Día Europeo de Protección de Datos 2016

Monográfico de la Asociación Profesional Española de Privacidad

Artículos del Monográfico de APEP

Agencia Española de Protección de Datos: El futuro de la protección de datos.

La protección de datos en Europa estará definida en los próximos años por el nuevo Reglamento General, cuya aprobación definitiva es ya inminente. La revisión del marco legal europeo de protección de datos era una necesidad impuesta por los avances tecnológicos experimentados en los últimos años, el fenómeno de la globalización y los cambios jurídicos e institucionales operados en la Unión Europea. Esa necesidad de renovación no parte de una renuncia al modelo establecido por la todavía vigente Directiva de 1995. Sin perjuicio de que algunas disposiciones de la Directiva sean mejorables y de que fuera también necesario profundizar en la armonización de las legislaciones nacionales, el proceso de reforma ha estado presidido por un consenso general en torno a la idea de que los valores y principios contenidos en la Directiva siguen siendo plenamente válidos. Una vigencia que consagró la inclusión de la protección de datos dentro de la Carta Europea de Derechos Fundamentales y que han avalado algunas recientes decisiones clave del Tribunal de Justicia de la Unión. El nuevo Reglamento nace, por tanto, bajo la premisa de asegurar la continuidad en los principios informadores del modelo europeo de protección de datos, al tiempo que se actualizan los procedimientos y garantías mediante los que se pretenden implantar. Continúa leyendo aquí.

Ricard Martínez, presidente la Asociación Profesional Española de Privacidad (APEP?: El futuro de la privacidad.

El 28 de enero de 2016 marca un momento crucial para el derecho fundamental a la protección de datos y sus profesionales. El Reglamento general de protección de datos, que previsiblemente se aprobara entre marzo y abril, define un escenario nuevo en muchos sentidos profundizando en otros en la experiencia adquirida durante el último decenio. Se trata de una norma de nueva generación orientada a un escenario de innovación tecnológica que percibimos que crece con progresión casi geométrica superando los límites físicos de la Ley de Moore. Las leyes y constituciones de los años 70 se ordenaban a proteger al ciudadano frente al Estado. Muy pronto se percibió que tanto el Convenio 108/1981 como la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos iban a jugar un papel determinante en la orientación del llamado mercado de la privacidad. Continúa leyendo aquí.

Salomé Adroher Biosca: Nuevas tecnologías de la información y comunicación: un nuevo marco legal de protección a la infancia y a la adolescencia.

Las TICS son una *oportunidad* pero también un *riesgo* particularmente, para los menores. Esta doble faceta fue reconocida por el Comité de Derechos del Niño de Naciones Unidas que en sus Recomendaciones a España en 2010 insta a nuestro país a que prosiga "su labor de promover la existencia de medios de comunicación de calidad que contribuyan a la alfabetización digital de los niños, garantice que la televisión pública tome la iniciativa, y ejerza una función de liderazgo en la creación de programas responsables durante las horas de máxima audiencia de los niños, dando prioridad al desarrollo de éstos y no a los beneficios económicos, y contando con la participación de los niños en la elaboración del contenido y el diseño de los programas infantiles, aliente a las empresas que operan en el sector de Internet a que adopten códigos de conducta adecuados, y aliente la capacitación de los niños y los adultos para navegar con seguridad en Internet". Continúa leyendo aquí.

Josep Aragones Salvat: El futuro de la protección de datos.

Ya era hora que los ciudadanos europeos se sientan protegidos por su legislación delante de las organizaciones internacionales que procesan sus datos personales. La determinación de la UE en no dejarse amedrentar por las superpotencias comerciales y normalizar para todos los países de la UE un único reglamento que proteja nuestros derechos vislumbra un objetivo en el cual Europa puede empezar a no sentirse solo como un mercado sino como un proyecto de derecho al servicio de sus ciudadanos. Cuando una denuncia interpuesta en el tribunal europeo contra Facebook, por un simple abogado austríaco, el Sr. Max Schrems, puede provocar la anulación de un acuerdo entre UE y EEUU, quiere decir que la Justicia funciona y que nuestros derechos son respetados. Continúa leyendo aquí.

María Arias Pou: El deber de información en el Reglamento General de Protección de Datos.

Un año más celebramos el Día Europeo de Protección de Datos. Este año nos encuentra a todos revisando el último texto que se ha publicado en relación con el Reglamento General de Protección de Datos, RGPD. Dedicaré este artículo a analizar cómo ha quedado redactado el deber de información al titular de los datos. Hace un año, en esta misma sede, manifesté mi opinión sobre las principales novedades que, en su día, la Propuesta de Reglamento General de Protección de datos recogía en relación con este deber. Algunas de estas novedades se han mantenido en el texto definitivo y otras fueron desechadas ya en la versión de la Propuesta de Reglamento aprobada por el Consejo el pasado 15 de junio de 2015. Continúa leyendo aquí.

Sandra Ausell Roca: La privacidad: un reto transversal para una sociedad de derechos. La sociedad cambia, la tecnología avanza y el derecho siempre les acompaña.

Cada paso que damos en nuestra vida cotidiana es susceptible de generar información. Desde la primera consulta que hacemos al despertar cada mañana a nuestro Smartphone para apagar la alarma y ver el tiempo previsto para ese día, pasando por los registros de las compras realizadas mediante tarjeta bancaria que entregamos junto a la tarjeta de fidelización, – la cual nos permite acumular puntos y conseguir esos

"grandes beneficios o estupendos regalos"-, continuando con las correspondientes llamadas telefónicas profesionales y personales susceptibles de ser grabadas, las consecutivas búsquedas en Google Maps para localizar nuestros destinos a lo largo del día y elegir la ruta más conveniente cada vez, sumado a las decenas de capturas hechas a nuestra imagen recorriendo la ciudad en los transportes públicos o en las vías por las que circulemos, incluso en los pequeños comercios que visitemos; Continúa leyendo aquí.

Javier Cao Avellaneda: El impacto de la notificación de violaciones de seguridad del Nuevo Reglamento.

Como todos los años, toca celebrar en APEP el Día Europeo de Protección de Datos y quiero plantear reflexiones sobre el impacto que puede tener la regulación sobre la obligación de notificar las violaciones de información en materia de protección de datos y sus posibles beneficios. Toda organización que se precie debiera tener control sobre sus sistemas de información. En este sentido, la monitorización del funcionamiento es una actividad básica para la gestión y control de los sistemas de información. Sin embargo, en materia de seguridad esta es una tarea no muy común en muchas grandes organizaciones que siguen como máxima de protección aquello de "*no news, good news*". Este es precisamente uno de los axiomas corporativos que más daño hacen a la gestión de la seguridad de la información, ¿Por qué? Las tres dimensiones de la seguridad no se comportan igual frente a los daños. En cada caso, el proceso de gestión de incidentes requiere acciones muy diferentes según el tipo de amenaza y sobre qué dimensión se produce pero no siempre la ausencia de efectos o daños no implica que no estén ocurriendo cosas. Continúa leyendo aquí.

Sara María Fernández: Legitimación para el tratamiento de datos de clientes con fines de marketing en el nuevo Reglamento Europeo: el fin de los contratos "con casilla".

En el nuevo Reglamento Europeo de Protección de Datos se establece el consentimiento como una de las bases para el tratamiento de datos personales, entendiéndose por tal una declaración o clara acción afirmativa que implique que el titular está de acuerdo con dicho tratamiento. En una primera lectura, esta redacción podría interpretarse como que el tratamiento de los datos de sus clientes con fines de marketing por parte del prestador de un servicio requeriría de esa acción afirmativa por parte del cliente, cuando hasta ahora, el Reglamento

español de Protección de Datos admitía el consentimiento informado, en el que no se requería acción alguna por parte del titular de los datos, y bastaba con un simple preaviso de un mes **(art.14 del RD 1720/2007).**

Sin embargo, el nuevo Reglamento Europeo incorpora el interés legítimo **(art. 6.1 f)** como una de las bases que legitiman el tratamiento de datos, con la condición de que no prevalezcan derechos fundamentales, y que el tratamiento en cuestión responda a las expectativas razonables que hubiera podido tener el titular de los datos, en el momento y habida cuenta del contexto en que fueron recabados. Continúa leyendo aquí.

Ramón Ferri Tormo: El reto de la privacidad en la ciudad inteligente

El Ayuntamiento de Valencia está firmemente comprometido en convertir a Valencia en una ciudad justa y equitativa, centrada en el ciudadano, que mejore continuamente su sostenibilidad y resiliencia aprovechando el conocimiento y los recursos disponibles, especialmente las Tecnologías de la Información y la Comunicación (TIC), para mejorar la calidad de vida, la eficiencia de los servicios urbanos, la innovación y la competitividad sin comprometer las necesidades futuras en aspectos económicos, de gobernanza, sociales y medioambientales. En la medida en que el Ayuntamiento de Valencia avanza a una Administración Abierta, Electrónica y hacia la transparencia se puede hablar de Valencia como una ciudad inteligente que hace uso de los avances tecnológicos para mejorar la calidad de vida de sus habitantes. Continúa leyendo aquí.

Héctor Guzmán Rodríguez: Protección de datos: Mucho pasado, un presente incompleto y la ilusión del futuro.

En este Día Europeo de la Protección de Datos 2016, hablar del futuro de este derecho suena tentador después de los diversos sucesos (jurídicos y no jurídicos) que hemos atestiguado, tan solo en el 2015, por no ir más lejos. En la Unión Europea (EU), la inminente adopción del Reglamento General de Protección de Datos (RGPD), prevista para la primavera de este mismo año, ha traído consigo múltiples reacciones y opiniones que no dejan de alertar sobre los numerosos cambios y retos que esta normativa traerá consigo, tanto para los sujetos obligados como para las autoridades nacionales europeas; sin dejar de mencionar la información sobre los beneficios que dicho Reglamento traería para los ciudadanos y residentes europeos. Continúa leyendo aquí.

Carmen López Belda: La protección de datos y el terrorismo internacional.

Con los recientes atentados producidos en París, Copenhague, África, Oriente Medio, nos cuestionamos de qué forma se puede armonizar la política de Protección de Datos Europea, con la lucha contra la delincuencia organizada y los actos de terrorismo internacional. Sabemos, que los terroristas utilizan en gran medida los viajes en avión para pasar de un país a otro, en principio con total impunidad, y conseguir sus objetivos criminales, bien sea colocando bombas en los aviones, o inmolándose en un espacio público de gran afluencia para causar el mayor número de muertos posible. Esta preocupación de los gobiernos europeos para poder controlar a los pasajeros de vuelos internacionales, impulsó la creación del Registro Europeo de Nombres, que se conoce con las siglas inglesas de PNR (Registro de Datos de los Nombres de los pasajeros), con el objetivo de permitir la localización de sospechosos de cometer actos delictivos graves y organizaciones terroristas internacionales. Continúa leyendo aquí.

Paloma Llaneza: ¿Están sustituyendo los algoritmos el juicio humano? Volar por debajo del radar.

China está implantando un nuevo sistema (Social Credit System "SCS") que permite evaluar la capacidad crediticia de sus ciudadanos, como ya hacen las entidades financieras occidentales con todos nosotros. El sistema ferozmente ambicioso, autoritario, tecnológicamente sofisticado y disruptivo ha sido diseñado, según un documento oficial, como *"un componente importante del sistema de economía de mercado socialista"* ya que *"sus requisitos inherentes fijan la idea de una cultura de sinceridad, lo que permite promover la sinceridad y las virtudes tradicionales".* Esa redacción vaga pero con una gran carga de reproche (¿quién no ha escuchado cuando uno se queja de la vigilancia electrónica "yo es que no tengo nada que ocultar"?) en realidad habla de control de los ciudadanos: con la figura del *"crédito social"* las autoridades chinas planean hacer algo más que conocer la capacidad de endeudarse de sus ciudadanos, quieren evaluar la confiabilidad de los ciudadanos en todas las facetas de su vida. Continúa leyendo aquí.

Esther Mitjans: La múltiple vigilancia en el entorno digital.

Los últimos atentados en París han contribuido más, si cabe, a que baste con que un político invoque la seguridad para acabar con toda discusión o debate sobre la privacidad al considerarla concepto abstracto y poco relevante. A pesar de ello, los usuarios de las redes sociales se siguen quejando de que las tecnologías se utilizan para el control social. Y es cierto, pues los datos masivos, o BIG DATA, permiten que determinadas categorías de personas sean injustamente objeto de sospechas por su perfil o discriminadas por un mal uso de sus datos sensibles. No obstante, también el rastro que dejan estos usuarios en internet les genera riesgos. El propio individuo se convierte también en vigilante de aquellos con los que se comunica. Va dando sus datos personales y siente curiosidad por la información de los otros. Se asume un riesgo tanto frente a los próximos, ya sean familia, amigos o vecinos, como frente a desconocidos. Muchos temen más este control interpersonal que el de las instituciones estatales. Continúa leyendo aquí.

José Leandro Núñez García: Consentimiento... ¿explícito?

El largo proceso que va a llevar, con casi total probabilidad, a la aprobación del nuevo Reglamento europeo de protección de datos, además de servir de práctico recordatorio del complejo procedimiento legislativo de la Unión, ha dado lugar al replanteamiento de algunos de los elementos básicos que, hasta ahora, definían este derecho fundamental. Terminados los trílogos, el texto aprobado por la comisión LIBE el pasado 17 de diciembre refleja los acuerdos alcanzados tras las negociaciones interinstitucionales. Uno de los aspectos en torno a los que giraron las discusiones fue, precisamente, la definición de consentimiento: uno de los pilares del sistema. ¡Ahí es nada! Continúa leyendo aquí.

Ana M. Peiró Peiró y Purificación Ballester Navarro: Pacientes empoderados, TIC y protección de datos en el sistema sanitario.

La práctica de la medicina conlleva tomar decisiones por parte del médico y del paciente en base a una filosofía de la libertad. Sin embargo, no hay, en contra de lo que pudiera parecer, un concepto objetivo de salud o de bienestar, porque en su definición intervienen siempre valores, y éstos no sólo no son homogéneos en las sociedades pluralistas. Se plantea un

problema y es el de saber qué debe entenderse por «mayor beneficio» y quién debe definirlo. Estos quedan, en principio, a la libre gestión de los individuos, de acuerdo con sus peculiares sistemas de valores y proyectos de vida. [1]Para que sea posible, es fundamental que el paciente disponga de la información relevante, completa y no sesgada, mediante un proceso continuo de comunicación. Es preciso que el paciente esté empoderado. De hecho, la OMS considera que el "empoderamiento" es un concepto esencial de la promoción de la salud integrando el fomento de la participación en las decisiones, la pertenencia y contribución a una sociedad plural, respetando a la persona y protegiendo su dignidad. Continúa leyendo aquí.

Alejandro Perales: La vigencia del consentimiento en el futuro de la protección de datos personales.

La aprobación el pasado diciembre en el Parlamento europeo de la propuesta de Reglamento General de Protección de Datos encamina ya esta norma hacia su recta final, que previsiblemente culminará con su aprobación en la primavera de 2016. La opción de recurrir a un Reglamento puede resolver en buena medida el problema de fragmentación normativa derivada de las diferencias en la transposición de las actuales Directivas al ordenamiento jurídico de los diferentes Estados miembros, fuente siempre de inseguridad jurídica; pero suscita también inevitables suspicacias desde países que, como España, disfrutan de un modelo razonablemente garantista y en la "banda alta" de la protección de datos en Europa. Continua leyendo aquí.

Javier Puyol: El proyecto de Reglamento Comunitario de Protección de Datos de Carácter Personal es algo más que una nueva norma.

Ante la perspectiva de su próxima aprobación, cabe afirmar que la aprobación del nuevo Reglamento Comunitario en materia de Protección de Datos, constituye uno de los más importantes procesos legislativos llevados a cabo en la historia jurídica de la Unión Europea. Su periplo legislativo hasta su entrada en vigor, representa un hecho ciertamente singular, novedoso, y que hace referencia al desplazamiento de una ley orgánica española, que de facto queda sin efecto, por una ley europea que regula un derecho fundamental como es "*el habeas data*". Y todo ello, sobre la base de la nueva normativa que se caracteriza por su aplicabilidad directa, no encontrándose, consecuentemente con ello,

necesitada de transposición legislativa nacional, y que en definitiva, supone que sean los propios ciudadanos los que puedan invocar la aplicabilidad esta norma directamente ante cualquier Juzgado o Tribunal. Continúa leyendo aquí.

Raúl Rubio: Privacidad y seguridad, un debate de actualidad.

Puede que el momento actual, el debate entre la seguridad del estado y la privacidad de los ciudadanos se encuentre en su momento más álgido. A raíz de los últimos atentados terroristas, es inevitable que se planteen toda clase de preguntas: ¿se actuó de forma diligente?, ¿qué tipo de información tenían los servicios de inteligencia antes de los atentados? y, sobre todo, ¿qué podemos hacer para evitar que vuelva a pasar?

Es a raíz de esa última pregunta que los Estados Miembros de la Unión Europea se están replanteando la manera en que sus servicios de inteligencia y sus fuerzas y cuerpos de seguridad obtienen la información necesaria para cumplir sus funciones. El actual debate no se centra únicamente en que tengan una mayor dotación económica, sino también de que dispongan de los mecanismos adecuados (tanto jurídicos como técnicos) para dar respuesta a las actuales amenazas a la seguridad de un estado y sus ciudadanos. Continúa leyendo aquí.

Andrés Sanz: Big Open Data y Salud:Un gran poder conlleva una gran responsabilidad.

No sería de recibo publicar mis primeras líneas en esta web sin agradecer a Ricard Martínez, entre otras muchas cosas que le debo, su invitación a escribir unas palabras a modo de reflexión en el Día Europeo de la Protección de Datos.
Centremos, pues, el tema: los conceptos Open Data y Big Data son conocidos para la mayoría de los lectores asiduos de esta web. Ambas herramientas, usadas correctamente, aportan muchísimas más ventajas que inconvenientes; pero lo cortés no quita lo valiente, y resulta evidente que estas herramientas pueden conllevar un riesgo para la privacidad de los ciudadanos; y, claro está, cuanto más sensibles sean los datos objeto del tratamiento, más peligroso será el resultado de un uso inadecuado de las herramientas de análisis. Podemos reformular la idea de la siguiente forma: si sumamos, por un lado, la creciente tendencia de los organismos públicos y privados a publicar datos de salud y, por otro, las herramientas de análisis de datos cada vez más potentes, obtenemos la capacidad de

analizar y, en consecuencia de prever, la evolución de la salud de toda una población. Continúa leyendo aquí.

Eduardo Vendrell Vidal: La Educación en Informática y la Protección de los Datos. Un camino por recorrer.

A primera hora de un día cualquiera, compruebo el correo electrónico. Recibo, entre decenas de correos no deseados, una convocatoria a una charla organizada por una entidad pública. Resulta que una vez acudí a otro evento emprendido por esta entidad, al cual me registré con mi dirección de correo, y es por ello que me incluyen en una lista de distribución. Sin embargo en la convocatoria que hoy recibo aparezco entre el resto de destinatarios revelados, una nube de direcciones de correo entre las que reconozco a algunos contactos que yo tengo guardados en mi agenda.

Buceo entre otros correos y descubro otro mensaje en el que se me traslada (a mi y a otros destinatarios) el acta definitiva de una Comisión de la que formo parte en la misma entidad pública anterior. No se nos envía un documento, sino un enlace a un conocido servicio de información en la nube. Se trata de un uso habitual por parte de esta entidad pública, que almacena por practicidad la información que genera en este recurso, haciendo por tanto dejación de su obligación de custodiar la información oficial propia. Continúa leyendo aquí.

Óscar Zurriaga: Protección de datos e investigación en salud en Europa: ¿de pretérito indefinido a futuro perfecto?

Uno de los problemas al que se enfrenta un paciente afecto de una enfermedad rara, llamadas así por su escasa frecuencia, es el del desconocimiento. Pocos profesionales sanitarios conocen a fondo su enfermedad, el desarrollo de instrumentos diagnósticos y de tratamiento es escaso y todo ello condiciona demoras diagnósticas, insuficiencias o carencias terapéuticas y ocasiona un agravio que se añade al dolor del propio padecimiento. En esas circunstancias los pacientes, y sus familias, lo que desean es conocer otros casos como el suyo, saber dónde están y qué les está sucediendo y son proclives a que lo que a ellos les pasa, en definitiva los datos que se pueden extraer de su situación, sirva para mejorar no sólo su propia condición sino la de otros. Continúa leyendo aquí.

Más información y entrevistas:
Juan Antonio Ibáñez
TF. +34 644 879 832
oficina.tecnica@apep.es
http://www.apep.es
@AsociacionAPEP

Más información sobre el Día Europeo de Protección de Datos:

Consejo de Europa.

Supervisor Europeo de Protección de Datos.