defensa de la Privacidad y los Derechos Digitales --sin ánimo de lucro-- ha preparado una campaña de crowdfunding a través de la plataforma Goteo.org para financiar el funcionamiento de la web.

https://www.europapress.es/sociedad/noticia-lanzan-lista-viernes-lista-robinson-contra-spam-electoral-mail-telefono-20190311142348.html

---

Android permite que gran número de actores monitoricen y obtengan información personal de usuarios, según un estudio

MADRID, 18 (EUROPA PRESS)

El modelo de permisos del sistema operativo Android y de sus apps permite que un gran número de actores puedan monitorizar y obtener información personal de los usuarios a nivel del sistema operativo, según el estudio 'An Analysis of Pre-installed Android Software' ('Análisis del software preinstalado en dispositivos Android') del Instituto IMDEA Networks y la Universidad Carlos III de Madrid.

Según ha informado este lunes la Agencia Española de Protección de Datos (AEPD), que contribuye con la difusión del informe "debido al impacto masivo" que sus resultados tienen en la privacidad y la protección de los datos personales de los ciudadanos, el estudio será presentado en el 41 Edición IEEE Symposium on Security and Privacy.

La institución española ha explicado que el usuario final desconoce la presencia de estos actores en sus terminales Android y las implicaciones que dichas prácticas tienen sobre su privacidad, según se desprende del estudio. Además, la presencia de este software con privilegios de sistema dificulta su eliminación sin ser un usuario experto.

Respecto a otros resultados de la investigación, la AEPD ha apuntado que, aparte de los permisos estándar definidos en Android y bajo control del usuario, los investigadores han identificado "más de 4.845 permisos propietarios o personalizados por los intervinientes en la fabricación de los terminales".

"Este tipo de permisos permite que apps publicadas en Google Play eludan el modelo de permisos de Android para acceder a datos del usuario sin requerir su consentimiento al instalar una nueva app", según ha destallado la Agencia Española de Protección de Datos.

En relación con las apps preinstaladas en los dispositivos, se han identificado más de 1.200 compañías, así como la presencia de más de 11.000 librerías de terceros (SDKs) incluidas en la mismas. "Gran parte de las librerías están relacionadas con servicios de publicidad y monitorización *online* con fines comerciales. Las apps preinstaladas se ejecutan con permisos privilegiados y sin posibilidad, en la mayoría de los casos, de ser desinstaladas del sistema", ha destacado.

Por otro lado, el análisis del comportamiento del 50% de las apps identificadas revela que "una fracción importante de las mismas presenta comportamientos potencialmente maliciosos o no deseados, como muestras de malware, troyanos genéricos o software preinstalado que facilitaría prácticas fraudulentas".

Sobre la información ofrecida al iniciar un nuevo terminal, la AEPD ha señalado que se pone de manifiesto "un déficit de transparencia de las apps y del propio sistema operativo Android al mostrar al usuario una relación de permisos distinta de la real, limitando su capacidad de decisión para gestionar su información personal".

La investigación abarca más de 82.000 apps preinstaladas en más de 1.700 dispositivos Android fabricados por 214 marcas, tiene entre sus objetivos identificar los agentes presentes en el software preinstalado en Android y que utilizan el acceso privilegiado a recursos del sistema para la obtención de datos personales de usuarios.

El informe pretende asimismo revelar los acuerdos comerciales entre vendedores de dispositivos Android y terceros, incluyendo organizaciones especializadas en la

monitorización y rastreo de usuarios y en proporcionar publicidad en Internet; detectar y analizar vulnerabilidades y otras prácticas opacas; y analizar la transparencia en la información proporcionada al usuario.

https://www.europapress.es/sociedad/noticia-android-permite-gran-numero-actores-monitoricen-obtengan-informacion-personal-usuarios-estudio-20190318151404.html

---

La Lista Robinson permite desde hoy a los ciudadanos limitar la recepción de publicidad por sectores económicos

MADRID, 8 (EUROPA PRESS)

La Lista Robinson, el servicio de exclusión publicitaria creado por la Asociación Española de Economía Digital (Adigital), permitirá a partir de ahora a los ciudadanos limitar la recepción de publicidad por sectores económicos.

Así lo ha dado a conocer este lunes 8 de abril Adigital en un acto para presentar las novedades del servicio, gratuito para los ciudadanos, que cuenta con más de 850.000 registrados, y permite gestionar el ejercicio del derecho de oposición del tratamiento de sus datos para fines publicitarios. El encuentro ha tenido lugar en la sede de la Agencia Española de Protección de Datos (AEPD).

El director general de Adigital, José Luis Zimmermann, ha detallado las novedades del servicio, entre las que destaca la posibilidad de que los ciudadanos limiten la recepción de publicidad de forma gratuita no solo por canales (teléfono, SMS, correo electrónico o postal), sino también por sectores publicitarios. Además, se ha creado un nuevo servicio de gestión de reclamaciones de los usuarios.

Preguntado sobre si se ha previsto la posibilidad de exclusión de propaganda política, José Luis Zimmermann ha respondido que no se ha contemplado porque ese aspecto no se halla "entre los fines de la asociación". "No sé si en algún momento en el futuro podría darse algún tipo de colaboración con el sector público", ha planteado.

Por otro lado, la Lista Robinson ofrece otra novedad para las empresas y es que incluye un nuevo sistema de consulta del servicio sin coste para pymes y autónomos hasta los 30.000 registros anuales. Se realiza a través de una nueva API, que ha incorporado un proceso de cifrado y pseudonimización de datos mejorado.

Según establece la nueva Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) en su artículo 23, las empresas que pretenden realizar comunicaciones de mercadotecnia directa deben consultar los sistemas de exclusión publicitaria previamente, excluyendo así de sus comunicaciones los datos de los afectados que hubieran manifestado su oposición o negativa a las mismas. No será necesario realizar la consulta cuando el afectado haya prestado su consentimiento expreso a la empresa en cuestión para recibir la comunicación.

En el marco de la presentación, la directora de la Agencia Española de Protección de Datos (AEPD), Mar España, ha defendido la utilidad de esta herramienta, que ha calificado como "un buen servicio público". Así, ha afirmado que espera que 2019 acabe con "un mayor número de usuarios y una sistematización de las pymes que se adhieren a la consulta de este tipo de servicio".

"Es un servicio en el que ganan todos. Gana la empresa porque se asegura la certeza de los ciudadanos consumidores que no estén inscritos en la Lista Robinson; y gana la sociedad en su conjunto", ha recalcado la directora de la AEPD, que ha añadido que el reto pasa por dar a conocer a todas las empresas la existencia de esta herramienta.

La presidenta de Adigital, Carina Szpilka, ha señalado que la Lista Robinson es "un ejercicio de autorregulación por el compromiso de la empresas para este uso responsable" y ha indicado que la actualización del servicio viene motivada por la necesidad de adaptación a la nueva regulación de datos personales, pero también de "adaptación a los tiempos".

En este sentido, Szpilka ha manifestado que se trata de un sistema "con una tecnología más sofisticada", donde se ha invertido en la seguridad en la trasmisión de la información y en la facilidad en el uso del sistema. "Lo que queremos es que los más de 800.000 ciudadanos que ya están adscritos a la lista se sientan protegidos, pero que también sea fácil para las empresas consultar quiénes están adheridos", ha apostillado.

La Lista Robinson, que nació en 1993 como una herramienta de autorregulación que permitía a los usuarios oponerse al envío de publicidad, ya cuenta con más de 800.000 registrados. Las últimas cifras de Adigital, determinan que en 2017 se dieron de alta casi 60.000 usuarios, mientras que en 2018 se superaron los 250.000, un 400% más que en el año anterior. "Sospechamos un aumento de altas importante en 2019", ha afirmado Zimmermann que cree que el servicio podría cerrar el curso con un millón de usuarios.

https://www.europapress.es/sociedad/noticia-lista-robinson-permite-hoy-ciudadanos-limitar-recepcion-publicidad-sectores-economicos-20190408120602.html

---

La tecnología permite a ONG como Cruz Roja y MSF salvar y mejorar vidas mediante el uso de datos

MADRID, 20 (EUROPA PRESS)

Los datos personales suelen ser actualidad por las malas prácticas en su recogida, almacenamiento y tratamiento, sobre todo, por parte de empresas. El caso Cambridge Analytica, que destapó la filtración y uso con fines de propaganda política de los datos de al menos 87 millones de usuarios de Facebook sin la debida autorización, puso en el punto de mira la protección de los datos personales.

En un contexto global donde los tratamientos de Big Data analizan grandes volúmenes de datos y las aplicaciones móviles que se utilizan a diario los recogen, las 'app' instaladas en cualquier dispositivo móvil pueden acceder a la identidad, los contactos, la ubicación, los archivos multimedia, entre otra mucha información. No obstante, la recogida de estos datos puede servir no solo para mejorar las condiciones de vida de las personas sino también puede llegar a salvarlas.

Con la popularización de los teléfonos móviles, las organizaciones sin ánimo de lucro han comenzado a desarrollar su labor de ayuda a la sociedad sirviéndose de los datos. Así, Cruz Roja ha adaptado su servicio de teleasistencia, nacido hace tres décadas, convirtiéndolo en Teleasistencia móvil.

En torno a 120.000 personas utilizan este servicio en sus distintas versiones, que asiste personas mayores; personas con discapacidad auditiva, física y/o visual; personas convalecientes de accidente u operación; personas con deterioro cognitivo; mujeres víctimas de violencia de género, etc.

"La eclosión de los smartphones nos permitió convertir un terminal, que en principio estaba pensado para hablar por teléfono, enviar datos y acceder a internet, en un equipo que es capaz de cuidar a personas que tienen algún tipo de dificultad", señala a Europa Press el director de Servicios Tecnológicos Digitales de Cruz Roja, Carlos Capataz.

En este sentido, Capataz asegura que estas herramientas de teleasistencia son las que "más datos generan", fundamentalmente, de localizaciones, y detalla que registran en torno a 10 millones de posiciones mensuales.

De este modo, señala que no se trata de un pulsador de alarma, sino que cuando el usuario se incorpora al servicio se recoge "información detallada" como el nombre y apellidos, las dolencias que pueda tener, vecinos que se puedan movilizar en una situación de emergencia, e incluso, dónde está la llave de paso del gas. "Información muy, muy amplia que en una situación de emergencia el operador prácticamente no tiene que preguntar al usuario qué es lo que ocurre o a quién puede pedir ayuda", subraya.

Respecto a la protección de los datos, Capataz destaca que los servicios jurídicos de Cruz Roja son "muy exquisitos" en ese cumplimiento del Reglamento General de Protección de Datos (RGPD) y que la organización quiere "ir más allá" en esta materia.

Así, aparte de anonimizar los datos, Cruz Roja apuesta por desarrollar sus propios sistemas. "Cuando un fabricante nos ofrece una tecnología para implementar somos muy celosos de que esa información quede albergada en nuestros sistemas. Ellos dicen: en la nube. Y yo les digo: ¿de quién es esa nube? A mí me gustan las nubes de la Cruz Roja", argumenta.

"Aunque sea información anónima y aunque ese acceso fuese totalmente legal, los datos son lo que vale dinero hoy en día y somos muy celosos de que no se moneticen los datos de los usuarios, aunque se salven los aspectos legales de quitar nombre apellidos", subraya, para después agregar que en la ONG procuran ser "muy rigurosos" y "muy exquisitos".

Capataz considera fundamental que las personas confíen en ellos: "La información la vamos a usar sólo para ayudar", recalca el directivo de Cruz Roja, que pone de manifiesto la importancia de que las herramientas no sean de uso común. "Las nuestras son profesionales, desarrolladas por nosotros y para nosotros, y están ubicadas en nuestro sistema", subraya.

TECNOLOGÍA AL SERVICIO DE LOS PACIENTES

Por otro lado, el uso de la tecnología aplicada a la salud y el desarrollo de aplicaciones va en aumento a nivel global, por ejemplo, registros médicos electrónicos, aplicaciones móviles, telemedicina, drones, robots, análisis de Big Data, biométricas, etc. "MSF reconoce las posibilidades que ofrece la tecnología y estamos aprendiendo a aprovecharlas en beneficio de nuestros pacientes", indican a Europa Press desde Médicos Sin Fronteras (MSF).

En este sentido, la ONG explica que está trabajando en sistemas electrónicos de registro de datos y en el desarrollo de algunas aplicaciones que le permitan mejorar su atención a las personas más desfavorecidas.

En concreto, detalla que dos aplicaciones que está empezando a utilizar son eCare, que sirve para ayudar a diagnosticar y tratar algunas de las enfermedades más recurrentes en los menores de 5 años a nivel de atención primaria; y KOBO, una plataforma móvil de compilación de datos para la realización de encuestas nutricionales para conocer el estado nutricional de un grupo de población.

Preguntada sobre qué datos recopila y cómo se tratan, la organización sin ánimo de lucro asegura que "los datos médicos que recopila MSF son los estrictamente necesarios" para el cuidado y tratamiento de los pacientes y para la gestión de sus proyectos. "Es importante limitar claramente el objetivo para el que se recogen los datos y el tiempo durante el que se guardarán con ese único propósito", recalca.

eCare y KOBO no incluyen ningún dato personal que pueda identificar al paciente, comenta MSF, que añade que eCare, sirve "únicamente para monitorear la aplicación de un protocolo médico, y en el caso de KOBO, los datos están gestionados por un comité ético que valida los contenidos y una vez finalizada la encuesta los datos son agregados y se eliminan los detalles".

"La política de MSF para la protección de datos médicos es muy estricta para asegurar la protección del paciente y exige manejar los datos médicos de pacientes y comunidades de forma responsable, respetando la confidencialidad de los datos médicos, la privacidad y la integridad de los pacientes, la ética de médica, la legislación, las reglas y las prácticas", aclara MSF.

En este contexto, la doctora en Ingeniería Informática, investigadora y directora del Máster Universitario en Seguridad TIC de la Universidad Europea, María Teresa Villalba, señala a Europa Press que las ONG o entidades sin ánimo de lucro que usen o traten datos personales a través de sus apps móviles deben tener en cuenta que "tienen una responsabilidad en la protección de los derechos y libertades de las personas de las que tratan sus datos".

"No cumplir con esa responsabilidad, puede ocasionar un daño importante no sólo a los individuos, sino a la sociedad, sobre todo si tratan categorías especiales de datos o datos de colectivos vulnerables", detalla la experta.

Desde la Agencia Española de Protección de Datos (AEPD), organismo que dirige Mar España, indican que la designación del Delegado de Protección de Datos, tanto si es obligatorio como si la organización lo asume de forma voluntaria, "aporta confianza a la ONG", y recuerdan que puede ser una persona interna o externa.

Finalmente, la institución aclara que, "en lo que se refiere al Reglamento General de Protección de Datos (RGPD), a las entidades sin ánimo de lucro que efectúen tratamientos de datos personales a través de aplicaciones móviles, ya sea de sus socios u otros colectivos de personas implicadas en su actividad, se les aplican las mismas obligaciones que a cualquier organización".

https://www.europapress.es/epsocial/cooperacion-desarrollo/noticia-cuando-correcto-uso-datos-ayuda-mejorar-salvar-vidas-20190420130954.html

---

Protección de Datos recibe casi 50 reclamaciones por publicidad electoral de partidos políticos

MADRID, 26 (EUROPA PRESS)

La Agencia Española de Protección de Datos (AEPD) ha recibido cerca de 50 reclamaciones por publicidad electoral de partidos políticos, de ellas, "hay una referencia escasísima" al polémico artículo 58 bis de la Ley de Régimen Electoral General (LOREG) sobre la utilización de medios tecnológicos y datos personales en las actividades electorales.

Así lo han indicado a Europa Press fuentes de la institución que dirige Mar España y que han destallado que estas reclamaciones se encuentran en fase de análisis, es decir, que todavía no han sido ni admitidas a trámite ni desestimadas.

El artículo señala que la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

De este modo, la ley permite a los partidos políticos, coaliciones y agrupaciones electorales utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

Según la norma, el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

El pasado mes de marzo, el Tribunal Constitucional (TC) admitió a trámite el recurso presentado por el Defensor del Pueblo contra el artículo de la Ley de Régimen Electoral General (LOREG) que permite la recopilación de datos personales relativos a las opiniones políticas de las personas en redes sociales por parte de los partidos políticos en el marco de sus actividades electorales.

https://www.europapress.es/sociedad/noticia-proteccion-datos-recibe-casi-50-reclamaciones-publicidad-electoral-partidos-politicos-20190426141005.html

---

Crecen casi un 33% las reclamaciones presentadas ante Protección de Datos en 2018 hasta las 14.146

MADRID, 21 (EUROPA PRESS)

Las reclamaciones presentadas ante la Agencia Española de Protección de Datos (AEPD) durante 2018 se incrementaron un 32,8% hasta alcanzar las 14.146, y en el primer año de aplicación del Reglamento General de Protección de Datos (RGPD) -- desde el 25 de mayo de 2018 al 15 de mayo de 2019-- se han presentado ante un total de 14.397 reclamaciones.

Así lo ha dado a conocer la institución, que ha publicado este martes 21 de mayo su Memoria 2018, donde recoge las actividades realizadas en el ejercicio de referencia, las cifras de gestión, las tendencias destacadas, las decisiones y procedimientos más relevantes del año, y un análisis de los retos presentes y futuros.

En cuanto a la temática, las reclamaciones corresponden a inserción indebida en ficheros de morosidad (16%), videovigilancia (11%), servicios de Internet (10%), reclamación de deudas (10%), Administración Pública (7%), sanidad (7%), publicidad -excepto spam- (5%), comercios, transporte y hostelería (5%), entidades financieras/acreedoras (4%) y publicidad a través de e-mail o teléfono móvil (4%).

Respecto a las reclamaciones resueltas con respuesta satisfactoria tras haberlas remitido al responsable o al delegado de protección de datos (DPD), la AEPD ha indicado que se han producido 863 durante 2018 y 2.079 hasta el 15 de mayo de 2019. Así, dos de cada tres quejas que se envían al responsable o al DPD se resuelven de forma satisfactoria para el particular.

Además, la mitad de las reclamaciones admitidas en la Agencia se resuelven en una media de 100 días, sin tener que esperar los más de 200 días de media del modelo anterior. Por otro lado, el traslado de la reclamación al responsable o DPD no implica necesariamente que no se vayan a realizar actuaciones inspectoras a posteriori, ya que la Agencia tiene potestad para investigar los mecanismos establecidos por la empresa. De hecho, un 13% de esas 863 reclamaciones (110) están en proceso de investigación.

En cuanto a los casos con otras autoridades europeas (sistema coordinado), de los casi 400 casos analizados, en 2018 la Agencia se ha personado como interesada en 237 de ellos, siendo autoridad líder en 11. Desde el 25 de mayo de 2018 al 15 de mayo de 2019, la Agencia ha analizado 1.026 casos procedentes de otras autoridades europeas, actuando como interesada en 539 de ellos y siendo autoridad líder en 18.

Respecto a las reclamaciones sobre ejercicio de derechos, durante 2018 se han resuelto 1.784 peticiones en la Agencia. De ellas, casi 200 (191) corresponden a reclamaciones por derecho al olvido. La proporción estimadas/desestimadas de estas 191 tutelas/reclamaciones es prácticamente de un 50%.

Sobre las entidades reclamadas, Google y sus servicios aglutinan 125 de las 191 (65%), 18 a medios de comunicación (9%), 14 a otros buscadores de Internet (7%), 13 corresponden a Administraciones Públicas y boletines (6%), cifras que se completan con un apartado de peticiones a 'Otras entidades'.

BRECHAS DE SEGURIDAD

Durante 2018 se han puesto en marcha procedimientos para la gestión de las notificaciones de brechas de seguridad y evaluaciones de impacto. Desde el 25 mayo

de 2018 hasta el 31 de diciembre, se atendieron 44 consultas previas sobre evaluaciones de impacto y se recibieron un total de 547 notificaciones de quiebras de seguridad.

Según la Agencia, tras el análisis y la clasificación de estas últimas, un total de 16 se han remitido a la Subdirección General de Inspección de Datos, que afectaban a datos de salud, menores, ideología política, y tratamientos masivos de datos.

Del 25 de mayo de 2018 al 15 de mayo de este año) se han recibido 966 notificaciones de brecha de seguridad. Un 72% de ellas indican que se ha comprometido la confidencialidad de los datos personales y un 36% indican compromiso de la disponibilidad.

En este caso, más del 53% de las notificaciones de brechas de seguridad tienen como origen un contexto externo e intencionado y, de ellas, el 44% fueron a consecuencia de ciberincidentes mediante algún tipo de técnicas de hacking, malware o mediante phishing. Respecto a los aspectos procedimentales, el análisis de los incidentes de seguridad notificados apunta a que el 31% de éstos se deben a la pérdida o robo de dispositivos o documentación.

En 2018 se han dictado 907 resoluciones sancionadoras (434 con sanción económica, 96 con resolución de infracción a Administraciones Públicas y 377 apercibimientos). En lo referente a la temática de los procedimientos sancionadores, destacan, por este orden: Contratación fraudulenta, inserción indebida en ficheros de morosidad, videovigilancia, spam (LSSI), publicidad (excepto spam), servicios de Internet, reclamación de deudas, telecomunicaciones, Administración Pública y sanidad.

En el caso de las dos principales (morosidad y contratación fraudulenta), representan, respectivamente, 3.770.803 euros (29%) y 4.979.200 euros (38%) sobre el total del volumen de sanciones (12.824.454 euros). Con respecto al año anterior, crecen las reclamaciones por contratación fraudulenta y descienden levemente las de morosidad.

Estas dos áreas acumulan un 67% del volumen total de sanciones impuestas en 2018. En cuanto a la temática de las infracciones por parte de las AAPP, estas declaraciones de infracción están motivadas, entre otros casos, por publicación de datos desproporcionados en páginas web de Administraciones locales, accesos indebidos a datos de terceros por parte de trabajadores públicos o incumplimiento de medidas de seguridad.

En cuanto a las cifras de Delegados de protección de datos (DPD) notificados ante la Agencia, en 2018 se tramitó la inscripción de 20.043 Delegados de Protección de Datos (17.296 del sector privado y 2.747 del sector público). Cuando ha transcurrido casi un año completo desde la aplicación del RGPD, se han comunicado 34.193 DPDs (29.908 del sector privado y 4.285 del sector público).

En lo relativo a los servicios de ayuda que presta la Agencia para la adaptación al Reglamento, la Herramienta Facilita RGPD, orientada a pymes que realizan tratamientos de bajo riesgo, ha sido utilizada en 2018 en más de 150.000 ocasiones, una cifra que se amplía a 170.000 a fecha 15 de mayo de 2019.

Por otro lado, el canal Informa RGPD, que presta soporte en aquellas dudas y cuestiones que puedan derivarse de la aplicación del RGPD, ha atendido en 2018 un total de 4.116 consultas. Hasta el 15 de mayo de 2019, esa cifra se ha ampliado a las 4.607. Las consultas más usuales son las relativas a la obligatoriedad de nombrar un DPD, cuestiones sobre videovigilancia o la utilización de la huella y datos biométricos

como medidas de control de acceso y horario del trabajo.

Se han planteado 1.564 cuestiones ante el área de menores de la Agencia, lo que supone un incremento de casi el 75% con respecto a 2017 (895). En cuanto a la temática de las consultas, las más frecuentes son la toma de imágenes y si es necesario el consentimiento para ello, tanto en las aulas, como en eventos escolares y extraescolares (campamentos, excursiones, funciones teatrales, etc.), así como quién debe otorgar el consentimiento para tratar datos personales de menores cuando los padres están separados.

https://www.europapress.es/sociedad/noticia-crecen-casi-33-reclamaciones-presentadas-proteccion-datos-2018-14146-20190521140616.html

---

El Reglamento Europeo de Protección de Datos cumple hoy un año de aplicación con más reclamaciones y concienciación

MADRID, 25 (EUROPA PRESS)

El Reglamento General de Protección de Datos (RGDP) cumple un año de aplicación efectiva este sábado 25 de mayo, un periodo que ha traído consigo cambios en la mentalidad y en la forma de actuar de las empresas y de los ciudadanos, con un incremento en el número de reclamaciones.

Así lo explica a Europa Press el coordinador de la Unidad de Apoyo y Relaciones Institucionales de la Agencia Española de Protección de Datos (AEPD), Jesús Rubí, que se muestra "satisfecho porque hay una gran conciencia de que el sistema ha cambiado y de que hay que adaptarse a un modelo distinto".

Asimismo, Jesús Rubí hace hincapié en que el último Barómetro del CIS de 2018 reveló que "a un 76% de los españoles, tres de cada cuatro, les empieza a preocupar mucho o bastante la protección de datos personales, aunque, a pesar de esa preocupación, no hacen un ejercicio tan activo de los derechos que tienen, pero sí es una preocupación creciente".

Según asegura Rubí, "las consultas han llegado a cerca de 750.000 en el año 2018 y se han incrementado también las reclamaciones a partir de la aplicación efectiva del reglamento". Desde el 25 de mayo de 2018 al 15 de mayo de 2019 se han presentado ante la AEPD un total de 14.397 reclamaciones.

De cara a la implementación del RGPD, el 85% de las empresas tomaron medidas para actualizar los permisos, según un estudio elaborado por HubSpot, recogido por Entelgy. "Esto hizo que desaparecieran numerosos envíos masivos de email marketing", la compañía.

Una de las novedades que trajo consigo la nueva normativa fue la sanción. Así, se prevé sancionar las infracciones con multas que pueden alcanzar hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa con respecto al ejercicio anterior.

Como recuerda Entelgy, la primera gran multa por incumplimiento de la normativa en toda Europa llegó seis meses después de la entrada en vigor del reglamento, cuando una organización portuguesa fue sancionada con 400.000 euros por permitir el acceso indebido a datos de los usuarios sin su consentimiento expreso. Además, una compañía alemana y otra austriaca fueron otras de las sancionadas, con una multa que superaba los 24.000 euros en total.

"Se ha producido un salto en la forma de cumplir de las empresas y en la proactividad en el ejercicio de derechos de los ciudadanos", destaca Rubí, que añade que en 2018 también ha habido "una información pública que ha lesionado de una manera importante la imagen sobre tratamiento de datos de importantes prestadores de servicios en Internet y esto también contribuye a todo este fenómeno".

A su juicio, "se ha iniciado un proceso de una mayor consolidación en lo que se refiere al derecho de la protección de datos, tanto por parte de quienes tienen que cumplir como por parte de quienes tienen que hacer efectivos y exigir el cumplimento de sus derechos".

INCREMENTO DE CONSULTAS

Con motivo del primer aniversario de aplicación de la norma europea, Rubí reconoce que la Agencia ha detectado en este periodo "un problema general" a la hora de adaptarse al nuevo modelo y de conocer cómo se aplica. "Una vez que ha empezado a aplicarse el Reglamento se ha producido un incremento importante de las consultas que han planteado las empresas y ciudadanos, que en este último caso se han multiplicado", señala.

En concreto, el coordinador de la Unidad de Apoyo y Relaciones Institucionales de la AEPD detalla que las consultas más habituales sobre el RGPD han tenido que ver con la aplicación de la norma cuando las empresas son de fuera de la Unión Europea o con la elaboración de perfiles en Internet siguiendo la navegación de los usuarios.

Otro "volumen importante" de preguntas han estado relacionadas, según indica Rubí, con "los derechos de acceso y supresión; y el derecho a la portabilidad, es decir, conseguir trasladar la información que tenía alguien que trataba los datos a un nuevo prestador de servicios". "Hay un volumen relevante también de consultas sobre el derecho al olvido en relación con los motores de búsqueda en Internet", agrega. Durante 2018 se han resuelto 1.784 peticiones en la Agencia. De ellas, 191 corresponden a reclamaciones por derecho al olvido.

PERIODO DE "TRANSICIÓN" DE DOS AÑOS

El reglamento se aprobó y entró en vigor en mayo de 2016, pero comenzó a aplicarse de manera obligatoria el 25 de mayo de 2018, según recuerda Rubí, que añade que en este tiempo la Agencia ha desarrollado un "abanico amplísimo" de actividades informativas y ha ofrecido "muchísimas orientaciones, guías, herramientas prácticas", como Facilita_ RDPD. "Es un cambio de mentalidad muy importante, de ahí que hayamos hecho toda esta actividad. En principio, estamos satisfechos del resultado que ha empezado a tener", asegura.

Finalmente, Jesús Rubí cree en España aún no se ha instalado "esa cultura" y, en consecuencia, "hay que seguir desarrollando actuaciones, insistiendo desde el punto de vista práctico en cómo ir resolviendo las dudas que se están suscitando sobre la aplicación del reglamento y en cómo ir desarrollado y actualizando herramientas".

https://www.europapress.es/sociedad/noticia-ano-aplicacion-rgpd-mas-reclamaciones-mayor-concienciacion-20190524120423.html

---

AEPD prepara un procedimiento de urgencia para reclamar la retirada de Internet de videos de ciberacoso o *sexting*

MADRID, 25 (EUROPA PRESS)

La directora de la Agencia Española de Protección de Datos (AEPD), Mar España, ha asegurado que espera poder presentar "antes del verano" un nuevo servicio que permite la tramitación urgente de las reclamaciones antes la Agencia para la retirada de videos en Internet en casos de ciberacoso o sexting antes de que se vuelvan virales.

Así, ha pedido a los ciudadanos que, antes de reenviar sin consentimiento un vídeo de índole sexual, "sean conscientes de las responsabilidades penales" y del "destrozo de una vida o de una familia" que puede suponer esa acción. El pasado mes de mayo una empleada de Iveco se quitó tras difundirse un vídeo de contenido sexual suyo entre sus compañeros de trabajo.

"Seremos mucho mejores como ciudadanos y como país", ha explicado este martes la directora del órgano estatal, Mar España, en la inauguración de la XI Sesión Anual Abierta de la Agencia Española de Protección de Datos (AEPD) que se celebra en el Centro de Conferencias Pablo VI de Madrid. La jornada ha sido inaugurada por la ministra de Justicia en funciones, Dolores Delgado.

Según ha recordado España, la AEPD está trabajando con los Ministerios del Interior y Educación, la Delegación de Violencia de Género, la Fiscalía General del Estado y con el Consejo General de la Abogacía para que cuando una víctima acuda a pedir asesoramiento a un abogado o a denunciar ante las autoridades sean informados de que pueden acudir a la Agencia para evitar que el vídeo se vuelva viral y se retire en 24 horas.

La Agencia prevé poner en marcha un cauce extraordinario y urgente en su sede electrónica para la presentación de reclamaciones por este tipo de contenidos. Tras valorar dicha reclamación, la Agencia podría, en su caso, enviar un requerimiento de medidas cautelares en la vía administrativa a la empresa de internet o el responsable para que retiren de forma inmediata esos contenidos.

"Espero que antes del verano podamos presentar este nuevo servicio a la sociedad", ha detallado España, que ha adelantado que cuando la Agencia reciba la reclamación esta irá por un cauce "extraordinario y urgente".

UNA CUESTIÓN DE SALUD LABORAL

Por otro lado, la directora ha destacado que la AEPD también está trabajando con el Ministerio de Trabajo para difundir, dentro del Plan de Riesgos Laborales y en el marco de la formación en materia de prevención, que cuando se produzcan conductas de este tipo en el seno de la empresa se debe mandar una notificación urgente para "intentar acotar y eliminar el video antes de que el daño sea irreparable". "Afecta a la salud laboral", ha recalcado.

En este sentido, Mar España ha aseverado que "todos" tienen la obligación de denunciar estos casos y que las empresas "no pueden decir" que es un tema personal. "No. En el momento en que el departamento de Recursos Humanos se entere o los propios compañeros tienen la obligación de denunciar", ha insistido.

Durante su intervención, la directora de la AEPD se ha felicitado por que "por fin" se ha logrado regular la obligación de que las administraciones educativas tienen que

implementar en el currículo el uso responsable de Internet y las nuevas tecnologías, a través de la inclusión del Artículo 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

"Podemos evitar muchísimos problemas de ciberacoso, de suicidios escolares, de violencia de género, responsabilidad de los menores cuando tengamos sistematizado ese uso curricular con absoluta normalidad", ha defendido España, quien ha añadido que los materiales catalogados por etapas pedagógicas llegarán a "8 millones de escolares".

Por otra parte, España ha indicado que la Agencia ha acometido un "profundo" proceso de reorganización interna para adaptarse el Reglamento y a la aplicación de la Ley Orgánica 3/2018 destacando, entre otros aspectos, y ha destacado el intenso trabajo de sensibilización dirigido a responsables y encargados de tratamiento sobre sus obligaciones.

Asimismo, ha anunciado la próxima publicación de la actualización de la Guía de cookies, realizada en colaboración con el sector de la publicidad *online*, y otras iniciativas como una herramienta de análisis de riesgos y evaluaciones de impacto, la Guía de protección de datos en el ámbito de las relaciones laborales, y las Guías para pacientes y usuarios de la sanidad y para profesionales sanitarios.

El principio de responsabilidad activa y los mecanismos de supervisión de las autoridades de control para una actuación homogénea ante los desafíos globales; el papel del delegado de protección de datos tras un año de aplicación del Reglamento; los criterios respecto de las figuras del responsable, encargado y corresponsable del tratamiento; la vinculación entre el derecho a la protección de datos de carácter personal y otros derechos fundamentales y libertades que conforman la sociedad democrática, o la gestión del riesgo tecnológico en los tratamientos de datos han sido otros de los temas abordados durante la XI Sesión Anual Abierta de la AEPD.

https://www.europapress.es/epsocial/derechos-humanos/noticia-aepd-prepara-procedimiento-urgencia-reclamar-retirada-internet-videos-ciberacoso-sexting-20190625135645.html