ESPECIAL

"Ojo al dato"

DE Tecnología & Sentido Común

ESPECIAL
AGOSTO
2024

ESPECIAL "Ojo al dato"

DE Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Miguel Angel Arroyo - Hack & News
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Marcos Navarro - Ai Robot
Víctor Almonacid - La Nueva Administracion
Jesús López Peláz - Consejo de Amigo
Renato Aquilino - Marcos y Normas
Alex Aliaga - Radio Security
Marta Martín - Mentes Divergentes

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
soluciones@businessandcompany.com

EDITA
Business, Technology & Best Practices, S.L.
Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://tecnologiaysentidocomun.com
soluciones@businessandcompany.com

ISSN 2951-8180

Ricard Martínez Martínez

Profesor en el Departamento de Derecho Constitucional, Ciencia Política y de la Administración y Director de la Cátedra de Privacidad y Transformación Digital. Doctor en Derecho por la Universitat de València. Miembro de la mesa de expertos en datos e Inteligencia Artificial de la Consejería de Innovación y Universidades de la Generali- tat Valenciana. Miembro del grupo de expertos para la elaboración de una Carta de Derechos Digitales de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Econó- micos y Transformación Digital. Ha sido Presidente de la Asociación Profesional Española de la Privacidad y responsable del Área de Estudios de la Agencia Españo- la de Protección de Datos.

LinkedIn:
https://www.linkedin.com/in/ri- cardmartinezmartinez/

Twitter:
https://twitter.com/ricardmm

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

Director Académico:

Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es

ESPECIAL AGOSTO 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

índice

#TYSC

Premios recibidos

Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

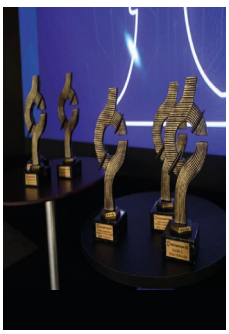
itSMF ESPAÑA

Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad

La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC

apep

Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

eset

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.

AVIS@ ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

El dato y la agenda legislativa

Escribo en Bruselas en un 15 de julio. Con independencia de lo que las encuestas pueden señalar carezco de información sobre el resultado final de las elecciones del próximo 23. Es el momento óptimo para escribir este artículo, ya que el desconocimiento proporciona objetividad a la hora de enfocar la cuestión que nos ocupa. Esta va a ser sin duda la legislatura del dato. Acompañará a la definitiva conformación de los espacios europeos de datos, a la consolidación del programa Década Digital Europea y su programa legislativo, y a la implementación del conjunto de políticas públicas que permitan transformar nuestra realidad social, económica y administrativa. Así, gestionar, crear y usar el dato, será sin duda uno de los retos más importantes de esta legislatura en todas las dimensiones desde el Gobierno de España hasta el menor de nuestros municipios.

La Unión Europea, es determinante para el mercado global de las tecnologías de la información, aunque ocupa un lugar subordinado en su producción. Competimos con el liderazgo de Estados Unidos con China como potencia emergente segundo gran jugador en esta liga. Somos segundones, probablemente estamos a la cabeza de la segunda división en una situación particularmente paradójica. Es innegable nuestra capacidad para investigar, crear e innovar. Aunque dicho talento acabe desplegándose al servicio del equipo ganador reclutando nuestras personas o comprando nuestras empresas en cuanto despegan.

La UE trata de revertir este estado de cosas mediante el programa Década Digital Europea, el impulso de la inteligencia artificial. Busca impulsar un modelo de investigación, innovación y emprendimiento con perfiles propios. Allí donde la Unión es un gigante, en la regulación, se propone un ecosistema normativo que, partiendo de la afirmación de la soberanía digital, pretende crear un conjunto de procedimientos de ingeniería normativa que disciplinen el desarrollo, implantación y el ciclo de vida de los entornos digitales. Aunque existan riesgos desde el punto de vista de las reglas de competencia en el comercio internacional el mensaje para el conjunto de la industria pretende ser muy claro: si usted desea operar en el mercado europeo deberá tener en cuenta las reglas que nos hemos dado. Y no nos referimos específicamente a normas como el RGPD, sino a una cultura que centra en la garantía de la dignidad y en la ética de los derechos fundamentales su modelo social y político.

CONTINÚA EN PRÓXIMA PÁGINA

Pero no basta con el despliegue de un marco normativo. La transformación digital no opera desde la legislación, opera desde la inversión en un modelo perfectamente planificado que debe ser capaz de adaptarse de modo muy flexible a un contexto en el que la disrupción tecnológica se sucede en espacios temporales cada vez más breves. En este sentido, el impulso de lo público resulta trascendental. Por un de esas paradojas de la historia, podemos alcanzar hoy los objetivos que persiguió la legislación sobre reutilización de la información del sector público desde hace 20 años. Hoy, la infraestructura y las capacidades del software permiten una analítica de datos sencillamente insospechable hace tres décadas. Sin embargo, los entornos de open data del sector público se han manifestado como insuficientes. Es por ello, a la UE impulsa un nuevo modelo de calado profundo.

La monetización de la privacidad ha puesto en manos de muy pocas empresas un volumen descomunal de datos que además se retroalimenta de los repositorios de open data que el sector público pone a su disposición. La debilidad de las instituciones y el mercado europeo es significativa en este ámbito. De ahí, que el esfuerzo de la UA consiste en movilizar el volumen de datos existente y facilitar su reutilización salvaguardando los derechos. Se trata de una estrategia compleja.

En primer lugar, asistimos a una reordenación que procura empoderar a la ciudadanía respecto del control de sus datos e imponer a los operadores dominantes, obligaciones de servicio. Se propone la creación de ecosistemas de intermediación de datos en los que la tecnología, por ejemplo la privacidad diferencial, permita el acceso a datos que han sido vedados a la administración, la industria, y la investigación por cuestiones regulatorias y que, sin embargo, han sido recogidos y explotados masivamente por operadores foráneos sobre la base de un sencillo consentimiento informado obtenido en el contexto de mercados de servicios monopolistas respecto de los cuales el sujeto únicamente podía participar e integrarse o ser un paria social. Por otra parte, se trata de construir un ecosistema funcional a las propias características de la economía de la UE. En ausencia de grandes campeones industriales y en un mercado caracterizado por una estructura de pequeña y mediana empresa se busca promover servicios de intermediación capaces de proporcionar soporte para que las Pymes puedan transformar radicalmente su modo de entender el análisis de los datos.

Para que todo ello sea posible, resulta imprescindible la definición de políticas públicas. La reordenación de los sistemas de información del conjunto de la administración y la generación de espacios de datos reutilizables a partir de los de la ingente cantidad de fuentes disponibles resulta imprescindible. Hay sectores líderes como la investigación en salud y el turismo que abren el camino y que demuestran que nuestro país podría ser altamente competitivo mediante una infraestructura pública de espacios de datos eficiente y basada en un modelo de cumplimiento normativo riguroso que aporte confianza, fiabilidad y robustez. Por otra parte, debemos apostar de modo muy claro por la promoción del talento. El pensamiento computacional sigue sin llegar a nuestras escuelas del mismo modo que el pensamiento científico se aleja cada vez más de amplias esferas de la población y, particularmente, de sectores universitarios. Seguimos sin ser capaces de integrar de modo flexible a las nuevas profesiones en la infraestructura administrativa. Los procesos de selección de personal, las relaciones de puestos de trabajo, y el modelo salarial no pueden competir con el sector privado. Otro tanto sucederá, sin el caso de recurrir a la externalización no garantiza la titularidad de la creación promovida con dinero público y sin garantizarse retornos de inversión.

En cualquier caso, desde la perspectiva de esta columna, debemos subrayar la importancia estratégica para una sociedad basada o dirigida por los datos de apostar por perfiles profesionales, más allá de los analistas de datos por los desarrolladores de software. Los expertos en privacidad, los que incorporan los valores de la ética y el humanismo, los expertos en gobernanza de la tecnología o los expertos en ciberseguridad son profesiones imprescindibles para sustentar la transformación digital que enfrentamos.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es

¿Campeones de la privacidad?

La privacidad es uno de los protagonistas mediáticos más relevantes. Y en esta materia se cumple la regla la conocida regla del periodismo según la cual es noticia que la persona haya mordido al perro. A diferencia de lo que sucede en esta revista, las buenas prácticas no venden. Ni en los medios convencionales, ni en los entornos sociales, se dedica espacio a las buenas prácticas y mucho menos a una consideración positiva de los profesionales. Es importante tener en cuenta las condiciones materiales en las que se despliegan las tareas propias de la persona delegada en protección de datos o experta en seguridad. La realidad es contraintuitiva, incluso contrafactual. En países maduros, -Alemania, Francia o España-, la protección de datos no es necesariamente una práctica consolidada ejercida por profesionales de alto nivel y dotada de recursos suficientes.

Las capacidades profesionales tienden a incrementarse de modo significativo. Ello se debe a distintos factores de impulso. La aparición de profesiones con contornos precisos y en contextos regulados ha facilitado extraordinariamente el diseño de planes de formación, de naturaleza universitaria y a través de actividades vinculadas a esquemas de certificación profesional. Por otra parte, es verdaderamente apreciable como las distintas entidades que agrupan a los profesionales de la privacidad y la seguridad en este país dedican un esfuerzo significativo a planes de formación que aseguran la adecuada calidad profesional de las personas asociadas. Por último, en un escenario que no dibujamos en su integridad, cabe referirse a los esfuerzos de los reguladores proporcionando guía, opinión e incluso herramientas útiles para el desempeño profesional.

Pudiera entonces parecer que estamos en el mejor de los mundos, pero no es así. La realidad es muy distinta. En primer lugar, no es en absoluto inusual que los obligados a contar con asesoramiento profesional de calidad se limiten a tomar decisiones meramente epidérmicas: nombrar a una persona delegada de protección de datos. Y así esta posición en más de un entorno público se ha convertido en un refugio profesional, en lugar de destino final o en una tarea asumida por la fuerza y con poco deseo. En el sector privado, en un contexto caracterizado por una estructura de pequeña y mediana empresa, recurrente se contratan servicios de baja calidad. Por si fuera poco, la dotación de medios suele ser sencillamente ridícula. Si resulta sorprendente que en instituciones de alta complejidad como las universitarias la plantilla no exceda en muchos casos de una única persona experta con algún soporte administrativo y con dedicación compartida, todavía resulta más angustioso cuando el equipo en una comunidad autónoma, o en una gran corporación pública o privada, presenta una plantilla insuficiente en relación con el volumen de personal y la intensidad los tratamientos. Si además no hay soporte, ni gobierno en los procesos las condiciones de cumplimiento normativo en protección de datos van a ser sin duda ingobernables.

CONTINÚA EN PRÓXIMA PÁGINA

De otro lado, el ejercicio profesional se despliega en un entorno hostil desde el punto de vista mediático. En tiempos de riesgo sistémico el modo usual de contemplar la privacidad y a sus profesionales se parece más bien al linchamiento en la vía pública. Ajusticiamiento más doloroso cuando procede de un colega. Resulta extraordinariamente sencillo y rentable el ataque, un modo de autopromoción personal. El ejercicio de la libertad de expresión, incluida la crítica más acerba, siempre es legítimo y constitucionalmente irreprochable. Sin embargo, me preocupan extraordinariamente aquellos casos en que nuestro colectivo profesional se embarca en un ejercicio de ensañamiento. Incluso, disponiendo de la libertad que concede la atalaya de la academia se tiene la ineludible obligación de plantear juicios críticos pero prudentes, duros si fuera necesario, pero respetuosos. En nada nos engrandece criticar con saña a nuestros colegas profesionales. Y no se trata de defender ningún tipo de espíritu corporativo, sino de considerar bajo qué condiciones el ejercicio de la crítica pública en nuestro ámbito debería regirse también por ciertas buenas prácticas.

En primer lugar, resulta muy conveniente tener en cuenta si nuestra opinión va a generar alarma pública. Porque en tal caso no sólo afectamos la reputación del responsable del tratamiento o el encargado, sino que adicionalmente estamos generando angustia en la población. La crítica debe ser razonada y razonable y acompañada de consideraciones que ayuden a que la sociedad, entienda y, si fuera posible, aprenda por el camino gestionar su privacidad. Por otra parte, en de casos extremos como infracciones o brechas, conviene asegurarse de conocer con detalle el asunto y de ejercer una crítica racional y fundada. Aunque la libertad de expresión, no se encuentre vinculada por los hechos sino por nuestra percepción de los mismos, en tanto que profesionales venimos obligados a un rigor particular también cuando opinamos.

De otro lado, resultaría de agradecer que se ejerza nuestra libertad crítica al colectivo profesional desde el respeto. Debo confesar que siempre siento empatía cuando leo noticias sobre infracciones al RGPD en alguna organización. Todos y todas hemos tenido que lidiar con una brecha de seguridad, con un riesgo de incumplimiento o con una situación descontrolada. Forma parte de nuestro oficio. Por otra parte, cuando éste se despliega en entidades carentes de cultura corporativa que no refuerza nuestro trabajo, nuestro desempeño se parece más a un ejercicio en la cuerda floja atravesando un precipicio que a una tarea medianamente razonable. Así que en nada nos enriquece el despliegue de crueldad o desprecio respecto de las entidades que sufren un incidente ni de las personas que en ella desempeñan tareas relacionadas con la privacidad o la seguridad.

Desde el punto de vista profesional, abordar de este modo casi salaz las cuestiones de privacidad ni nos convierte en campeones de la privacidad, ni nos enaltece, ni nos engrandece. Probablemente nos envilezca. Es bastante más sencilla en la crítica fácil que el análisis proactivo y constructivo. Y esto no sólo opera destruyendo reputaciones, sino que caracteriza a quienes ejercen este tipo de prácticas desde el punto de vista de su confiabilidad profesional. Es el momento de reforzar la figura de las personas delegadas de protección de datos, de las profesionales en privacidad y seguridad.

Es tiempo de construir una reputación positiva, de trabajar conjuntamente para mejorar las condiciones de ejercicio profesional y el despliegue material del cumplimiento de la normativa en todos los ámbitos. Y esta noble tarea exige de prudencia, templanza, buen juicio y vocación de servicio.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

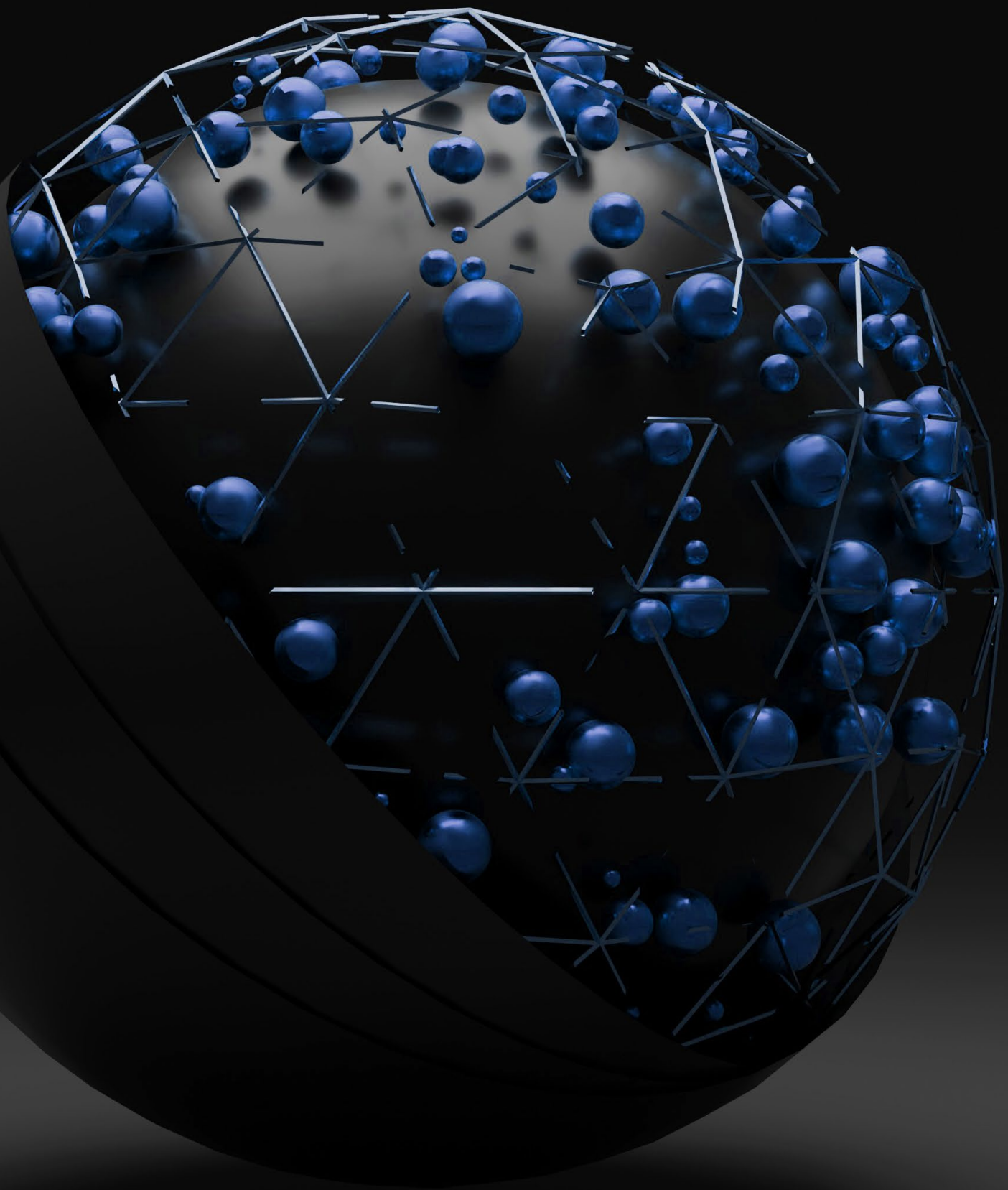
Espacios de Datos: progresar desde el dato a la inteligencia

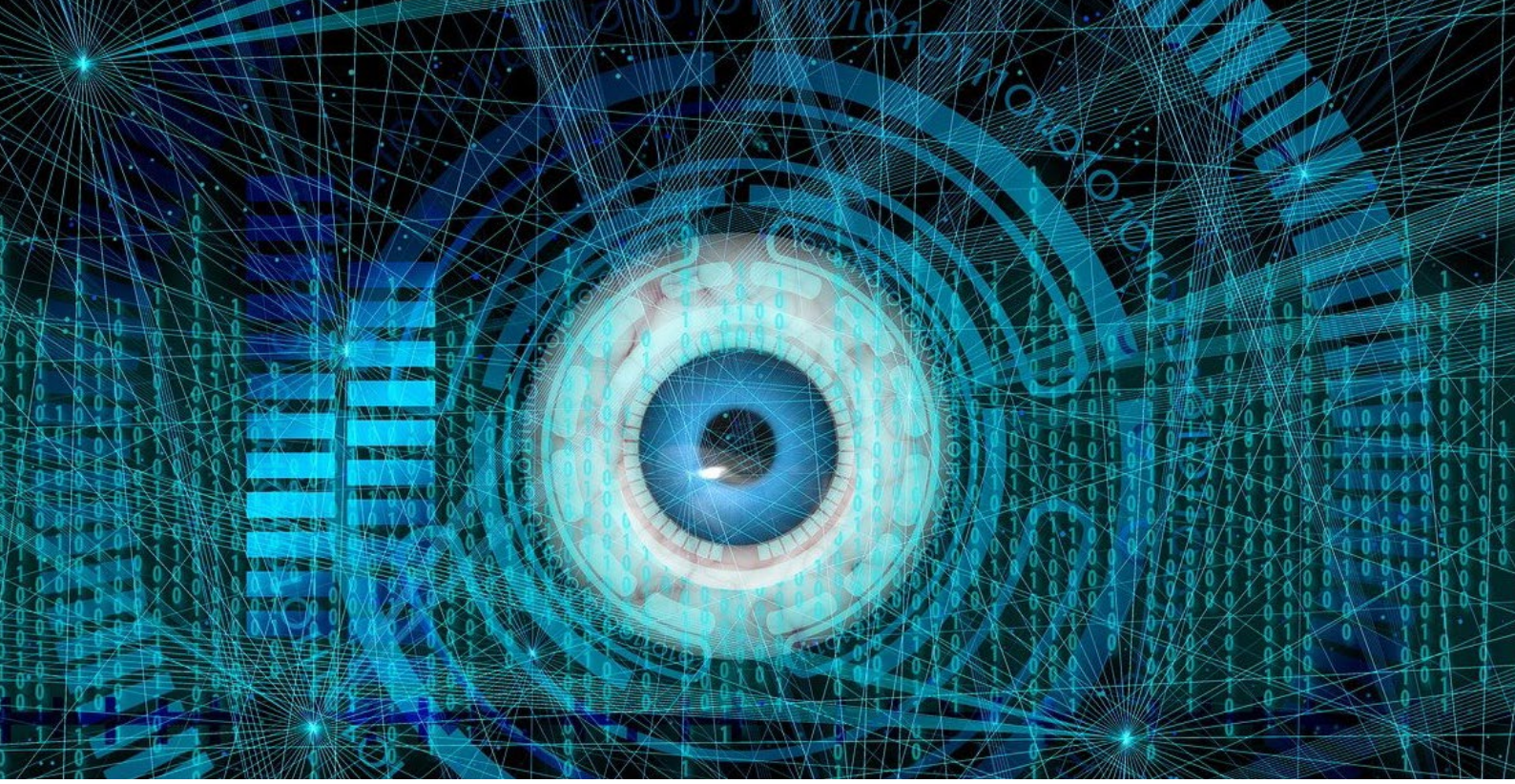
En un número anterior de Tecnología y Sentido común reflexionamos sobre la importancia de definir estrategias públicas de inversión orientadas a la construcción de los espacios de datos. Se afirmaba y, como en tantas otras ocasiones que, de ser cierto el paradigma de la Data Driven Society, el despliegue de los espacios de datos iba a jugar un papel esencial desde un punto de vista instrumental para la construcción, el uso o el desarrollo de entornos para la analítica de la información. La automatización de procesos y la evolución hacía modelos de decisión basados en datos los hace imprescindibles. Este artículo pretende ser una continuación del anterior aportando un conjunto de consideraciones que a nuestro juicio resultarían estratégicas para construir un espacio de datos.

En primer lugar, debemos entender que la construcción de espacios de datos no es un patrimonio exclusivo del sector público. Ciertamente este sector es el que se cuenta con mayores condiciones y posibilidades de desarrollo. Primero, la inversión pública puede provisionar fuentes de financiación estable y compartir el significativo volumen de datos de los que disponen los distintos gobiernos. Si el sector público concibe estos espacios, no como meros repositorios sino como entornos dinámicos y abiertos a la prestación de servicios de análisis de datos con particular atención a la investigación, la innovación y el emprendimiento sin duda operarán como catalizadores en el desarrollo del país. En esta línea apunta el diseño estratégico de la Unión Europea en el Open Data, Data Governance Act y la futura regulación del espacio de datos de salud. Por otro lado, las políticas europeas no excluyen espacios de datos del sector privado como entornos que propongan marcos colaborativos capaces de retroalimentar el crecimiento económico y el emprendimiento sin afectar al mismo tiempo a elementos esenciales de la actividad empresarial, como son la preservación de la propiedad intelectual y de los secretos comerciales e industriales.

Esta necesidad es particularmente significativa en un entorno como el de nuestro país, integrado por pequeñas y medianas empresas. Esta estructura empresarial escasamente puede soportar los costes que comporta la adaptación a la dimensión analítica de la transformación digital, tanto desde un punto de vista jurídico como de los recursos humanos necesarios para conseguirlo. Ello implica, salvo que se trate de una empresa especializada sectorialmente, no poder sufragar los costes de un delegado de protección de datos y o un analista de datos o no disponer de un volumen de datos cualitativa y/o cuantitativamente significativos. Por ello, la construcción de espacios de datos puede generar el contexto adecuado que permita financiar estos costes ofreciendo a nuestras PYME una ventaja competitiva. Aquí el papel de la Administración, de las asociaciones empresariales o de las cámaras de comercio puede ser absolutamente vital.

CONTINÚA EN PRÓXIMA PÁGINA





Por último, existe un último escenario pendiente de ser explorado¨: el altruismo de datos. Sería recomendable inspirarnos en aquello que hemos aprendido en el ámbito de la salud, a la hora de definir las condiciones el mismo. Debe tenerse en cuenta que para la promoción del altruismo de datos partimos de una situación tan contraintuitiva como paradójica. La mayor parte de nuestra sociedad carece de la menor prevención a la hora de registrarse en servicios de la sociedad de la información aparentemente gratuitos cuyo objeto de negocio es la monetización de los datos. Por otra parte, los expertos en protección de datos de este país hemos generado una sensación de desconfianza general de la población frente a los tratamientos de datos, particularmente cuando afectan al sector público. Este estado de cosas produce relaciones asimétricas en el mercado tanto desde el punto de vista de cada individuo, como en la competición entre empresas. Así, aquella entidad que es capaz de identificar un producto social único o exclusivo que ofrece al público como una suerte de regalo caído del cielo será capaz de acumular grandes volúmenes de datos en muy poco espacio de tiempo. Sin embargo, ante una petición de datos perfectamente razonable de una pequeña y mediana empresa europea, el consumidor recuperará la cultura de desconfianza y es altamente probable que tienda al rechazo. En el caso del sector público hemos generado una imagen clara de Estado Leviatán voraz en la captación de datos para controlar a la población que me temo no se corresponde con la realidad de las democracias de la Unión Europea. Por ello, la promoción del altruismo de datos requiere buscar condiciones de excelencia. Probablemente deberíamos poner en nuestro foco la experiencia adquirida en las donaciones de órganos o de sangre.

Por tanto, para ser capaces de disponer de lagos de datos se requiere en primer lugar generar confianza desde un empoderamiento del ciudadano. Aspectos como la transparencia, la garantía en la seguridad de la información, o la adecuada administración de los datos poseerán un valor crucial a la hora de promover la confianza de la ciudadanía. De lo contrario, el ejercicio de derechos de oposición al tratamiento o la presentación de denuncias podrían crecer significativamente. La gestión de los derechos, y particularmente del consentimiento evoluciona hacia hacía tecnologías de empoderamiento. Es necesario ofrecer herramientas de control efectivo en “un clic” y asegurar la debida retroalimentación con la comunicación de los logros alcanzados gracias a ese tratamiento de datos. Y ello sin perder de vista los riesgos asociados a la fatiga del clic. Incluimos, desgraciadamente, que un donante de datos, tarde o temprano dejara de serlo si 10 veces al día tiene que consentir un tratamiento y este problema es muy difícil de resolver. Por otra parte, debemos señalar, que los modelos de gobernanza basados en el cumplimiento normativo resultan esenciales para garantizar la calidad y confiabilidad de los datos. Es evidente, que la reutilización depende de un conjunto de procesos técnicos que tienen en cuenta su estructura, formato, clasificación y catalogación, así como todos los procesos que proporcionan condiciones de curación, validación y enriquecimiento de los datos. Pero no suficiente. Satisfacer los principios básicos de protección de datos, de legalidad y legitimidad, asegurar los juicios de proporcionalidad, de adecuación a fin o especificación de finalidad, de minimización de datos, o aplicar el enfoque de riesgo y la protección de datos desde el diseño y por defecto, constituyen herramientas imprescindibles para asegurar calidad y confiabilidad.

Por último, y aunque se trate de una cuestión que se viene predicando de la inteligencia artificial, es fundamental reforzar el concepto de diseño responsable. Esta responsabilidad no sólo es ética, tiene como marco de referencia ineludible la garantía de los derechos fundamentales de las personas y el cumplimiento del ordenamiento jurídico vigente en toda su extensión. Se trata por tanto de un modelo de gobernanza jurídica y tecnológica que debe llevarnos desde el dato a la inteligencia.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Certificación de privacidad de la AEPD: ¿mérito o requisito?

Garantizar condiciones adecuadas para el ejercicio profesional de las personas delegadas de protección de datos, así como para su formación y desarrollo de las debidas cualificaciones ha sido una constante a lo largo de toda mi carrera. Es esta una profesión en la que, en función de nuestra formación y compromiso podemos operar con un cierto grado de autoridad, vivir en la angustia permanente, pero también desplegar nuestras funciones desde la indigencia, cuando no la estulticia intelectual. Hace unos meses una conversación con un estimado colega incrementaba más si cabe mi constante preocupación en esta materia. Certificado en privacidad en prácticamente todos los estándares que uno pueda imaginar, esta persona, titular de una pequeña empresa, podía ser excluido de una licitación pública ya que no solo se le exigía la certificación de privacidad de la Agencia Española de Protección de Datos sino también la existencia de un suplente con la misma certificación. Y así, dicho desde el respeto, lo que había aparecido como un elemento para dotar de seguridad al mercado se convertía en un requisito para el acceso profesional. Esto sin duda resulta particularmente contradictorio en una profesión que no se encuentra regulada. Y convierte un examen de "tipo test" en un criterio de calidad.

Pero antes de reflexionar sobre esta materia conveniente posicionar esta figura en el contexto de las organizaciones. En principio, el diseño institucional, el DPD tiene por objeto ser un oficial de cumplimiento normativo con funciones de supervisión, control, formación y soporte, así como de atención directa a la ciudadanía, en el contexto de entidades que, por sus propias características, así lo requieran. El legislador español ha considerado que acudir esta figura cuando uno no es un sujeto obligado incorpora un plus de diligencia que debería ser contemplado en los procedimientos de inspección y sanción. Por tanto, el Reglamento General de Protección de datos y en su implementación la legislación española ha considerado que existen un conjunto de entidades en las cuales ya sea por razón del volumen de los datos tratados, por la naturaleza cualitativa de los tratamientos, por su naturaleza institucional o por la singular vulnerabilidad de los sujetos, cuyos datos son objeto de recogida y tratamiento, deberían ser asistidas por un experto con profundo conocimiento del RGPD y de aspectos como la seguridad, para contribuir a garantizar el cumplimiento de la norma.

Esta conformación convierte al DPD en un sujeto, particularmente importante dentro de la de la organización. En una sociedad en constante transformación digital prácticamente no existirá un solo proceso que no deba ser acompañado en su diseño, implementación y durante todo el ciclo de vida por el DPD. Por tanto, es imprescindible que este tipo de profesional se caracterice por su compromiso, conocimiento de la organización y del marco normativo y tecnológico y por su capacidad. Sin embargo, a pesar del altísimo

nivel de exigencia que ha caracterizado la legislación española desde su origen vivimos en un país que siempre cumplió con la norma de modo epidérmico. De ahí que hayan proliferado como flores de mayo los negocios de protección de datos basados en plantillas de copia y pega, que determinadas empresas se hayan enriquecido con cargo a los fondos de formación mediante corruptelas, o que sencillamente aparecieran en el mercado herramientas para crear empresas de protección de datos mediante cursos de formación de un día.

Acude a mi memoria una nota de prensa de la AEPD recordaba que no se puede auditar el cumplimiento de la legislación de protección de datos y la seguridad mediante una checklist formalizada por teléfono. En este contexto previo al RGPD, únicamente las empresas sometidas a un mayor riesgo regulador contaban con lo que podríamos definir un ancestro del DPD. Y sobre este sustrato de mera apariencia, particularmente grave en lo que se refiere a la Administración Pública, se implanta la figura del delegado de protección de datos en España. A nadie se le escapa que los criterios de selección de los DPD suelen ser de lo más variopinto. Existen entornos administrativos en los que para no incrementar el gasto se han reclasificado puestos en plantilla sin inversión en formación, se ha nombrado delegados de protección de datos de mera apariencia, o se ha externalizado un esfuerzo significativo al coste de un contrato menor.

Desconozco en profundidad la realidad del sector privado, pero el panorama no tiene por qué ser mucho más alentador. Y es aquí donde la aparición de los esquemas de certificación, contribuye de algún modo a ofrecer confianza y seguridad del mercado respecto de las ofertas existentes en el asesoramiento en esta materia. Sin embargo, viene bien a mi memoria una frase que se convirtió en un mantra para la APEP cuando realizamos la primera revisión de nuestro modelo de certificación: una certificación será tan valiosa como lo sea la peor de las personas certificadas. La reflexión que

CONTINÚA EN PRÓXIMA PÁGINA

desde entonces vengo realizando de manera cíclica a la luz de mi experiencia profesional como docente universitario me hace plantearme muy seriamente si en este país estamos siguiendo el camino adecuado en la formación e implantación de la figura de la persona delegada de protección de datos.

En primer lugar, la construcción de la certificación de privacidad auspiciada por la AEPD se caracteriza por un desprecio significativo de la formación universitaria. Así, disponer de un título oficial es poco menos que un mérito más en el esquema de certificación. Al parecer ofrece más seguridad realizar un cursillo de 200 horas que un master de 1500 con prácticas obligatorias y la ineludible obligación de resolver un caso de uso en el trabajo final de master. Permítanme mis lectores que me sorprenda de ello.

Por otra parte, el mercado necesita de dos criterios de confianza esenciales a la hora de seleccionar y contratar profesionales. El primero de ellos es tener la seguridad de que cuentan con una formación suficiente, formación que se extiende mucho más allá del RGPD, al marco normativo aplicable al sector y al propio modelo de negocio. En segundo lugar, la referencia de experiencia es relevante. Es natural, que un recién egresado aspire a puestos técnicos que le permitan crecer en su carrera profesional hasta alcanzar las cualidades que se esperan de un buen DPD. Nada de eso sucede en la certificación de la AEPD. Basta con 200 horas de formación y superar un examen tipo test. Sin embargo, en el desempeño profesional, un delegado de protección de datos nunca, y debo insistir nunca y subrayo por tercera vez nunca, se va a enfrentar a problemas cuya solución se basa en respuestas binarias o en la elección de un criterio específico.

La mayor parte del tiempo. Nuestro trabajo se desliza en el difícil territorio del Congo. Las respuestas binarias del tipo sino se producen generalmente en el juicio de legalidad de un tratamiento, y sólo parcialmente a la hora de verificar la proporcionalidad. El resto del tiempo se requiere una visión amplia del ordenamiento jurídico, un conocimiento profundo de cada una de las actividades del tratamiento, y una y un enorme y una capacidad enorme de análisis del funcionamiento del flujo del aire de los flujos de información para proporcionando un enfoque de riesgo, definir modelos de cumplimiento normativo. Y un test no demuestran nada de eso. Así pues, no puedo sino concluir este artículo, desde la más profunda de las preocupaciones. Si nos enfrentamos a una certificación que no distingue cualitativamente ni por experiencia, ni por sector de actividad, ni por condiciones de ejercicio profesional, que se supera con ustedes, y que además se convierte en estándar de referencia para ganar concursos para para ganar licitaciones promovidas por la propia administración pública puede que estemos consolidando el marco de referencia para unos deseos de baja calidad y cuando no para la corruptela.

Eso sí, todos con su certificado. No me cabe duda que la certificación de la agencia está siendo obtenida por titulados universitarios y por delegados de protección de datos con un alto nivel de experiencia en un contexto. Y es el modo correcto, es decir, convertir la certificación en un club de cualidad si se añaden a criterios adicionales de comprobación.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

La gobernanza de datos presupuesto de la Inteligencia Artificial

Cuando llegue a las manos de nuestros lectores y lectoras este artículo es altamente probable que el texto definitivo de la Artificial Intelligence Act haya visto la luz. Una cuestión que ha permanecido constante en todas las versiones es la de la gobernanza de datos. Los modelos de cumplimiento normativo en protección de datos, pero también en el uso de cualquier tipo de dato no personal, constituyen un requerimiento previo para el desarrollo de cualquier sistema de IA. Aunque nuestro marco de referencia sea la regulación de los sistemas de alto riesgo lo cierto es que los principios de gobernanza deberían ser comunes a cualquiera de ellos.

Con independencia de los requisitos específicos, a los que después aludiremos, la norma contempla una alta exigencia en la garantía de la calidad y la representatividad de los datos. Así, los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, representativos y en la mayor medida posible, carecerán de errores y estarán completos. Además, deberán tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema de IA. Por último, tendrán en cuenta, en la medida necesaria en función de su finalidad prevista, las características o elementos particulares del contexto geográfico, conductual o funcional específico en el que se pretende utilizar el sistema de IA de alto riesgo.

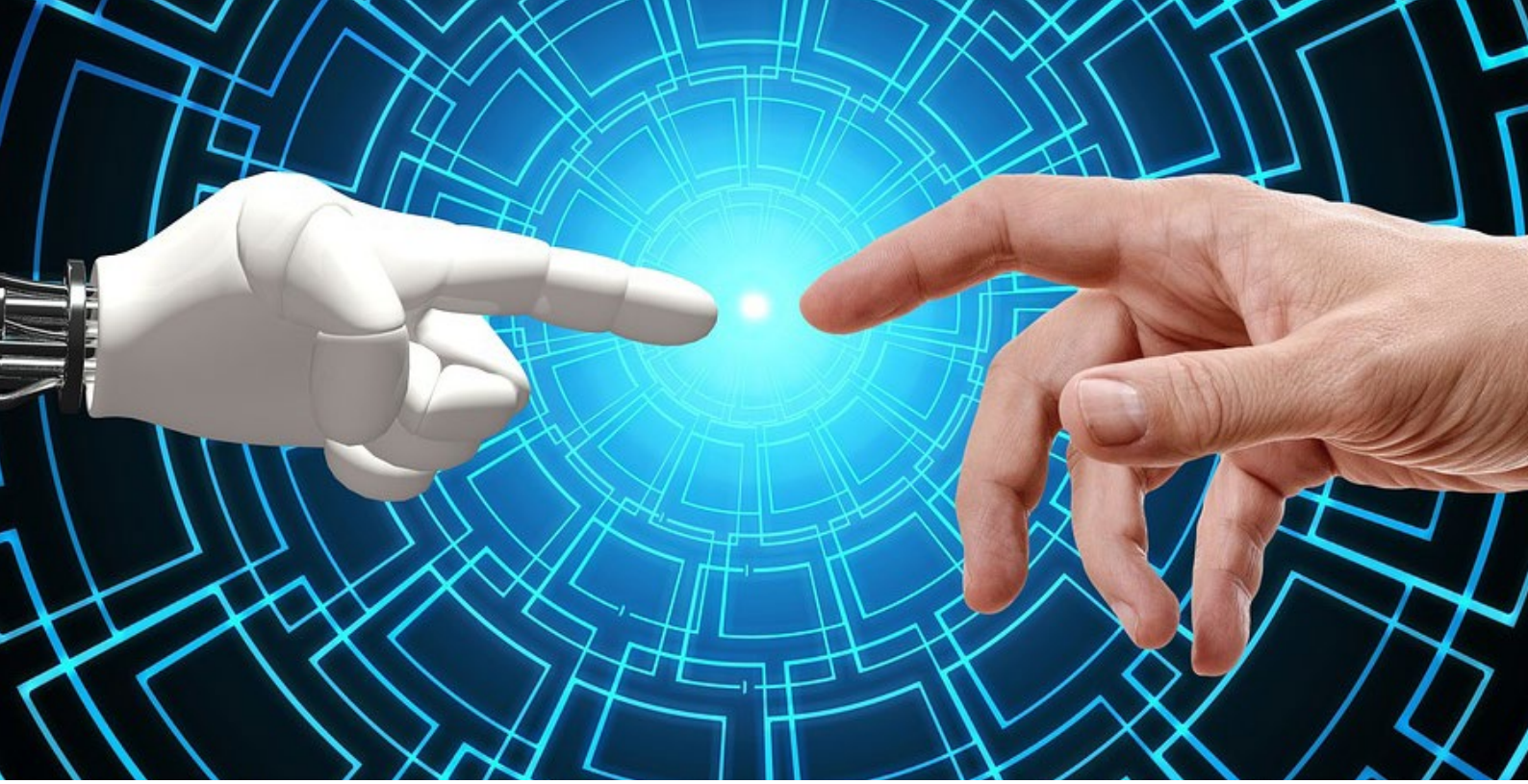
Para alcanzar estos objetivos es fundamental entender la metodología de protección de datos desde el diseño y por defecto. En la segunda dimensión el principio de minimización de datos deberá interpretarse como una regla de ajuste proporcional. Ni es tolerable la bulimia de los datos ni es admisible limitar el volumen, calidad o naturaleza de los datos de modo tal que se ponga en riesgo su calidad y se diseñen sistemas que ofrezcan resultados potencialmente discriminatorios. Desde el primer valor el enfoque de riesgos del RGPD, y particularmente en materia de derechos fundamentales y evaluación de impacto relativa a la protección de datos, deberían ofrecer una batería de medidas destinadas a prever y evitar los riesgos que se acaban de describir.

Por otra parte, y aunque AI Act se refiera a las categorías especiales de datos cabe considerar que la adopción de salvaguardias adecuadas para los derechos y las libertades fundamentales de las personas físicas, la utilización de las medidas de seguridad y las técnicas de tratamiento de datos personales ya sea en la anonimización, o especialmente cuando esta sea imposible, deberían ser reglas aplicables en todos los casos como buena práctica.

Por otra parte, la norma propone un conjunto de prácticas centradas en: a) la elección de un diseño adecuado; b) los procesos de recopilación de datos; c) las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, el enriquecimiento y la agregación; d) la formulación de los supuestos pertinentes,

CONTINÚA EN PRÓXIMA PÁGINA


AI



fundamentalmente en lo que respecta a la información que, ateniéndose a ellos, los datos miden y representan; e)la evaluación previa de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios; f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas físicas o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión; g) la detección de posibles lagunas o deficiencias en los datos y la forma de subsanarlas.

En resumen, el modelo de gobernanza de datos se alinea y recoge todos y cada uno de los procesos que derivan del Reglamento General de Protección de Datos y que la Agencia Española de Protección de Datos ha documentado de modo muy preciso en dos guías de obligada lectura: "Una aproximación para la adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial", y "Requisitos para auditorías de tratamientos de datos personales que incluyan Inteligencia Artificial". Se trata de documentos tan precisos, como exigentes y que deben sin duda conducirnos a una reflexión estratégica ¿estamos preparados para acometer esta tarea?

En mi opinión la respuesta debe ser negativa, aunque esperanzada. De un lado, es desgraciadamente conocido el alto nivel de dificultad que plantea el cumplimiento normativo de esta materia en la Administración. Si a ello unimos décadas de digitalización el problema presenta una magnitud considerable. En nuestro país, aunque se hayan alcanzado altas cotas de interoperabilidad, no existe una única administración electrónica, puede que las haya a cientos. Junto a la AGE, cada Comunidad Autónoma, cada Diputación o cada universidad pública han trazado su propia ruta. Y lo mismo ha sucedido en la sanidad donde al menos la proliferación de "setas" y reinos independientes de micro-tratamientos seguramente no existan. No obstante, las tareas de la Oficina del Dato y los esfuerzos en la construcción de un espacio de datos de salud nacional apuntan en la dirección correcta.

El mundo de la empresa será harina de otro costal. La gran empresa de nuestro país lleva décadas invirtiendo en compliance. Sin embargo, el territorio de la pequeña y mediana empresa es un erial de cumplimiento meramente formal y epidérmico muchas veces alimentado por buhoneros, cuando no corsarios con patente concedida por los fondos públicos de formación. Y en esto los servicios de intermediación de datos que nazcan al amparo de la Data Governance Act, tienen una ingente tarea. Por muy cuidados que sean sus recursos, sin un realineamiento de las PYME sus fuentes de datos internas pueden resultar jurídicamente inservibles. Si el país desea despegar en el mercado de la Inteligencia Artificial como producto o como servicio las políticas públicas y las decisiones empresariales que aseguren una adecuada gobernanza del dato serán imprescindibles.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Evento de Cierre de Temporada 2024 de las Revistas Tecnología y Sentido Común y Stakeholders.news

El 19 de julio de 2024, las revistas Tecnología y Sentido Común y Stakeholders.News celebraron el Cierre de su novena y tercera temporada respectivamente con un interesante evento en la sede de UNE Asociación Española de Normalización, en Madrid.

En una tradición que se inició el pasado año 2023, las revistas Tecnología y Sentido Común y Stakeholders.News prepararon un cierre de temporada a la altura tanto de la calidad de sus contenidos como del nivel de sus colaboradores. Con la inestimable colaboración de UNE Asociación Española de Normalización, el día 19 de julio de 2024 se reunió en Madrid un granado grupo de profesionales, entre los que estaban algunos de los colaboradores de nuestras revistas.

El evento comenzó con una bienvenida a cargo de Paloma García, Directora de Programas de Normalización y Grupos de Interés de UNE, y de Javier Peris, Director de las revistas Tecnología y Sentido Común y Stakeholders.News, en el que agradecieron a los presentes su asistencia, sobre todo a aquellos afectados por el incidente global en sistemas de información de grandes compañías de todo tipo que se dio en esa fecha.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Tras la bienvenida, se dio paso al ponente principal del evento, Ramsés Gallego, primer español (y tercer europeo) en ser nombrado para el "Hall of Fame" de ISACA internacional, evento que tuvo lugar en este 2024. Renombrado conferenciante, deleitó al público asistente con su charla "De Gestionar a Gobernar …. con 'G' de Ganar", en la que glosó las bondades de dar ese salto hacia el gobierno de las Tecnologías de la Información, sobre todo en los aspectos relacionados con la ciberseguridad. Ciertamente, un lujo contar con él para el evento.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

El siguiente acto fue la mesa redonda con cinco de los autores que colaboran con la revista Tecnología y Sentido Común en el que participaron: Alejandro Aliaga líder de la seccion “Radio Security”, Renato Aquilino líder de la sección “Marcos y Normas”, Marlon Molina líder de la seccion “Es Tendencia”, Marcos Navarro líder de la seccion Ai Robot” que a partir de la proxima temporada pasará a llamarse “Ai Futuro” y Manuel Serrat líder de la seccion “Futuro y Seguridad”.

Durante la mesa redonda de Tecnologia y Sentido Común, estos cinco representantes respondieron a las preguntas del presentador y director de la revista, Javier Peris, acerca de los contenidos de la temporada que terminaba, y de qué se podía esperar de sus secciones en cuanto a contenidos y novedades en la décima temporada de la revista.

Alejandro Aliaga centró su intervención en recordad que el objetivo de su sección “Radio Security” es concienciar a los lectores de que existen vectores de ataque no convencionales asociados con las comunicaciones inalámbricas, y que, por la evolución tecnológica, es difícil que éstos se reduzcan.

Por su parte, Renato Aquilino, en su sección “Marcos y Normas” ha centrado sus contenidos en poner de manifiesto el gap existente entre las normas y quienes las escriben, frente a quienes las han de convertir en realidad en las organizaciones, algo que resulta extremadamente complejo en algunos casos.

Por lo que respecta a Marlon Molina, con su sección “Es Tendencia”, ha tratado de contar a los lectores en esta temporada que termina los temas que, mes a mes, han atraído la atención del sector por diferentes motivos.

Marcos Navarro anunció que su sección, a partir de la décima temporada, cambiaba de enfoque y de nombre, para explicar cómo es la vida en 2024, sólo dentro de diez años, gracias a tecnologías como la Inteligencia Artificial y la Robótica.

En cuanto a Manuel Serrat, explicó que con su sección “Futuro y Seguridad” ha tratado de poner el foco en aquellos aspectos de la evolución tecnológica que pueden suponer algún tipo de riesgo, y concienciar a los lectores para evitarlos.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Finalizada esta mesa redonda, se llevó a cabo la segunda Mesa Redonda, que contó con cuatro de los colaboradores de la revista Stakeholders.News: Juan Manuel Domínguez líder de la Seccion "Organizaciones Resilientes", Luis Morán líder de la sección "Personas y Procesos", José Antonio Puentes líder de la seccion "Tendiendo Puentes" y Juan Jesús Urbizu líder de la seccion "Tecno-transformación".

Dada la temática de la revista, fundamentalmente dirigida a aquellos profesionales de la gestión de proyectos, programas y portfolios y áreas conexas, las preguntas para los participantes en la mesa redonda se centraron en poner de relieve la necesaria aplicación de estándares y buenas prácticas en cada uno de los ámbitos que tratan las diferentes secciones de la revista.

Juan Manuel Domínguez, a través de su sección "Organizaciones Resilientes", expuso aspectos tales como que, en Japón, con aproximadamente 120 millones de habitantes, hay 45.000 empresas centenarias, frente a las poco más de 5.000 que existen en España con 48 millones de habitantes.

Luis Moran comentó algunos de los temas que había tratado durante esta tercera temporada en su sección "Personas y Procesos", y avanzó alguna de las cuestiones que va a tratar en la cuarta temporada de la revista.

José Antonio Puentes (sección "Tendiendo Puentes") compartió con los presentes algunas vivencias personales, relacionadas con las dificultades que la gestión de proyectos enfrenta en determinadas organizaciones.

Por último, Juan Jesús Urbizu, que estas temporadas ha escrito en su sección "Tecno Transformación", apuntó algunas de las cuestiones más relevantes a las que se enfrenta el gestor de proyectos, programas y portfolios en relación con la digitalización de las organizaciones, y más desde la irrupción para el gran público de los sistemas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

Tras las dos mesas redondas, Javier Peris anunció el nombramiento de los tres embajadores de la revista Stakeholders.News en Hispanoamérica más concretamente en Puerto Rico, Uruguay y El Salvador.
En Puerto Rico contaremos cada mes con la participacion de Nesty Delgado en Uruguay contaremos con Daniel Sorokins y en el pais de la eterna sonrisa "El Salvador contaremos con Luis Guardado quienes fueron nombrados y serán a partir de ahora Embajadores de Stakeholders.news.

Los actos de cierre de temporada terminaron con la entrega de los premios Tecnología y Sentido Común y Stakeholders. News, en esta ocasión en su edición de 2024.

El "Premio Tecnología y Sentido Común 2024" recayó en el Consejo General de Colegios Profesionales de Ingeniería Informática (CCII), por su aportación al progreso de la sociedad de la información, el impulso al desarrollo ético de los avances tecnológicos y la defensa y promoción de la ingeniería en informática. El premio fue recogido por José García Fanjul, secretario del CCII y vicedecano del Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Por otro lado, el "Premio Stakeholders.News 2024" fue otorgado a la Agencia para la Administración Digital de la Comunidad de Madrid, por haberse convertido en referente en la innovación y digitalización de la administración pública y por su compromiso con el cumplimiento y la excelencia del servicio al ciudadano. Este premio fue recogido por Zaida Sampedro Préstamo, subdirectora general de Transformación y Gestión del Cambio de la Agencia para la Administración Digital de la Comunidad de Madrid.

Al terminar el acto, todos los presentes pudieron disfrutar de un magnífico networking alrededor de un espectacular catering que se sirvió en las mismas instalaciones de UNE, con lo que se dio por cerrada la temporada de ambas revistas. ¡Nos vemos en septiembre!

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

UNE Normalización Española

Progreso compartido

une.org

El síndrome del burnout en las personas delegadas de protección de datos del sector público

Es prácticamente imposible que quién lee estas páginas no conozca a profesionales de la privacidad que hayan renunciado a su puesto en el sector público. Salvo en supuestos muy precisos en las grandes administraciones del sector público este es un oficio que se ejerce en la mayor de las indigencias. Y ello se debe a razones estructurales más que evidentes. En primer lugar, y sin ningún género de dudas, existe un vicio fundacional que deriva de la interpretación de la vieja LORTAD y de su interpretación por la doctrina administrativa. No será este autor quien cuestione las elaboradas creaciones dogmáticas que afirman que imponer multas al sector público no supone otra cosa que trasladar recursos públicos entre administraciones. Tampoco discutiré que una grave afectación al presupuesto de un ayuntamiento redunde en perjuicio de la ciudadanía. Pero lo cierto es que el resultado no es otro que desincentivar el cumplimiento normativo.

En este ecosistema, y como resultado de esa carencia de un enforcement disuasorio se producen dos resultados a cuál más perverso. Desde el punto de vista de la gestión de plantillas ni se considera esencial garantizar que todo el personal esté formado en protección de datos, ni se definen para el personal técnico funciones de soporte al cumplimiento en cada área. Así, muchas administraciones cuentan con servicios de contratación funcionalmente incapacitados para reconocer un encargado del tratamiento en un contrato menor o evaluar las condiciones exigibles desde el punto de vista de la seguridad. Disfrutamos de gestores deportivos cuya incapacidad para tratar la información de menores salta a la vista, o entidades de calidad que, sin rebozo alguno proponen técnicas de evaluación que lesionan gravemente derechos fundamentales.

Por supuesto, el conocimiento estratégico de los altos responsables brilla por su ausencia. Esperar que entiendan que sin garantía del derecho fundamental a la protección de datos la transformación digital de la administración es sencillamente inviable y el uso de la inteligencia artificial una utopía, es sencillamente creer en imposibles. La incultura en protección de datos deviene así en un obstáculo insalvable que se proyecta en un segundo nivel todavía más crítico. No existe ninguna necesidad de considerar la materia ni un objetivo valioso, ni un recurso necesario o, ni siquiera, un gasto que asumir. No es ocioso recordar que el anteproyecto de la actual Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales tanto en su texto, como en su memoria de impacto, refería que la implantación de la figura del delegado debía realizarse a coste cero.

El resultado de esta serie de catastróficas desdichas no es otro que el nombramiento de personas delegadas de protección de datos carentes de recursos, y no siempre con la adecuada formación. Y, en estas condiciones, es imposible desplegar un modelo eficiente de cumplimiento normativo. Esta afirmación

CONTINÚA EN PRÓXIMA PÁGINA


NYC
US OPEN

se entenderá mucho mejor desde un enfoque práctico. Desde el primer día en su puesto de trabajo la persona nombrada se enfrenta a la necesidad de definir un mapa de procesos por lo demás bastante obvia. La primera regla es evidente: debes conocer tu organización. Ello implica disponer de capilaridad en términos organizativos y ser capaces de tejer un conjunto de alianzas personales y funcionales. Pero también, desplegar tareas de auditoría, por otra parte, obligatorias con el RGPD en la mano.

Con esta información, procede definir un modelo de cumplimiento en el que el registro de actividades de tratamiento cuyo conocimiento público es un incentivo, se configure como ruta de llegada y como precondición. Nadie, y ello incluye al gobierno político de la entidad y a su alta dirección técnica, debería tratar ni un solo dato fuera de los procedimientos reglados ni antes de la publicación en el registro. Así, sólo deberían poder iniciar un procedimiento quienes tengan poder de decisión operativa y respaldo organizativo y presupuestario.

Y aquí, es dónde nuestro DPD puede seguir la ruta del RGPD, licitud, legalidad proporcionalidad y adecuación (artículo 5), análisis de riesgos para los derechos y o evaluación de impacto relativa a la protección de datos (artículos 24 y 35), análisis de riesgos en seguridad (artículos 32 y 35), definición de las medidas y programación del tratamiento desde la protección de datos desde el diseño y por defecto (artículo 25) y… vestir el santo en transparencia, relaciones con terceros, responsabilidad demostrada…

Y para hacer todo esto, tenemos a una persona con un mínimo o nulo soporte, a la que no se financia una formación de alto nivel y que carece una estructura de apoyo. Cuando existe esta es ridícula atendido el volumen de personal que trata datos o la diversidad y complejidad de tratamientos. Y así, a nuestra persona delegada de protección de datos se le exige que resuelva los problemas bajo una premisa esencial: no dar la lata.

Y ello tiene una consecuencia inmediata si el o la profesional son personas honestas y competentes. Primero, el trabajo diario las desborda. Es como si uno fuera bombero en una ciudad donde hay edificios encendidos 24 horas al día, 7 días a la semana.

El segundo estadio es el de la transferencia de responsabilidad. Esto es muy curioso, aunque la LOPDGDD regule negro sobre blanco la indemnidad del DPD por las infracciones el responsable del tratamiento internamente se le considera culpable y uno acaba incluso creyéndolo. Y así, se produce una inversión inmoral del criterio de responsabilidad en la que la función esencial del DPD consiste en no molestar y decir que sí a todo.

Y, puesto que es la única persona que sabe que el rey está desnudo, debe cubrir sus vergüenzas si fuera necesario. Y para ello debe traicionar su misión fundamental que no es otra que soportar el funcionamiento de la entidad y a la vez asegurar la garantía de los derechos fundamentales.

E inevitablemente sucede lo obvio: el *burnout* aparece y en lugar de hacer lo que se debería, esto es poner en conocimiento de la AEPD que se están laminando las funciones y el estatuto de independencia, se renuncia al puesto desde una lealtad institucional tan encomiable como perversa. Pero no se preocupen nuestros lectores, a la administración no le faltarán candidaturas internas complacientes. Y si no, no hay problema. Con un contrato menor, o en todo caso inferior al coste de un grupo A1, seguro que encontramos alguna empresa de reconocido prestigio.

Y no lo duden, capaz de copiar pegar un modelo basado en "*templates*" de diseño impecable, de proporcionar atención telefónica, y de poner al servicio del responsable del tratamiento personas que suelen desconocer las más elementales rutinas y la naturaleza de la tarea administrativa. Esto sí, en el papel, que como decimos los profesionales lo aguanta todo, el modelo de cumplimiento normativo será tan aparente como irreal …

Y a seguir.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

MPPM® MGEIT® eGob®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Proteger a los menores: un reto de país

La Agencia Española de Protección de Datos ha dedicado un significativo esfuerzo en los últimos años a incrementar las garantías para la protección del derecho a la protección de datos de los menores impulsando políticas públicas significativas. En su extensa sección dedicada estas materias pueden encontrarse recursos de todo tipo. Debe señalarse que la primera guía con un decálogo de recomendaciones para padres y otro para los propios menores se publicó en el período en el mandato del doctor Artemi Rallo Lombarte (2007-2011) junto con la traducción de manuales desarrollados por la autoridad irlandesa destinados específicamente a los docentes. Salvo con alguna contada excepción, en la que la AEPD decidió no tutelar a menores obligados a subir a YouTube vídeos exámenes de la asignatura de inglés, la trayectoria de la autoridad ha sido impecable y caracterizada por un crecimiento constante. El penúltimo hito en esta materia ha sido la presentación de una metodología para la verificación de edad.

Finalmente, el presidente del Gobierno de España anunció en la celebración del Día Internacional de la Protección de Datos varias medidas estratégicas para la generación de un entorno digital seguro para la juventud y la infancia. A nuestro Gobierno le preocupa significativamente el incremento del consumo de pornografía por parte de los menores de edad, así como su sobreexposición a los riesgos de Internet. Por ello propone alcanzar un gran acuerdo de país para proteger a los menores en la red basado en tres ejes: la aprobación de una ley integral para la protección de los menores en Internet, el impulso de una estrategia multidisciplinar desde el ámbito educativo, situando la prevención y la formación como un eje clave, y la creación de soluciones tecnológicas que impidan el acceso al contenido para adultos por parte de los menores de edad.

En lógica coherencia con este anuncio, el Consejo de ministros de 30 de enero de 2024 aprobó la creación de un comité de personas expertas encargado de diseñar una estrategia de país que promueva un entorno digital seguro para las niñas, niños y adolescentes. Este grupo estará compuesto por un máximo de 50 miembros cuenta con representación del Observatorio de Infancia, el Observatorio Español del Racismo y la Xenofobia, el Consejo Estatal de Participación de la Infancia y de la Adolescencia, el Consejo de la Juventud, el Consejo Asesor Digital Joven, la AEPD, el Consejo Escolar del Estado, el INCIBE, la CNMC y el Consejo de Consumidores y Usuarios.

CONTINÚA EN PRÓXIMA PÁGINA

Incluye representación de las confederaciones de asociaciones de madres y padres de alumnos y de organizaciones del tercer sector. Junto a ellos se integrará un grupo de expertos que integra profesionales de distintas áreas de conocimiento especializado.

El Comité abordará una ardua tarea y un alto nivel de exigencia para sus integrantes. Es evidente que la situación actual despierta un cierto grado de alarma social no exenta de buen fundamento.

Afrontamos un escenario tan complejo como ambivalente. Por un lado, resulta imprescindible afrontar riesgos sistémicos para toda una generación de niños, jóvenes y adolescentes. Por otro, resulta crucial asegurar su competencia digital. Es momento de felicitarse por la adopción de una estrategia integral y también de recordar la profunda responsabilidad que corresponde a los expertos y expertas en protección de datos y seguridad en este ámbito.

El Gobierno aborda con valentía y determinación un problema sistémico que no sólo afecta a España como muestran distintas acciones en la Unión Europea y Estados Unidos para la protección de los menores frente a los riesgos que derivan de las redes sociales. Nuestro gobierno afronta la cuestión desde bases sólidas.

La Carta de Derechos Digitales, en la que este articulista autor tuvo el honor de participar, incorporaba un conjunto de medidas y recomendaciones estratégicas no sólo en materia de garantía de los derechos de los menores, sino en todos los aspectos relacionados con su empoderamiento, formación y capacitación. El otro gran precedente al que me quiero referir es la Ley de Protección de Datos Personales y garantía de los derechos digitales. Desde esta ley es necesario apelar a la responsabilidad de las personas profesionales en materia de privacidad, la LOPDGDD forma parte de su estado del arte.

De hecho, la Ley Orgánica de Protección Jurídica del Menor afirmaba desde 1996 la garantía del interés superior del menor. Tenemos la obligación de interpretar y aplicar sistemáticamente el ordenamiento jurídico. La ley del 96 asegura el interés prevalente del menor, el RD 1720/2007 regulo el consentimiento en protección de datos, el RGPD lo contempla específicamente, y finalmente la LOPDGDD a la perspectiva del consentimiento del menor le ha sumado la inclusión de una compleja batería de medidas que afectan singularmente a padres, empresas y entornos escolares.

Los mensajes de la AEPD y la decisión política del Gobierno nos recuerdan que tenemos un elefante en nuestra habitación. Los entornos que tratan datos de menores, ya sea porque sea porque este su objeto de negocio, ya sea en virtud de obligación legal o porque encuentran un interés en ello, deberían ser particularmente rigurosos a la hora de definir condiciones de cumplimiento normativo. Y no es porque no existan instrumentos, ni por qué no se haya señalado por el regulador que bajo ciertas condiciones de vulnerabilidad y uso de tecnología, la evaluación de impacto en la protección de datos es un instrumento indispensable.

Por ello, este artículo quiere ser un llamamiento expreso, claro y preciso a los profesionales para que abandonen los modelos de mero cumplimiento formal y apuesten de manera radical por la protección de datos de los menores desde el diseño y por defecto. Es hora de mirar en nuestras propias casas y verificar en cuantos casos hemos sobreexpuesto la imagen y la información de los menores sin ninguna necesidad para ello. Hemos de revisar nuestras políticas y, en aquellos casos en los que nuestro está diseñado para ser consumido por una persona mayor de edad debemos introducir barreras de acceso.

La iniciativa del gobierno debe ser entendida como una llamada a la acción de todos los sectores. Nuestros lectores saben que tras cada nueva ley orgánica de protección de datos, las organizaciones se han comportado como si no existiera ninguna experiencia previa aplicable ni utilizable con un adanismo inverosímil.

Del mismo modo que de un modo artero la excusa de la ausencia de regulación ha servido para diseñar entornos de cuya calificación nos abstendremos.

A nuestro juicio, los mensajes de la autoridad de protección de datos y el Gobierno son muy claros: sin perjuicio del diseño de una nueva política integral debe cumplirse la ley, desde ya, sin excusas, con el mayor de los compromisos.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

La pequeña y media de la empresa y el reto de la inteligencia artificial

Si, se cumplen las previsiones a lo largo de este mes, en el peor de los casos en el inicio del próximo será publicado el Reglamento de la Unión Europea que regula la inteligencia artificial. Sin duda esta norma puede parecer lejana y poco relacionada con la actividad de la pequeña y mediana empresa, con una excepción, aquellas empresas cuyo objeto de negocio sea precisamente el desarrollo de la IA. Sin embargo, la realidad dista mucho de ser esta. Nuestras PYMEs deben interiorizar una cuestión muy clara la IA se va a integrar en sus modelos de negocio de modo natural e ineludible en un muy corto plazo.

En primer lugar, porque una parte significativa de los procesos productivos va a integrarse en dispositivos conectados capaces de incorporar herramientas de IA embebidas en el sistema. Además, la IA va a permear de modo significativo todos los procesos de distribución de bienes y servicios, desde el bot de asistencia a las herramientas de soporte a procesos de toma de decisión a la hora de distribuir nuestros productos. Por otra parte, servicios que nos prestan terceros como la confección de nóminas o la gestión de la contabilidad van a incorporar herramientas de inteligencia artificial destinadas a automatizar procesos que implicarán un cambio cultural interno significativo. Así nuestra gestión contable, fiscal o laboral deberá incorporar rutinas y procedimientos que sean funcionales a los nuevos modelos de gestión.

Podemos considerar distintos ejemplos que muestran bajo qué condiciones la IA podría el corazón de nuestros negocios, comenzando por aquello que podría parecer más alejado del mundo de la tecnología. Hoy en día mediante sensorización IoT tenemos la capacidad de monitorizar un entorno agrícola desde la siembra hasta la distribución del producto. Existen experimentos innovadores que por ejemplo miden las condiciones específicas de la tierra sobre la que se siembra, permitiendo tomar decisiones en relación con el riesgo el abono y los cuidados que necesita una cosecha. Al saber tradicional del agricultor se suma una tecnología capaz de analizar hasta el último componente químico, de correlacionar el grado de humedad, la temperatura y el pronóstico meteorológico para tomar decisiones en tiempo real sobre condiciones de riego y abono incluidos el día, la hora, y el volumen del agua que se va utilizar.

En la práctica, ello supone maximizar la eficiencia con ahorros significativos de costes que podrían alcanzar perfectamente un 20%. También se están desarrollando experimentos interesantes sobre toma de en la recolección. Nuestro sistema puede informar las condiciones de maduración de la cosecha y ayudar en la estrategia de comercialización. Esto es, podríamos decidir si de acuerdo con su estado de maduración, apariencia externa, y calidad, debería comercializarse en el mercado europeo o en mercados de proximidad. Y hablamos aquí de un modelo decisional básico. Imaginemos que el proceso se le incorporan datos sobre perfiles de consumo, mercados de futuros, canales de distribución, disponibilidad de fletes y cualquier otra información susceptible de orientar un proceso de decisión. A poco que este tipo de tecnologías escalen estaremos hablando de pequeñas empresas agrícolas utilizando la tecnología de modo intensivo y generando Marketplace para la negociación en tiempo real.

Pero es que este tipo de modelos podemos escalarlo a cualquier tipo de proceso productivo de una pequeña y mediana empresa. Por ejemplo, podríamos introducir modelos de gestión soportados por inteligencia artificial, tanto en los procesos de gestión y producción interna como desde el punto de vista del cliente. Así, la inteligencia generativa del lenguaje va a ahorrar tiempo y dinero en la redacción de documentos trasladando al administrativo la tarea de asegurarse de su calidad y precisión.

CONTINÚA EN PRÓXIMA PÁGINA

Por otra parte, la analítica de recursos humanos y del desempeño puede contribuir a mejorar de modo significativo, la eficacia y eficiencia de nuestra plantilla y soportar con datos procesos de toma de decisión en los incentivos a la producción, las contrataciones, y los ascensos que eliminen subjetividad y dejen arrinconadas ciertas corruptelas de todos conocidas que promueven a día de hoy una selección inversa de talento.

La pregunta que sin embargo nos debemos hacer es si la pequeña y mediana empresa está en condiciones de ser capaz de gestionar jurídicamente este reto. Y en este momento nuestra respuesta no puede ser sino negativa. Somos herederos de un modelo de cumplimiento normativo en protección de datos que, como en más de una ocasión se ha señalado en esta Revista responde ineludiblemente a procesos puramente epidérmicos de rellenado de impresos proforma muy ajenos a un cumplimiento normativo real. Ni que decir tiene, que el desconocimiento de los requisitos de análisis de riesgos para los derechos fundamentales, de verificación del cumplimiento de los principios éticos de la inteligencia artificial son un reto sustancial. Y a ello se unirá el conocimiento de los complejos y profundos procesos que han aparecido no sólo en la legislación de protección de datos, sino en la referida ley de Inteligencia Artificial, en la data Governance Act o en la Data Act.

Ello implica, que las pequeñas y medianas empresas se enfrentan a un riesgo sistémico que podría impedirles alcanzar los objetivos que propone la transformación digital y la inteligencia artificial. Muchos de los procesos a los que nos hemos referido anteriormente son imposibles si no se cuenta con un esquema de cumplimiento normativo previo y con una confianza en la resiliencia jurídica de la organización. Es imposible implantar en el mercado un modelo de gestión del cultivo que sea integral y que atienda a la distribución si no somos conscientes de la confianza que nos ofrece y de si podría o no generar un riesgo sistémico para la cadena productiva en regiones con monocultivo. No plantean un riesgo que afecte a la protección de datos, pero un funcionamiento sesgado puede causar un profundo impacto en la economía.

Por otra parte, es imposible que seamos capaces de mejorar las cadenas de distribución y los modelos de comercialización de nuestros productos al consumidor final, si no hemos sido capaces de cumplir con garantías la normativa relativa a la protección de datos. La consecuencia inmediata es obvia, resultará sencillamente imposible utilizar nuestros propios conjuntos de datos para alimentar las herramientas de inteligencia artificial. Por último y no por ello menos grave cabe preguntarse si las consultoras que están asesorando a las PYMEs serán capaces identificar un proveedor confiable de servicios de inteligencia artificial. Por ello, es urgente y estratégico asegurar que ese conocimiento llegue al entorno productivo de nuestro país desde cualquiera de sus dimensiones.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es

Cookies: un desastre regulatorio

La regulación de las cookies y fingerprints ha sido la historia de un despropósito. Lo paradójico reside en que protegiendo nuestra privacidad vamos camino de acabar con el debate abierto y democrático. La esencia del derecho a la información consiste en promover la formación de una opinión pública libre y asegurar el acceso a distintas fuentes de información. El legislador, y las autoridades de protección de datos, no han encontrado soluciones funcionales. La mayoría de usuarios sigue aceptando cookies mientras los que las rechazan renuncian a la lectura de decenas de periódicos.

Vaya por delante una afirmación de principio: es absolutamente necesario asegurar que los medios de comunicación generen ingresos que aseguren su sostenibilidad e independencia. Ha sido la evolución de la tecnología y más de un error en la definición de la legislación y su aplicación, las que nos han llevado hasta aquí. El órdago más reciente, el "o cookies o pagas" no es otra cosa que el último acto de un proceso de alineación con las políticas de las redes sociales y buscadores cuyas prácticas han llevado a la empresa periodística al borde de la extinción.

Internet ha producido una mutación en el modo de actuar la empresa periodística y en el de consumir la información. Antes de internet la publicidad contextual financiaba los medios que contaban con usuarios fidelizados y con ecosistemas de uso compartido, del bar a la biblioteca, que incluso no generando ingresos directos expandían el efecto de la publicidad. La prensa escrita ha visto constantemente reducida la clientela en soporte papel, ha sido víctima del "todo gratis" de buscadores y redes, así como de agregadores de todo tipo. También cambiaron los hábitos de lectura que se han hecho muy dependientes del titular y del like. Aquí se produjo seguramente la primera falla regulatoria. Nadie pareció ver ningún problema inicial en el que quienes no producían la información explotasen sus resultados convirtiéndose de facto en los operadores publicitarios dominantes. Y así, los medios tradicionales se encontraron con una injusta situación de hecho: al mismo tiempo que descendían sus ventas en el mundo físico se reducían sus anunciantes.

CONTINÚA EN PRÓXIMA PÁGINA

Sin embargo, lo que preocupaba al legislador, no sin razón, era la constante pérdida de privacidad cuando no la descarada manipulación emocional del consumidor primero con *cookies y fingerprints*, después con el perfilado y la inteligencia artificial aplicada al marketing emocional. Para "protegernos" se endurecieron las reglas sobre cookies y se fijaron reglas sobre el perfilado en el RGPD y la Ley de Servicios Digitales.

El resultado alcanzado puede resultar contraproducente. En el mundo de la analítica de datos es fundamental ser capaces de emular los efectos regulatorios con carácter previo. Por ello, es necesario dibujar el escenario de riesgos que al parecer no hemos tenido en cuenta. La gestión de las cookies ha sido una experiencia tediosa e ingobernable para el propio usuario. ¿A quién se le ocurrió que estaríamos dispuestos a abrir un cuadro de diálogo y andar marcando casillitas por proveedor? ¿Era consciente quién dictó las reglas de que algunos medios informan sobre más de 300 anunciantes? El resultado, es obvio: instalar bloqueadores de cookies.

En este contexto hay al menos dos soluciones que no han sido ensayadas y que resultan altamente dependientes de las llamadas tecnologías habilitadoras de la privacidad *(privacy enhancing technologies)*. De una parte, debería haberse apostado por herramientas vinculadas al navegador que facilitasen al usuario la predeterminación de su estándar de privacidad. De otra, sería razonable vincular ese perfil a un marco beneficioso para todas las partes. Por ejemplo, el usuario podría rechazar perfilados de alto nivel o definir preferencias sobre publicidad no deseada. Necesitamos gestionar un nivel de sofisticación alcanzado por la publicidad que la puede convertir en algo nocivo. El consumidor puede también tener preferencias ideológicas y sentir rechazo por un anunciante. ¿No existe en el estado de la técnica ninguna solución de equilibrio que permita al lector recibir publicidad bajo control y al medio financiarse con ella?

Ahora los medios no hacen otra cosa que aplicar las lecciones aprendidas de las redes sociales esto es situar al usuario frente a un todo o nada. Como suele decirse, el papel lo aguanta todo, así que o se aceptan las condiciones o se pagan 13 euros al mes para seguir disfrutando del subidón de endorfinas de los likes. Y este ha sido el punto de llegada de los medios. ¿Cuál es el resultado entonces de la regulación? A nuestro juicio se da un paso más en la pauperización del debate público y la calidad de la democracia. A diferencia de las redes sociales, el medio de comunicación es altamente dependiente del perfil del lector. Esto implica que ante el todo o nada la aceptación de las cookies dependerá del interés específico de la noticia. Y este hecho, puede agravar derivas patológicas o generar nuevos riesgos. Internet cambió el modo en el que las personas leemos. Los primeros 15 segundos definen nuestra atención, los siguientes 30 si vamos a decidir seguir en la página y superado el minuto es posible que profundicemos. Por otra parte, el presupuesto es limitado, para el usuario que no puede pagar por leer varios medios.

Por otra parte, buscadores y redes sociales han convertido al titular en la noticia en sí misma. Por tanto, se impone el clickbait y la rapidez en publicar. Estos dos fenómenos harto conocidos degradan el oficio periodístico a la caza del click, reduciendo no solo la calidad informativa sino los tiempos y las metodologías de verificación de la información. Y así, en este ecosistema en el que hay que sumar los algoritmos de personalización de las redes y buscadores que en la práctica distribuyen la información y mediatizan las elecciones de los lectores.

Finalmente, el o aceptas *cookies* o pagas, nos conduce a un escenario de fidelización del lector que sólo prestará atención al medio por cuyos contenidos paga. Y con algo tan obvio para cualquiera, como lejano a lo que piensan los reguladores, si al lector le interesa el titular aceptará las cookies. Ello, se quiera o no, contribuirá todavía más a la polarización que han generado las redes y, puede intuirse que al envenenamiento del debate público con *fake news*. ¿O es que alguien duda que los "medios" que las expanden no van a seguir abiertos y accesibles? Ello plantea un horizonte inmediato de una minoría de lectores segmentados, vinculados a una o dos cabeceras, junto a una inmensa mayoría de consumidores de información altamente influidos por el algoritmo de personalización y seguramente más motivados por el impacto emocional que por el análisis racional de la realidad. ¿Dónde queda ahora el libre mercado de las ideas?

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

La culpa es del DPO

No busquen el menor atisbo de ironía en el titular de este artículo: no la hay. A lo largo de los últimos tiempos vengo apreciando diversas situaciones en las que el ejercicio profesional de una persona delegada de protección de datos afecta gravemente a las condiciones de los tratamientos. No se trata necesariamente de un ejercicio profesional negligente, que también los hay, sino de modos de entender el ejercicio profesional que no puedo calificar sino de perturbadores.

A mi juicio no hay un modo necesariamente correcto de desplegar las tareas propias del DPO-DPD, es más sencillo identificar ciertos TICS que bajo ciertas condiciones generan malas prácticas. Las lecciones aprendidas provienen de los más diversos sectores y de distintos países lo que obliga a pensar desde un juicio crítico cuáles de ellas provienen del propio ecosistema y puedan alcanzar una naturaleza sistémica altamente peligrosa.

El primer supuesto al que quisiera referirme podría definirse como el ejercicio defensivo de las funciones de asesoramiento y supervisión. La característica más sobresaliente de este supuesto se traduce en un enfoque binario del tipo prohibido-permitido. En este modelo de bipartición "salomónica" el responsable, como las madres de la historia, sólo pueden llevarse al bebe entero. Salvo en el caso de manifiestas ilicitudes nunca a lo largo de mi vida profesional, académica o investigadora me he encontrado un solo supuesto de este tipo. Siempre hubo una inmensa escala de grises y por defecto mi tarea se despliega en el resbaladizo territorio del "cómo".

Esta apuesta se comprende en entornos sometidos a una alta presión regulatoria que obligue a un ejercicio defensivo. Y en este caso, las autoridades de protección de datos deberían reflexionar profundamente sobre su papel. Resulta mucho más peligroso, o incomprensible encontrarse con apologetas del "no" desde la soberbia, la ignorancia estulta o la comodidad. Vaya por delante un ejemplo: "esos datos son imposibles de anonimizar" y, por tanto, aplica el RGPD. Sin perjuicio de la expectación que despierta una futura sentencia del Tribunal de Justicia de la Unión Europea, ni una sola vez en mi vida tal afirmación ha venido respaldada por un informe técnico y un análisis de riesgos de reidentificación mínimamente sólidos. Es más sencillo decir no por teléfono o por mail que hacer tu trabajo.

Y este modo de hacer las cosas conduce a una segunda dinámica incluso más perversa que la anterior. Me refiero a la esos supuestos de ejercicio confortable obligado o autoinfligido. Basta con leer nuestros últimos trabajos sobre las condiciones de cumplimiento normativo por las administraciones para entender a lo que me refiero. La ausencia de soporte a la persona delegada de protección de datos, el hecho de ser completamente ignorada la conduce sin duda a dos posiciones: a la renuncia al puesto o a la melancolía. Aunque ciertamente, no es menos cierto que en algunos casos excepcionales es una posición buscada un modo de ser intencional del DPD.

CONTINÚA EN PRÓXIMA PÁGINA

En esta segunda posición todo fluye sin problemas. Sin embargo, sus efectos son todavía más demoledores que en el anterior caso como con posterioridad se abordará.

El tercer supuesto grave que cabría integrar en este catálogo de disfunciones sería el del enfoque inadecuado de la responsabilidad. En esta modalidad la persona delegada de protección de datos suele ser un apagafuegos y su solución una manta ignífuga que lo apaga todo al tiempo que lo cubre. En esta modalidad todo tratamiento por surrealista que resulte acabará sin duda en el registro de actividades de tratamiento. La gestión de las brechas de seguridad se orientará a demostrar que lo hicimos bien, y hay algo que les aseguro que nunca ocurrirá: el o la DPD nunca apreciará la existencia de una vulneración relevante en materia de protección de datos, ni la documentará ni mucho menos la comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento. Aunque esta sea su obligación conforme al artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En el primero de nuestros ejemplos la persona delegada de protección de datos se erige en la práctica en responsable del tratamiento y condicionará de modo determinante el futuro de su entidad. Proyectos enteros de investigación, innovación o emprendimiento penden de un hilo. El DPD protagonista, el artista del no, ocupa una posición protagonista y encubre sus carencias en la aparente defensa de los derechos fundamentales. Con frecuencia, consigue el efecto contrario.

Nuestros melancólicos e indolentes segundo y tercer caso dan cuerpo al viejo refrán del pan para hoy y hambre para mañana. Proporcionan a sus organizaciones una falsa sensación de seguridad y a sus gestores carta blanca para hacer su santa voluntad sin consecuencias. Pero a poco que sople el viento el castillo de naipes se derrumba. En el caso de la Administración, como ya sabemos es poco relevante, dos malos titulares y a seguir por donde solíamos. En el sector privado decenas de empleos pueden caer.

Pero, sobre todo en todos los casos, lo que realmente desconcierta es la falta de vinculación de estos profesionales con los derechos de las personas. La persona delegada de protección de datos se ocupa de asesorar, soportar, informar y asesorar en protección de datos. Y cuando esto no se hace no sólo se vulnera un derecho fundamental. No encontrar el modo de procesar datos en situaciones de urgencia, descapitalizar la investigación impedir la innovación son el germen de catástrofes futuras.

Y en todos y cada uno de los casos compartidos en este artículo podemos encontrar un nexo común: una incapacidad para entender el significado de la independencia profesional, para desplegar enfoques de riesgos y para orientar el diseño basado en la protección de datos desde el diseño y por defecto.

Tal vez, deberíamos repensar las certificaciones y la formación universitaria sobre privacidad a veces tan ancladas en la acreditación memorística de los conocimientos como alejadas de las competencias funcionales a los tratamientos de las entidades.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Innovar es cosa de todos: lecciones aprendidas en WAIQ Summer Course 2024

Por segundo año el Real Colegio Complutense en la Universidad de Harvard ha acogido el curso Web3, AI and Quantum Computing (WAIQ) se trata de una iniciativa en la que profesionales de muy distintas procedencias y estudiantes en formación hemos tenido la oportunidad de abordar el futuro inmediato de estas tecnologías. Las aulas de la Harvard Law School han acogido un debate con un alto nivel en el que ponentes y participantes han creado un marco de diálogo altamente creativo y no exento de intensidad emocional. Quiera finalizar el curso de Tecnología y Sentido Común alguna de las significativas lecciones aprendidas.

En primer lugar, resulta altamente enriquecedor poder sentar a una misma mesa investigación, innovación, tecnología y derecho. Surgen muchos puntos de encuentro que demuestran la importancia de incorporar la cultura del cumplimiento desde el diseño al ADN de las organizaciones. Sin embargo, por favor absténganse juristas tradicionales, profetas del moverse rápido y romper cosas y científicos descreídos. Porque ninguna de estas actitudes tradicionales conduce a buen puerto. En WAIQ la descripción del marco jurídico que nace era considerado desde un enfoque de código, de requerimiento para el diseño. Y otro tanto sucedió con los valores éticos. A un tiempo, desde el punto de vista jurídico se hizo indispensable un esfuerzo de entendimiento de la realidad.

La falsa dicotomía entre derecho e innovación debería ser rechazada y descartada. En realidad, es muy probable que el mantra de la Unión Europea como paraíso regulador que limita la innovación deba ser revisado desde otros puntos de vista. A mi juicio, el problema no reside en la disciplina del llamado paquete digital de Reglamentos y Directivas. Estas normas tienen de una parte una enorme componente reactiva. Es muy probable que sin el problema del “olvido”, el dumping normativo y el establecimiento en jurisdicciones “débiles”, o la monetización de nuestros datos personales, el Reglamento General de Protección de Datos hubiera sido innecesario.

Pero es indiscutible que todos estos hechos han sucedido. Y es posible que sin Cambridge Analytica y el lanzamiento masivo de ChatGPT el Reglamento de Inteligencia Artificial fuera otra cosa.

Por otra parte, todas estas normas son funcionales a proyectos muy precisos de la la Unión Europea en el Programa de Década Digital y en la ejecución de políticas instrumentales en el ámbito de los espacios de datos o la inteligencia artificial. Puede que se apunte un cierto repunte proteccionista, pero debemos entender que la UE trata de definir su propio espacio de desarrollo público y privado en un entrono muy fluido y cambiante. Sea cual fuere la razón para ello, el marco jurídico deviene un requerimiento indispensable para el desarrollo de las tecnologías digitales.

Respecto de estas últimas resulta fascinante apreciar su estado de desarrollo y madurez y los mundos que anuncian. La probablemente mal llamada inteligencia artificial está cada vez más presente, al punto de ser una herramienta cotidiana para una parte significativa de la población se sea consciente o no. En WAIQ tuvimos ocasión de departir con cierta profundidad los compromisos empresariales que supone, las oportunidades para el país y las condiciones de despliegue y adopción. Desde el punto de vista del jurista, al margen de una lógica preocupación por el futuro de la criptografía, resultó de altísimo interés apreciar las potenciales interacciones de futuro entre la computación cuántica y la inteligencia artificial. Particularmente como la altísima capacidad de cálculo puede acelerar los procesos y, al mismo tiempo, los algoritmos pueden empujar la programación y la eficiencia en la computación cuántica. Ello sin contar con el fascinante mundo de las arquitecturas de hardware cuyas distintas opciones causan una sensación similar a la contemplación de la Sagrada Familia o la Gran Pirámide.

CONTINÚA EN PRÓXIMA PÁGINA

Por otro lado, el mundo WEB 3 ofrece tantas formas de concebir lo digital como escenarios seamos capaces de imaginar. Desde el mundo financiero y la contratación, a los entornos de juego y socialización pasando por casi cualquier mundo que se pueda imaginar. Y además, en algunas presentaciones con un sustrato libre y libertario y un compromiso social que te devuelve a aquella Internet que parecía haberse ido para siempre.

Finalmente, resulto emocionante apreciar como organizaciones de todo el orbe y de cualquier tamaño imaginable, muchas de ellas de nuestro país, han integrado distintas estrategias de innovación de diverso tipo buscando ser mejores y más comprometidas con su entorno. No parece un camino sencillo, cada uno debe recorrerlo desde su cultura interna, o a fuerza de cambiarla, abordando un escenario de avance científico y tecnológico acelerado. Y ello obliga a reclamar políticas públicas y estrategias empresariales en España que consoliden nuestro talento y aseguren un despliegue que alcance a todos los segmentos.

Y la lección final es propia. Las organizaciones no pueden desplegar la innovación tecnológica desde la asunción de que al no haberse regulado su “gadget” no hay límites. El marco de los derechos fundamentales, la responsabilidad de no hacer daño y responder por el que se causara, y el marco normativo sectorial previo del segmento en el que se despliegue la actividad “aplican”. Lo mismo que lo hace una mínima ética corporativa. Y estos valores deben integrar el ADN de nuestras organizaciones. También debemos asumir un nuevo rol para los juristas: el de facilitador. No se confundan, el facilitador no te lo pone fácil ni te dice a todo que sí. Es quien desde la legalidad puede trabajar en equipos multi y/o transdisciplinares contribuyendo a que las cosas pasen.

Y, esta no es una responsabilidad menor. El principio que debe guiar nuestros pasos es el de la legalidad, pero desde un entendimiento operacional en el que nuestra labor no se aleja de la ingeniería de procesos como una barrera final, se integra en ella y evoluciona en cada iteración. En cada oficio hay valores, principios y metodologías imprescindibles. Los de los juristas crecen y se enriquecen en su contacto con la investigación, la innovación y el desarrollo de la tecnología. Nuestro reto es asegurar no sólo la legalidad sino también que la tecnología sea inclusiva, democrática y garante de los derechos fundamentales. No es precisamente una tarea menor.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader
P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Octubre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

P4MGO!

NUEVOS MASTERS

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es