Gestión de datos: reglas éticas y legislación

EN LA ERA DEL *BIG DATA* LAS EMPRESAS SE ENFRENTAN AL RETO DE MANEJAR DATOS QUE PUEDAN PERMITIR LA IDENTIFICACIÓN DEL SUJETO. ¿CÓMO HACERLO?

IDOIA PORTILLA

Las empresas han acumulado a lo largo del tiempo gran cantidad de datos: cifras de ventas, datos contables, facturación por cliente, pagos a trabajadores, pedidos a proveedores... En algunos casos, este registro se ha realizado cumpliendo obligaciones tributarias o legales, o simplemente para el seguimiento del negocio. Algunas organizaciones han completado esta información con estudios del sector o estudios cualitativos y cuantitativos pilotados por institutos de investigación de mercados. Con toda esta información y, sobre todo, gracias a un buen análisis de la misma, algunas organizaciones han podido descubrir nuevas oportunidades de negocio, abrirse a nuevos mercados y, en general, mejorar la posición frente a los competidores.

En la era actual, además de esta información, las empresas pueden acumular fácilmente datos provenientes de internet, por ejemplo, de redes sociales. Estas plataformas permiten, entre otras muchas cosas, que el público pueda dirigirse directamente a la empresa. De este modo, internet puede ofrecer a la empresa gran cantidad de información sobre los consumidores y sus intereses, como un servicio de atención al cliente de 24 horas/365 días al año.

Y la tecnología avanza ofreciendo nuevas fuentes de datos. Los móviles, los sensores digitales o los sistemas gps están registrando información automáticamente. Estamos *en la era del big data*: grandes volúmenes de datos, generados a gran velocidad y de formatos variados. Si además son veraces y ofrecen valor para el negocio, hablamos de *smart data*, de información con respuestas útiles para nuestro negocio.

Entre toda esta masa ingente de datos, las empresas se enfrentan al reto de manejar datos que pueden permitir la identificación del sujeto: los *datos personales*. Estos pueden ser una dirección de correo electrónico, la imagen de un rostro, un mensaje de voz, la localización geográfica obtenida a través de un móvil... Su principal característica es que exigen mayores medidas de protección por esta capacidad para identificar a la persona. De ellos se ocupan leyes como el Reglamento General de Protección de datos (RGPD) europeo, que se aplica desde mayo de 2018, o la ley española de protección de datos, aprobada en diciembre del mismo año.

A continuación comentaremos algunas reglas que nos pueden ayudar a almacenar y gestionar los datos de manera ética, sin olvidar algunas obligaciones que nos señala el marco legal, con especial atención a España.

La legislación no nos impide acumular información pero, si se trata de datos personales, nos exige protegerlos adecuadamente

¿PODEMOS ACUMULAR DATOS PERSONALES?

La legislación no nos impide acumular información pero, si se trata de datos personales, nos exige protegerlos adecuadamente. Aquellas empresas que dispongan de este tipo de datos, deberán organizar todo su sistema para cumplir la ley. Y no es una tarea sencilla.

Un aspecto esencial de la protección de datos es que va a requerir la implicación de todo el personal de la empresa. Los datos personales no se limitan a un departamento, sino que están presentes en las diversas áreas de negocio. Por poner ejemplos, en recursos humanos se manejan datos de empleados y potenciales candidatos que han entregado sus currículos; en compras tienen registrados datos de proveedores; en ventas, manejan información que identifica clientes; y en marketing se manejan tanto datos de proveedores de servicios como de clientes. Y cada empresa, con su idiosincrasia, deberá determinar qué datos personales almacena en cada departamento y cómo los está gestionando.

En este punto, el RGPD señala que

la empresa debe adoptar medidas de protección de los datos personales *desde el diseño*. Debe documentar las actividades de tratamiento de datos, identificar a sus responsables, y registrarlo todo para poder evidenciar el cumplimiento de la ley.

Por tanto, dado que se trata de una labor que va a implicar a toda la organización, hay que convencer al conjunto de su personal de la relevancia de una gestión correcta. Como utilizar argumentos legales a veces es complicado, por los términos que se emplean, animamos a trasladar a todos los equipos tres reglas éticas. Son sencillas y respetan la ley, por lo que si se incorporan a la cultura de la empresa, pueden ayudar a implementar los sistemas de protección de datos exigidos. Se trata de las siguientes tres reglas:

Regla 1: *Los datos personales son de cada individuo, no de la organización*.

Aunque los datos personales estén almacenados en nuestros sistemas informáticos o archivadores, no son nuestros y no podemos hacer con ellos lo que queramos. Tenemos los datos porque sus titulares nos han dado su consentimiento

Aunque los datos personales estén almacenados en nuestros sistemas informáticos o archivadores, no son nuestros

a que los guardemos; solo podemos utilizar esta información para aquello que nos haya dado su permiso; y no podemos compartir sus datos con otros sin su autorización.

Regla 2. *Almacenar menos datos y menos tiempo supone menos costes y menos riesgos.*

Custodiar datos es costoso por lo que lo ideal es mantener los mínimos posibles y el menor tiempo necesario. Este principio evita la acumulación de información sin tener clara su utilidad. Almacenar datos personales exige recursos de tiempo, personal y dinero. Pero, sobre todo, aumenta los riesgos de una brecha de seguridad. Cuantos menos datos personales retengamos, menores costes y peligros.

Regla 3. *Almacenar solo aquellos datos que ayuden a mejorar nuestros servicios.*

Unido al hecho de evitar acumular por acumular, está el motivo por el que registramos los datos, especialmente los de carácter personal (que pueden identificar a la persona). Si almacenamos información personal, se entiende que es para dar una atención más personalizada a estos sujetos, sean empleados, proveedores o clientes. Es decir, que los datos que almacenamos tienen valor porque permiten dar mejor servicio al público correspondiente.

Poner en práctica esta tercera regla implica que cada departamento debe pensar qué datos tiene y para qué. Por tanto, es la menos sencilla de acatar. Requiere que todos reflexionen sobre los usos de la información y su valor para la gestión. Sin embargo, siendo la regla más compleja, es imprescindible para almacenar solo lo necesario (regla 2) y evitar perjuicios a los titulares de los datos.

El seguimiento de estas reglas permite a cualquier organización gestionar éticamente la información personal que les han cedido sus dueños. A continuación veremos que, además, estas reglas nos ayudan a atender las exigencias de las leyes de protección de datos.

LA LEGISLACIÓN DE PROTECCIÓN DE DATOS PERSONALES

Tal y como hemos señalado al principio, las leyes clave sobre protección de datos en España son el *Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (conocido como Reglamento general de protección de datos y por sus siglas RGPD) y su adaptación a nuestro país, recogida en la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Para su mejor conocimiento, remitimos a la Agencia Española de Protección de Datos (www.aepd.es). A continuación vamos a destacar algunos aspectos relevantes. El RGPD, que se aplica desde ma-

yo de 2018, tiene como propósito dar a los estados europeos unos criterios comunes respecto a la protección de datos personales. De este modo es viable la cesión de información entre empresas con negocios en diversos países, asegurando que se aplican los mismos criterios y las personas tienen los mismos derechos. Dada la creciente internacionalidad de los mercados, esta armonización es una buena noticia para todos.

PRINCIPIOS BÁSICOS

Este reglamento europeo, junto a las leyes nacionales que se derivan de él, parten de seis principios básicos. El primero hace referencia a la *licitud, lealtad y transparencia*. Esto supone que los datos personales se tratan de manera lícita y tras dar información sencilla y clara a sus titulares. En esta misma línea, el segundo principio es la *limitación de la finalidad*: los datos deben recogerse con unos fines determinados, explícitos y legítimos, y no es posible utilizarlos por otros motivos. A esto deberíamos añadir la regla ética de usar los datos para servir mejor.

Volviendo a la legislación, ésta también se rige por los principios de la *minimización de datos* y la *limitación del plazo de conservación*. Por tanto, como hemos visto arriba, se deben recoger los datos mínimos que permitan alcanzar los objetivos y solo se guardarán largos periodos con fines archivísticos den interés general o científicos (históricos, estadísticos...).

Una posibilidad que cita la ley, unida a la minimización y la conservación de los datos, es la seudoanonimización. Si es necesario mantener los datos personales para usos posteriores, la legislación anima a que los datos personales se disgreguen del resto, seudoanimizando los datos. Esto implica separar los datos personales de modo que queden bajo mayor custodia y solo se pueda desanonimizar la información siguiendo un procedimiento establecido y en ciertas circunstancias.

En cuanto a las conservación de los datos, el RGPD destaca que los datos deben ser *exactos y actualizados*, y se debe *conservar de manera segura*. Esto requiere unos sistemas de almacenamiento con medidas de seguridad adecuadas, que deberán ser revisadas y actualizadas periódicamente. Pero, además, si pretendemos que los datos sean actuales, esto solo se puede asegurar dando el control de los mismos a sus titulares. Veamos qué supone esto explicando los derechos con los que cuentan los dueños de los datos.

La legislación se rige por los principios de la *minimización de datos y la limitación del plazo de conservación*

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

El nuevo reglamento de protección de datos ha ampliado los derechos pasando de los conocidos como ARCO (acceso, rectificación, cancelación y oposición) a los que algunos denominan con el acrónimo ARCOPOL: acceso, rectificación, cancelación, supresión o derecho al olvido, portabilidad, oposición y limitación del tratamiento.

Además, muy vinculado al big data y al uso de algoritmos, está el nuevo derecho "a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar" (art.22 del RGPD). Es el caso de la denegación automática de una solicitud de crédito o de contratación de un seguro médico en los que no medie intervención humana y sean los algoritmos los que decidan, en función de los datos personales disponibles. Detrás de esta propuesta puede entenderse que es necesario evitar que el sujeto se vea perjudicado por haber permitido el uso de sus datos personales. Si lo enlazamos a las reglas del punto anterior, se trata de guardar los datos personales que nos permitan dar mejor servicio, es decir, utilizarlos a favor de quien los cede, no en su contra.

Un punto muy importante en es-

te reglamento es que las personas puedan ejercer los derechos ARCOPOL (acceso, rectificación, cancelación, olvido, portabilidad, oposición y limitación del tratamiento). Este ejercicio de los derechos es, además, el modo de asegurarnos de que contamos con datos exactos y actuales. Por tanto, las personas deben poder acceder a sus datos y rectificarlos o borrarlos. Esto implica que las empresas dispongan de plataformas o procedimientos que permitan este control. Recordemos la primera regla ética: "Los datos personales son de cada individuo". Es decir, debemos respetar que ellos puedan hacer con sus datos lo que deseen.

En este apartado, no podemos dejar de lado los problemas que puede tener facilitar el ejercicio de algunos derechos. Es el caso del derecho a la portabilidad de los datos. Permitir esta acción exige a la empresa facilitar todos los datos que tiene de una persona a otra compañía, por ejemplo. Dado el gran número de formatos en los que es posible almacenar información, esta tarea no es técnicamente sencilla. Por tanto, habrá que estar atentos a lo que recomiende la Agencia Española de Protección de Datos sobre este punto.

A estos derechos se suma el *derecho a estar informado*, que también se reconocía en la legislación previa. El RGPD lo que añade es que la información sea clara y sencilla. Algunos expertos han llegado a plantear que sea el departamento de marketing y no el legal quien redacte las explicaciones de cómo se utilizarán los datos. Todo debe ser fácilmente entendible ya que el consentimiento debe unirse a una información concisa y comprensible. Detallemos un poco más este punto.

El consentimiento deber ser una manifestación libre y específica. El sujeto debe actuar afirmativamente

Todos los contenidos deben mostrarse de manera comprensible para un ciudadano medio

EL CONSENTIMIENTO Y LA NECESIDAD DE INFORMAR

En el RGPD, el consentimiento se define como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (art. 4).

El hecho de que sea una manifestación libre y específica implica que no se pueden dejar marcadas casillas ni condicionar la aceptación del consentimiento a la recepción de otros beneficios. Debe ser una acción afirmativa, donde el sujeto debe actuar, marcando una casilla, por ejemplo, que nos autoriza a disponer de sus datos.

Y esta manifestación es informada e inequívoca, es decir, debemos informar bien, con explicaciones sencillas, como hemos indicado anteriormente. Los términos legales no son comprensibles para todo el mundo así que, evitémoslos. Informar implica indicar el nombre de quién controlará los datos, el propósito de la recogida, el tipo de dato que se recoge, el derecho de abandono sin verse perjudicados, y si se cederán o no los datos a terceros, por ejemplo. Todos los contenidos son importantes y deben mostrarse de manera comprensible para un ciudadano medio.

Para completar los contenidos básicos con más información, podemos ayudarnos de una web, por ejemplo, facilitando un enlace a un contenido online o incluso un código QR que remitan a espacios donde pueda leerse todo. Incluso se puede pensar en mensajes grabados sencillos que permitan informar a personas con problemas de visión, o vídeos que compaginen audio e imagen.

Desde la ley, se anima a mostrar los contenidos sobre privacidad y protección de datos en un sistema de "capas" que permita mostrar en un primer nivel aquello más relevante, pero llevando a capas siguientes a quienes quieran saber más. Por ejemplo, una primera capa puede hacer referencia a los derechos y una segunda explicar cómo ejercerlos.

La *finalidad de la recogida de los datos personales* es uno de los aspectos que debe quedar bien claro. Se recomienda una descripción objetivo a objetivo, detallando los posibles usos de manera breve y sencilla y uno a uno. Esta presentación "granular" permite al titular de los datos autorizar solo algunos usos. De esta forma se logra que el consentimiento sea una "manifestación de voluntad libre, específica, informada e inequívoca", como dice el RGPD.

Por parte de la organización, la presentación de la finalidad objetivo a objetivo implica tener muy claros los usos que se darán a los datos. Como comentábamos en la tercera regla ética, esto requiere que cada empleado determine qué datos necesita y para qué. La tarea es compleja pero, como vemos ahora, es esencial para redactar el consentimiento exigido por la ley. En todo caso, recordamos la relevancia ética de reflexionar también sobre cómo ayudará esta información al propio titular de los datos. No olvidemos que debemos servirle mejor y no perjudicarle.

La importancia del obtener el consentimiento es clave, como seguramente todos ya habíamos intuido. Pero, por si alguien aún no está convencido, recordamos que no obtener adecuadamente este consentimiento puede suponer sanciones millonarias. Este es el caso de Google en Francia,

No obtener adecuadamente este consentimiento puede suponer sanciones millonarias

donde el organismo regulador de protección de datos ha sancionado a esta empresa con 50 millones de euros por el incumplimiento del reglamento. Concretamente, por la falta de información clara del uso de la información y englobar en un único consentimiento múltiples propósitos. Es decir, no facilitar el consentimiento informado requerido. Es muy probable que se trate de una sanción ejemplarizante pero, por eso mismo, debemos aprender: cuidemos los consentimientos y la información que ofrecemos.

LOS DATOS DE CATEGORÍAS ESPECIALES

Dentro de los datos personales, se encuentran los denominados "categorías especiales", conocidos en la legislación previa como datos "sensibles". En este grupo tenemos los datos de origen étnico o racial, genéticos, biométricos, de salud, vida y orientación sexuales, convicciones religiosas, afiliación sindical/política o infracciones y condenas penales.

Si nuestra empresa trabaja en un sector donde este tipo de información es relevante, somos un caso especial para la legislación y las exigencias son mayores. En todo caso, vuelve a aplicar todo lo anterior: los datos no son nuestros, sino de las personas; debemos acumular lo mínimo imprescindible y usar los datos en beneficio de su titular. Más aún, mejor tener todo anónimo o agregado.

Supongamos que nuestra empresa pertenece al sector farmacéutico: ¿necesitamos saber los nombres de las personas que sufren cierta enfermedad para darles un buen servicio? Seguramente no. Con saber la frecuencia con que ocurre ésta se puede atender bien las necesidades de los enfermos. Si trabajamos en el área política, tampoco es imprescindible saber qué ha votado cada persona. Conocer el reparto de votantes por secciones censales ofrece ya datos de gran valor para realizar campañas.

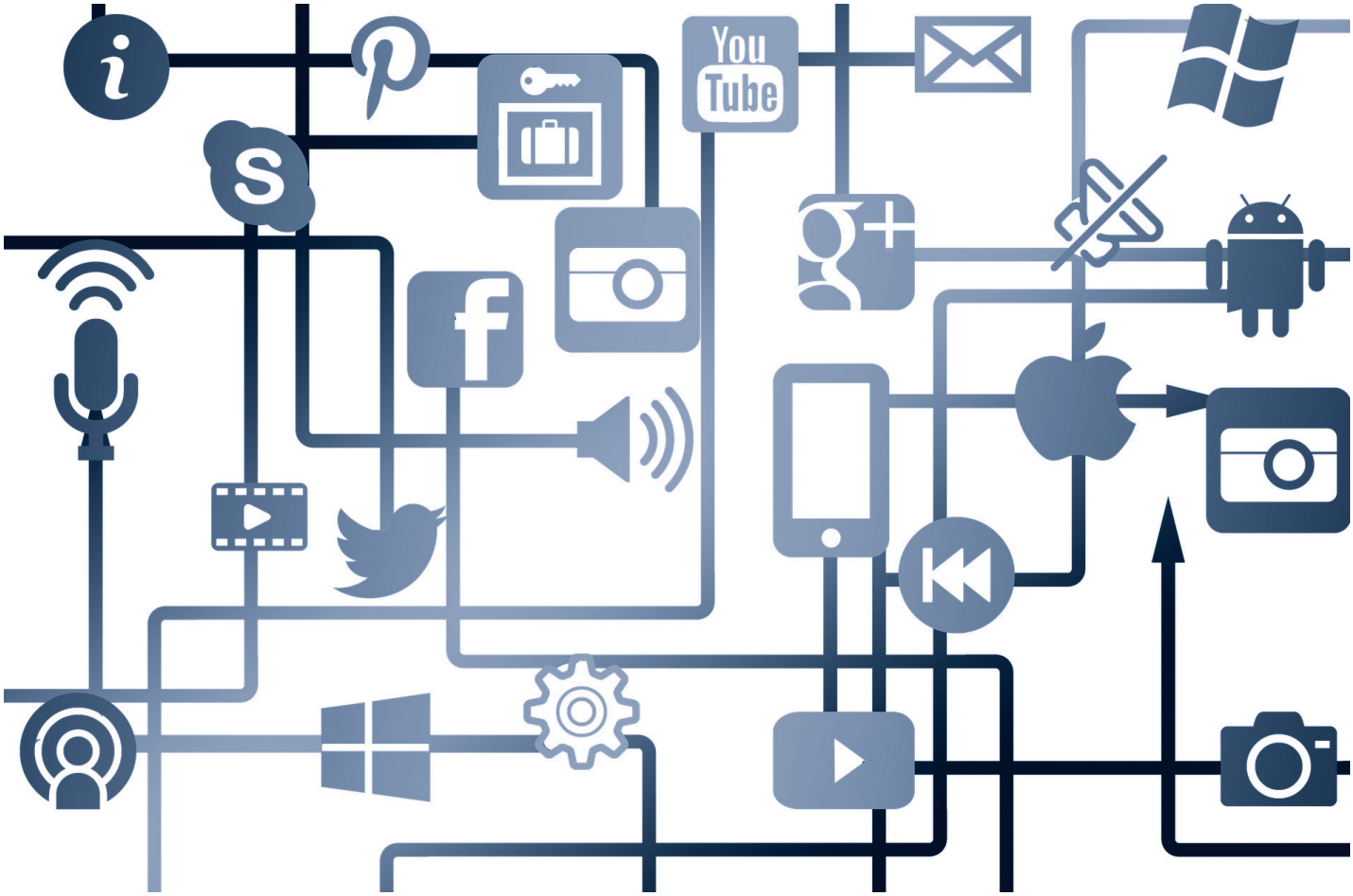
Pero, cuidado. Es bueno que todas las empresas revisen sus ficheros ya que es muy probable que, sin darnos cuenta, hayamos acumulado datos sensibles de nuestros trabajadores, por ejemplo. Podemos tener anotados en sus expedientes enfermedades que han padecido, afiliaciones a sindicatos o incluso creencias religiosas que les han obligado a ciertas bajas o tratamientos. Es decir, que todas las empresas pueden tener datos de categorías sensibles. En estas circunstancias, recomendamos una custodia más cuidada de los datos, con buenas medidas de seguridad y un estricto control de acceso.

LA ÉTICA TAMBIÉN APLICA AL RESTO DE DATOS

La información agregada como la publicada en estudios sectoriales o por los institutos de estadística no permite identificar a personas, por lo que se puede utilizar al igual que se venía haciendo. No le aplica la ley de protección de datos personales si estos no aparecen, es decir, si no es factible identificar a la persona titular.

También se pueden seguir utilizando datos de estudios de mercado como los procedentes de encuestas o paneles. Estas investigaciones pueden incluir información como edad, género o estado civil, pero éstas no permiten identificar al entrevistado. Por tanto, no son datos personales. Estas informaciones podemos guardarlas sin ningún problema, así como datos agregados resultantes de cualquier estudio que describa la población en su conjunto: porcentajes por género, municipio de residencia, situación laboral, etc.

El problema en la era actual es que algunos datos en principio anónimos puede que no lo sean al cruzarse con otros. En la era del big data, fusionar varias bases de datos de personas puede hacer que datos anónimos sobre un mismo sujeto permitan su identificación. Investigaciones como la de Latanya Sweeney en el "Identifiability Project" indi-



can que, conociendo el género, la fecha de nacimiento (día, mes y año) y el código postal, es posible identificar a una persona.

En este punto, vuelve a aplicar el principio de guardar solo lo estrictamente necesario. ¿Necesitamos día, mes y año de nacimiento de una persona? Probablemente no. Lo más habitual es registrar su edad, por ejemplo, y ésta no identifica a una persona en concreto. Si un seguimiento en gps puede señalar dónde vive y trabaja una persona e identificarla, quizás se puede reducir el número de decimales de la localización para que esta no sea tan exacta. Borremos de las bases de datos todo aquello que sea innecesario porque nos ayudará, como hemos dicho, a ahorrar recursos y evitar riesgos. Por tanto, hablemos o no de datos personales, la minimización de la información guardada es siempre lo más recomendable.

Con cualquier tipo de dato, también recomendamos ser éticos en su uso. Utilicemos los datos para dar mejor servicio, guiados por objetivos como lograr que nuestros empleados estén más contentos, atender mejor a nuestros clientes o mejorar la relación con los proveedores.

La ética en el manejo de datos es rentable porque minimiza los datos almacenados en volumen y tiempo. Pero también porque la empresa tendrá mejor reputación

SER ÉTICOS ES BENEFICIOSO PARA LA ORGANIZACIÓN

La ética en el manejo de datos es rentable porque minimiza los datos almacenados en volumen y tiempo, reduciendo los recursos necesarios, es decir, los costes en personal, tiempo y dinero. Pero también es rentable porque una empresa que cuide su gestión de datos tendrá mejor reputación. Aunque justificar con el opuesto no siempre es válido, vamos a recordar la crisis de Facebook y Cambridge Analytics. Estas empresas no fueron transparentes en el uso de los datos personales. No informaron de qué datos se obtenían, con qué propósito ni con quién se compartirían. Su comportamiento incumplió la legislación de protección de datos, además de carecer de ética al no beneficiar en modo alguno al titular de datos, sino buscar su manipulación. Como resultado, la reputación de Facebook se ha visto dañada, obligando a Mark Zuckerberg a dar explicaciones generalizadas, incluso ante el Congreso de Estados Unidos.

Facebook y Cambridge Analytics han demostrado que una marca que realiza un uso inadecuado de los datos personales puede ver dañada su reputación. Pero la repercusión de este caso va mucho más allá. La preocupación por nuestra privacidad y el uso que se hace de nuestros datos ha crecido en todos los grupos sociales.

El impacto del caso de Facebook es importante, pero no es lo único que ha llevado a la sociedad a preocuparse más por el uso que se hace de sus datos. La publicidad personalizada también tiene su parte de culpa. Muchas personas sienten que se viola su privacidad

cuando reciben publicidad de un producto similar al que estaban buscando previamente en internet. En principio se trata de darles mejor información pero ¿se lo hemos explicado correctamente? ¿Nos han pedido que les demos este servicio?

Seguramente no estamos explicando bien cómo se gestiona la publicidad actualmente, con envíos según información de cookies y sistemas similares. Una demostración está en el crecimiento de inscritos a la lista Robinson. Creada en 1993 en España como servicio para solicitar ser excluido de mensajes publicitarios, esta lista tuvo 60.000 altas en 2017, según Adigital, pero alcanzó las 250.000 en 2018. La recepción de publicidad targetizada genera sensación de intrusismo, y las personas tratan de protegerse.

Con la creciente sensibilización ante el uso de los datos, las personas se pensarán más cuándo y a quién ceden información sobre ellos y sus intereses

¿CÓMO DEBEMOS PROCEDER PARA SER ÉTICOS EN EL USO DE DATOS?

La creciente preocupación social por el uso que hace una organización de los datos, especialmente los datos personales, debe ser un acicate para la mejora de la gestión de la información. Reiteramos que hacerlo bien implica reducir costes, pero también dar buena imagen, lo que repercute directamente en la reputación de la empresa y su cuenta de resultados. Mucha gente se siente perseguida por las marcas de manera indiscriminada y no entiende qué ocurre. Es preciso explicar mejor el uso que hacemos de los datos y simplificar el contenido de las políticas de privacidad. Y esto requiere de un esfuerzo oganizacional. Todos los empleados deben determinar qué datos precisan, guardando solo los necesarios, el mínimo tiempo posible y respetando los objetivos para los que fueron recogidos.

Los datos personales precisan especiales medidas de protección y que los sujetos puedan ejercer sus derechos, controlando la información almacenada en la organización. Son suyos. La organización solo los custodia temporalmente para poder dar un buen servicio, así que debemos explicarlo bien para que se sientan ayudados, no perjudicados. Cada vez más, con la creciente sensibilización ante el uso de los datos, las personas se pensarán más cuándo y a quién ceden información sobre ellos y sus intereses. Y solo lo harán a cambio de servicios de valor y a las marcas en las que confíen. Esto exige ética, con tratamientos adecuados de los datos que nos ceden, tomando las medidas de protección debidas y pensando en el beneficio de esas personas •

PARA SABER MÁS: Normativa sobre protección de datos: https://www.aepd.es/normativa/index.html; Portilla, Idoia (2019), "Ante el caso de Facebook y Cambridge Analytica: Buenas prácticas para la creación y uso de bases de datos", en https://opinion.anuncios.com/2018/04/ante-el-caso-de-facebook-y-cambridge-analytica-buenas-pr%C3%A1cticas-para-la-creaci%C3%B3n-y-uso-de-bases-de-d.html