

REVISTA DE

PRIVACIDAD Y DERECHO DIGITAL

DIRECTOR DON PABLO GARCÍA MEXÍA

SUMARIO HISTÓRICO

INCLUYE TODOS LOS ARTÍCULOS
PUBLICADOS CON MENCIÓN DEL
TÍTULO, AUTOR, AÑO, NÚMERO Y MATERIA

TOTALMENTE ACTUALIZADO

RDU

El presente sumario pretende recopilar en un único documento, información detallada sobre cada uno de los artículos publicados en la Revista de Derecho Privacidad y Derecho Digital desde su lanzamiento, por lo que será actualizado a medida que se publiquen nuevos números.

El objetivo principal de este sumario es que el mismo sirva como elemento de consulta rápida para todos nuestros lectores y por ello, el mismo incluye, de manera ordenada, el detalle del: año y número de publicación, título, autor, sumario, resumen y palabras clave, estos dos últimos, en castellano e inglés.

Desde RDU queremos ofrecer a nuestros usuarios la mejor experiencia posible por lo que, además de poner a su disposición la información propiamente dicha, la herramienta utilizada para la publicación del presente sumario le permitirá realizar las siguientes operaciones que se detallan a continuación:

- Búsqueda por palabras.
- Establecimiento de marcadores.
- Descarga del documento.
- Copiar y pegar.
- Compartir en redes sociales.

Les informamos de que hemos realizado nuestros mejores esfuerzos por presentar toda la información de este sumario de manera correcta y fidedigna. Si a pesar de ello, usted encontrara alguna errata y/o error, le pedimos disculpas y le rogamos lo ponga en nuestro conocimiento a través de la dirección de correo electrónico: rdu@rdu.es



REVISTA DE

PRIVACIDAD Y

DERECHO DIGITAL

SUMARIO HISTÓRICO

NORMAS PARA LA REMISIÓN DE TRABAJOS PARA SU PUBLICACIÓN

La presentación de trabajos para su presentación está abierta a cualquier interesado. Todos los trabajos que se publiquen deberán haber superado un proceso previo de revisión y evaluación por parte del Consejo de Redacción de la revista aplicable en cada caso, en función de los criterios de originalidad, rigor, interés establecidos por RDU, entre otros.

La remisión de trabajos para su publicación supone la cesión, por parte de todos los autores del mismo, en favor de RDU, de un derecho exclusivo para la publicación, reproducción y comunicación publica del mismo en revistas científicas, para todo el mundo y por el plazo máximo que permita la ley.

A continuación se detallan los requisitos que deben cumplir los trabajos a efectos de su revisión:

ORIGINALIDAD Y AUTORÍA

Todo trabajo remitido para su publicación deberá ser original e inédito. En caso de que algún trabajo sea publicado en alguna otra publicación con posterioridad a su remisión a esta secretaría, el autor deberá notificarlo inmediatamente, para proceder a la devolución del mismo.

La autoría de los trabajos remitidos debe pertenecer a quien o quienes lo suscriban, lo que así se hará constar en la documentación que acompañe al trabajo.

DOCUMENTACIÓN

Junto con el trabajo se acompañará (i) un resumen ejecutivo (conforme al modelo adjunto como Anexo I), (ii) un breve CV de los autores y (iii) una copia firmada de las presentes normas.

Los datos personales que los autores faciliten durante este proceso así como cualesquiera otros datos que se generen con posterioridad como consecuencia de su relación con RDU, se incluirán en ficheros de los que RDU (con domicilio social en C/ Fray Juan Gil 7, Madrid; email: lopd@rdu.es) es responsable (el "Responsable"). Los datos serán tratados por el Responsable para el desarrollo, mantenimiento y control de la relación del autor con RDU y en particular, para gestionar la publicación de trabajos y la difusión de los mismos, así como para tramitar las peticiones que el autor nos dirija, conservar las comunicaciones para mejorar nuestro servicio así como para efectos estadísticos. Para ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos legalmente previstos, el Usuario debe enviar una solicitud por escrito al Responsable a la dirección o al email que se señala en esta cláusula, indicando en el asunto "Solicitud ARCO" y adjuntando copia del documento que acredite su identidad.

PRESENTACIÓN

Los trabajos se remitirán al correo electrónico articulos@rdu.es. El asunto del correo deberá indicar Remisión de Artículo seguido del título de la revista en la que se desee publicar. (ej: Remisión de artículo para la Revista de Derecho Urbanístico y Medio Ambiente). Todos los trabajos deberán estar redactados en castellano y acompañados de (i) un resumen de entre 100 y 120 palabras y (ii) un listado de cinco (5) palabras clave sobre el contenido del trabajo. Estos últimos elementos deberán estar redactados en castellano e inglés (ver modelo adjunto como Anexo I).

FORMATO

El formato de los trabajos deberá cumplir con las siguientes características:

- Tipo de letra: Times New Roman 12 y Times New Roman 10 para las notas a pie de página.
- Alineación: Justificada.
- Interlineado: sencillo.
- Citas: Deberán figurar a pie de página, numeradas correlativamente, haciendo referencia al autor del contenido, título original de la obra, fecha, editorial y página dónde encontrar la referencia original.
- Bibliografía: Deberá figurar, en su caso, al final del trabajo, numeradas correlativamente, haciendo referencia al autor del contenido, título original de la obra, fecha, número de edición y editorial.
- Otros elementos: Si se desea, pueden aportarse gráficos para su publicación, incluyendo la cita correspondiente, en caso de no ser propiedad del autor.
- Se recomienda que los trabajos no excedan en ningún caso de 30 páginas.

PROCESO DE EVALUACIÓN

Una vez recibido el trabajo, se dará acuse de recibo del mismo y se pasará a los correspondientes expertos que el Consejo de Redacción decida para su evaluación (mínimo dos). Una vez efectuada la misma, se dará cuenta de manera confidencial al autor o autores del resultado de la evaluación y, si esta es favorable, se procederá a la publicación del trabajo en la revista correspondiente, en el número y fecha que determine RDU.

En caso de que la evaluación del trabajo resultara desfavorable, se comunicarán al autor los motivos y le será devuelto con indicación, en su caso, de la posibilidad de que el mismo pueda ser revisado para su reevaluación.

FIRMADO EL/LOS AUTOR/ES

ANEXO I
MODELO DE RESUMEN EJECUTIVO

NOMBRE:
PRIMER APELLIDO:
SEGUNDO APELLIDO:
TITULACIÓN ACADÉMICA:
TELÉFONO:
EMAIL:
REVISTA EN LA QUE DESEA PUBLICAR:

* En caso de ser más de un autor, completar los datos personales y de titulación académica en el apartado observaciones.

TÍTULO DEL ARTÍCULO
PALABRAS CLAVE (CASTELLANO E INGLÉS)
RESUMEN EN CASTELLANO
RESUMEN EN INGLÉS
OBSERVACIONES

Año 2025

Número 38

CARTA DEL DIRECTOR

Por Pablo García Mexía

Los agentes de IA ¿Encaja el futuro de la IA en el Reglamento Europeo?

AI agents: does the future of AI fit into european AI act?

Por Carlos Fernández Hernández y Josu Andoni Eguiluz Castañeira

RESUMEN

Los agentes de IA basados en grandes modelos de lenguaje constituyen, hoy por hoy, la base fundamental de los futuros desarrollos de la IA en una multiplicidad de campos. Pero la rapidísima evolución de estas tecnologías y de sus avanzadas capacidades en aspectos como la capacidad de inferencia, de toma autónoma de decisiones y de actuación o agencia, plantean interrogantes sobre el encaje de estos sistemas en el Reglamento europeo de IA, cuyo marco podría verse desbordado por la potencialidad de estos agentes, dando pie con ello a lagunas o vacíos regulatorios en un campo con profundas implicaciones sobre los derechos fundamentales de las personas o la responsabilidad. El objeto de este artículo es analizar el alcance general de estos agentes en su estado actual y las consecuencias de su previsible evolución en el marco normativo europeo.

PALABRAS CLAVE: IA agéntica: Agentes de IA; Sistemas de IA; Sistemas de IA de propósito general; Riesgos; Autonomía; agencia

ABSTRACT

AI agents based on large language models currently constitute the fundamental basis for future AI developments in a multitude of fields. However, their rapid evolution and advanced capabilities in areas such as inference capacity, autonomy and agency raise questions about the fit of these systems within the European AI Act, whose framework could be overwhelmed by the potential of these agents, thereby giving rise to regulatory gaps or loopholes in a field with profound implications for human fundamental rights and liability. The purpose of this article is to analyze the general scope of these agents in their current state and the consequences of their foreseeable evolution within the European regulatory framework.

KEYWORDS: Agentic AI; AI Agents; AI systems; General Purpose AI systems; Risks; Autonomy; Agency

Identidad digital europea: El marco normativo eIDAS y su impacto en ciudadanos y empresas Españolas.

European Digital Identity: the eIDAS regulatory framework and its impact on spanish citizens and businesses.

Por Dra. Francisca M. Rosselló-Rubert

RESUMEN

El Reglamento eIDAS (UE) 910/2014 marcó un hito en la identificación electrónica y los servicios de confianza en la Unión Europea, facilitando transacciones digitales seguras y

transfronterizas. Con la llegada de eIDAS II (UE) 2024/1183 se introduce la Cartera Europea de Identidad Digital (EUDI Wallet): una solución innovadora que permite a ciudadanos y empresas gestionar de manera autosoberana y segura sus datos identificativos y demás atributos electrónicos.

Este artículo explora la evolución del marco normativo eIDAS y los fundamentos de la identidad digital (como la descentralización y la autosoberanía). También se estudian las funcionalidades de la EUDI Wallet, concretamente su interoperabilidad, su aplicación voluntaria en sectores públicos y privados y su desarrollo técnico mediante la “Caja de Herramientas Común” y los proyectos piloto europeos, así como su implementación en España, con énfasis en el proyecto nacional “Cartera digital” y el modelo catalán “idCAT”. El trabajo finaliza valorando el impacto de la EUDI Wallet en ciudadanos y empresas españolas, resaltando beneficios como la simplificación de trámites, la reducción del fraude y la promoción de la inclusión digital, junto a retos como la armonización técnica y su adopción masiva.

PALABRAS CLAVE: Identidad electrónica, identidad autosoberana, identificación electrónica, servicios de confianza, interoperabilidad, cartera europea de identificación digital.

ABSTRACT

The eIDAS (EU) Regulation 910/2014 marked a milestone in electronic identification and trust services in the European Union, facilitating secure and cross-border digital transactions. With the arrival of eIDAS II (EU) 2024/1183, the European Digital Identity Wallet (EUDI Wallet) is introduced, an innovative solution that allows citizens and businesses to manage their

identification data and electronic attributes in a selfsovereign and secure manner. This article explores the evolution of the eIDAS regulatory framework, the fundamentals of digital identity (such as decentralization and self-sovereignty), and the functionalities of the EUDI Wallet, highlighting its interoperability and voluntary application in public and private sectors. It also analyzes its technical development through the “Common Toolbox” and European pilot projects, as well as its implementation in Spain, with emphasis on the national project “Digital Wallet” and the Catalan model “idCAT”.

The analysis concludes by assessing the scope of the EUDI Wallet for Spanish citizens and businesses, highlighting benefits such as the simplification of procedures, the reduction of fraud, and the promotion of digital inclusion, along with challenges such as technical harmonization and its mass adoption.

KEYWORDS: Digital identity, self-sovereign identity, electronic identification, trust services, interoperability, european digital identification wallet.

Las demandas colectivas en Protección de Datos: ¿Nuevo ciberriesgo?

Class action lawsuits in data protection: a new cyber risk?

Por Francisco Pérez Bes

RESUMEN

Si bien el artículo 82 del RGPD ya prevé la posibilidad de que el afectado pueda reclamar al responsable del tratamiento una indemnización judicial por los daños morales causados, la nueva regulación europea contempla la posibilidad de que los

afectados interpongan demandas colectivas, que en otros países cercanos exigen indemnizaciones multimillonarias. Este escenario, a la vista de que la normativa de competencia desleal califica a la infracción de la normativa como práctica comercial desleal, abre la puerta a que se presenten este tipo de acciones por vía judicial, lo que puede suponer un gran perjuicio a las empresas demandadas, hecho este que, según se describe en este artículo, supone un riesgo empresarial relevante que debe ser prevenido y gestionado como tal.

PALABRAS CLAVE: Protección de datos, Reglamento General de Protección de Datos (RGPD), competencia desleal, práctica comercial desleal, demandas colectivas, responsabilidad, indemnización, riesgo, seguro, financiación de pleitos.

ABSTRACT

Although Article 82 of the GDPR already provides for the possibility of the data subject claiming compensation from the data controller for moral damages, the new European regulation contemplates the possibility of data subjects filing class action lawsuits, which in other nearby countries require multimillion-dollar compensation.

This scenario, given that unfair competition regulations classify the infringement of the regulations as an unfair commercial practice, opens the door to this type of legal action, which can be highly damaging to the companies sued. As described in this article, this represents a significant business risk that must be prevented and managed as such.

KEYWORDS: Data protection, General Data Protection Regulation (GDPR), unfair competition, unfair commercial practices, class actions, liability, compensation, risk, insurance, litigation funding.

El SANDBOX regulatorio de IA como medida de apoyo a la innovación en el Reglamento Europeo de Inteligencia Artificial.

The AI Regulatory Sandbox as a Measure to Support Innovation in the European Regulation on Artificial Intelligence

Por María Álvarez y Pablo Rodríguez

La ENCUESTA N° 38. Sentencia UNITED STATES V. GOOGLE (JUDGE AMIT MEHTA). En especial, su impacto respecto del navegador CHROME

Por Pilar Carrasco

EN RED N° 38

NOTICIAS DE LIBROS

Número 37

CARTA DEL DIRECTOR

Por Blanca Rodríguez Mimbrero

LA MEDICIÓN DE LA INNOVACIÓN Y EL PROBLEMA DE LOS INTANGIBLES.

Measuring innovation and the problem of intangibles.

Por M. Paloma Sánchez

EL PAPEL DE LA REGULACIÓN TECNOLÓGICA EN UN MUNDO DE CONVULSIONES GEOPOLÍTICAS.

The Role of Technological Regulation in a World of Geopolitical Upheaval

Por Ángel Gómez de Ágreda

RESUMEN

El desarrollo de la tecnología durante los dos últimos siglos había seguido una evolución lineal no disruptiva. Los estándares tecnológicos también abarcaban plazos largos en los que los periodos de adaptación repercutían en un diferencial muy pequeño de la población. En general, el mundo tecnológico era unipolar y eso confería cierta confianza a las potencias dominantes respecto del mantenimiento de su liderazgo. El crecimiento exponencial de las capacidades de la tecnología digital y su acelerada permeabilidad en la sociedad, unidos a la emergencia de potencias tecnológicas alternativas a las tradicionales obligan a encontrar nuevos equilibrios de poder.

PALABRAS CLAVE: regulación, geopolítica, estándares, gobernanza, inteligencia artificial.

ABSTRACT

The development of technology over the past two centuries had followed a linear, non-disruptive trajectory. Technological standards typically spanned extended periods, during which the processes of adaptation affected only a marginal segment of the population. Broadly speaking, the technological landscape was unipolar, affording the dominant powers a sense of confidence in the preservation of their leadership. However, the exponential growth of digital technologies and

their rapid diffusion throughout society-coupled with the emergence of new technological powers challenging the traditional hegemony-now necessitate the establishment of new balances of power.

KEYWORDS: regulation, geopolitics, standards, governance, artificial intelligence

SOBERANÍA TECNOLÓGICA, AUTONOMÍA ESTRATÉGICA... ¿CONTROL POLÍTICO?

Technological sovereignty, strategic autonomy...political control?

Por Jorge Villarino Marzo y Alfonso González de León

RESUMEN

El artículo aborda la evolución del concepto de autonomía estratégica en la Unión Europea, que se originó en seguridad y defensa y se amplió a la política exterior, culminando en la autonomía estratégica abierta tras la pandemia. Este concepto implica la capacidad de la UE para tomar sus propias decisiones y proteger sus intereses estratégicos. Para lograrlo, se considera fundamental la soberanía tecnológica y digital, buscando asegurar tecnologías críticas sin dependencias unilaterales, un objetivo reforzado por las actuales tensiones geopolíticas. No obstante, Europa enfrenta un desfase competitivo y una dependencia digital significativa frente a Estados Unidos y China en sectores clave como la nube, IA y semiconductores. La respuesta europea para garantizar su soberanía tecnológica ha incluido una fuerte regulación digital

y el fomento de la inversión en capacidades tecnológicas propias, y ha justificado también un resurgimiento del control político sobre sectores estratégicos mediante el cribado de inversiones extranjeras y la participación estatal en el ámbito empresarial.

PALABRAS CLAVE: autonomía estratégica, soberanía digital, dependencia, geopolítica, regulación

ABSTRACT

The article discusses the evolution of the concept of strategic autonomy in the European Union, which originated in the fields of security and defense and later expanded to foreign policy, culminating in the idea of open strategic autonomy after the pandemic. This concept refers to the EU's ability to make its own decisions and protect its strategic interests. To achieve this, technological and digital sovereignty is considered essential, with the goal of securing critical technologies without unilateral dependencies—an objective that has been reinforced by current geopolitical tensions. However, Europe faces a competitive gap and significant digital dependence on the United States and China in key sectors such as cloud computing, artificial intelligence, and semiconductors. The European response to safeguarding its technological sovereignty has included strong digital regulation and efforts to boost investment in its own technological capabilities. It has also led to a resurgence of political control over strategic sectors through mechanisms such as foreign investment screening and increased state involvement in business.

KEY WORDS: strategic autonomy, digital sovereignty, dependency, geopolitics, regulation

LA INNOVACIÓN, NO SOLO TECNOLÓGICA, PIEDRA FILOSOFAL DE LA PROSPERIDAD.

Innovation, not just technological, is the philosopher's stone of prosperity.

Por Jesús Banegas Núñez

RESUMEN

El progreso económico y social tiene que ver con el nivel y calidad de vida de la gente. Puesto que se puede describir, medir y comparar en el tiempo y en el espacio históricos, podemos aventurarnos a interpretar las claves que lo determinan. Hasta no hace mucho, mediados los años 40 del pasado siglo, no se conocían con rigor académico los factores que hacían posible el crecimiento económico generador del progreso de las naciones. El gran economista austriaco Joseph Schumpeter ya había anticipado, con su teoría de la “destrucción que creativa”, la importancia de la innovación tecnológica en la sostenibilidad del crecimiento de la riqueza. Un poco más tarde Robert Solow -premio Nobel, 1987- descubrió y cuantificó el determinante protagonismo del cambio tecnológico en el progreso económico y lo cuantificó en un 85%. Desde entonces la innovación tecnológica se puso muy de moda, incorporando más recientemente el marco institucional – social y político- que la posibilita, según Douglass North -premio Nobel, 1993-.

Partiendo del gran don humano de la creatividad, analizando los ambientes culturales e institucionales que posibilitan su desarrollo, tratando del diálogo de la tecnología con la ciencia, describiendo el funcionamiento de la innovación y también los tan velados como abundantes enemigos de la misma, en el

artículo se llega a la conclusión de que el progreso de la humanidad se produce en última instancia gracias a la libertad -no impedida- de emprendimiento de los seres humanos.

Cuando los emprendedores se encuentran libres de obstáculos para inventar e innovar, se produce el milagro del progreso geométrico de las condiciones de vida de la humanidad e incluso -en contra de los agoreros- la extensión de la oferta de recursos limitados.

PALABRAS CLAVE: Progreso económico y social, calidad de vida, crecimiento económico, innovación tecnológica, cambio tecnológico, destrucción creativa, instituciones sociales y políticas, creatividad humana, ambientes culturales e institucionales, diálogo entre tecnología y ciencia, funcionamiento de la innovación, emprendimiento, libertad de emprendimiento, obstáculos a la innovación, recursos limitados.

ABSTRACT

Economic and social progress has to do with people's standard of living and quality of life. Since it can be described, measured, and compared in historical time and space, we can venture to interpret the keys that determine it.

Until not long ago, in the mid-1940s, the factors that made posible the economic growth that generated the progress of nations were unknown with academic rigor. The great Austrian economist Joseph Schumpeter, with his theory of "creative destruction," had already anticipated the importance of technological innovation in the sustainability of wealth growth. A little later, Robert Solow—Nobel Prize winner, 1987—discovered and quantified the determining role of technological change in economic progress, quantifying it at 85%.

Since then, technological innovation has become very fashionable, more recently incorporating the institutional framework—social and political—that enables it, according to Douglass North—Nobel Prize winner, 1993.

Starting from the great human gift of creativity, analyzing the cultural and institutional environments that enable its development, discussing the dialogue between technology and science, describing the workings of innovation and also its much-disguised yet abundant enemies, the article concludes that human progress ultimately comes about thanks to the unhindered freedom of human entrepreneurship.

When entrepreneurs are free from obstacles to invention and innovation, the miracle of geometric progress in human living conditions occurs, and even—contrary to the prophets of doom—the expansion of the supply of limited resources.

KEYWORDS: Economic and social progress, quality of life, economic growth, technological innovation, technological change, creative destruction, social and political institutions, human creativity, cultural and institutional environments, dialogue between technology and science, functioning of innovation, entrepreneurship, freedom of entrepreneurship, barriers to innovation, limited resources.

IA, EUROPA, ESPAÑA Y EL DILEMA REGULACIÓN-INNOVACIÓN.

AI, Europe, Spain and the regulation-innovation dilemma.

Por Pablo García Mexía

RESUMEN

La inteligencia artificial está considerada como una “tecnología de uso general”, al modo de la electricidad o de Internet. A la vista de sus riesgos, el mundo entero está procediendo a su regulación. El modelo europeo es particularmente importante, por cuanto aspira a convertirse en paradigma global (como sucedió en la regulación europea de otras tecnologías digitales). Este artículo pretende explicar las dificultades de Europa para reducir su distancia respecto de los líderes hegemónicos en digital e IA, que son los EEUU y China, a partir del modelo regulatorio que viene siguiendo. Sin eludir las posibles alternativas en el plano de la regulación, el trabajo expone las medidas que la UE está adoptando al hilo del mandato de la Comisión iniciado en el otoño de 2024. Y concluye describiendo las singularidades de España en estos campos, al tiempo que proponiendo iniciativas que fortalezcan nuestras debilidades en innovación.

PALABRAS CLAVE: Inteligencia artificial (IA), tecnología de uso general, Unión Europea (UE), regulación digital, Reglamento de IA (AI Act), innovación, competitividad, avance digital, soberanía tecnológica, autonomía estratégica, Estados Unidos, China, Comisión Europea, España, liderazgo digital, geopolítica, geoeconomía, defensa.

ABSTRACT

Artificial intelligence is considered a “general-purpose technology”, akin to electricity or the Internet. Given its risks, the entire world is moving toward its regulation. The European model is particularly significant, as it aspires to become a global paradigm (as occurred with the European regulation of other digital technologies). This article aims to explain Europe’s struggle in narrowing the gap with the digital and AI hegemonic leaders—namely the United States and China—based on the

regulatory model it has been pursuing. While tackling possible alternatives in the regulatory sphere, the paper outlines the measures being adopted by the EU under the mandate of the Commission that began in the fall of 2024. It concludes by describing Spain's specific situation in these fields, while also proposing initiatives to address its weaknesses in innovation.

KEYWORDS: Artificial intelligence (AI), general-purpose technology, European Union (EU), digital regulation, AI Act, innovation, competitiveness, digital advancement, technological sovereignty, strategic autonomy, United States, China, European Commission, Spain, digital leadership, geopolitics, geoeconomics, defense.

LA CONSTRUCCIÓN DEL DILEMA ENTRE INNOVACIÓN-REGULACIÓN EN LA NARRATIVA DE LAS BIG TECH: UNA LECTURA CRÍTICA DE LA CORREGULACIÓN TECNOLÓGICA

The construction of the innovation-regulation dilemma in the Big Tech narrative: a critical reading of technological co-regulation.

Por Luis Bouza García

RESUMEN

Este artículo analiza cómo el modelo de corregulación adoptado por la Unión Europea en materia de gobernanza digital ha contribuido a reforzar el poder estructural de las grandes plataformas tecnológicas. A través de un enfoque de

análisis de discursos y marcos, se examina cómo el discurso sobre la necesidad de equilibrar innovación y regulación ha sido moldeado por actores con fuerte capacidad económica, comunicativa y de lobby. Aunque la corregulación se presenta como un mecanismo inclusivo y flexible, en la práctica reproduce asimetrías que otorgan ventaja a los intereses del sector tecnológico, permitiéndoles influir activamente en la elaboración normativa. La narrativa dominante asocia innovación con desregulación y eficiencia, desplazando los debates sobre derechos fundamentales y control democrático. El artículo concluye que el dilema entre innovación y regulación, lejos de ser un conflicto técnico neutral, se ha convertido en una herramienta discursiva que legitima la hegemonía normativa de las big tech. Así, la Unión Europea corre el riesgo de institucionalizar un modelo de gobernanza digital que, en nombre de la competitividad y la innovación, debilita su capacidad para proteger el interés público y garantizar una regulación más democrática.

PALABRAS CLAVE: Corregulación, Innovación, Regulación digital, Plataformas tecnológicas, Poder discursivo.

ABSTRACT

This article analyzes how the co-regulatory model adopted by the European Union in digital governance has reinforced the structural power of major technology platforms. Using a discourse analysis approach, it examines how the discourse around balancing innovation and regulation has been shaped by actors with significant economic, communicative, and lobbying capacity.

While co-regulation is officially presented as an inclusive and flexible mechanism, in practice it reproduces asymmetries that

benefit the tech sector by allowing it to actively influence rule-making. The dominant narrative links innovation with deregulation and efficiency, displacing concerns about fundamental rights and democratic oversight. The analysis concludes that the innovation–regulation dilemma, rather than being a neutral technical conflict, has become a strategic discursive tool that legitimizes the normative dominance of big tech. As a result, the European Union risks institutionalizing a model of digital governance that, in the name of competitiveness and innovation, undermines its ability to protect the public interest and ensure genuinely democratic regulation.

KEYWORDS: Co-regulation, Innovation, Digital regulation, Tech platforms, Discursive power.

INNOVACIONES DISRUPTIVAS Y POLÍTICA CIENTÍFICA: EL ESTANCAMIENTO DE EUROPA

Disruptive innovations and reserach policy: Europe's stagnation

Por Alonso Rodríguez Navarro

RESUMEN

Las innovaciones disruptivas son una base importante en la economía de los países desarrollados, que se originan a partir de los avances científicos producidos por una investigación muy competitiva en la frontera del conocimiento. En una primera parte, este artículo describe cómo medir esa investigación competitiva, que es el primer paso para el desarrollo de políticas científicas que conduzcan a avances científicos disruptivos. En la segunda parte se explican los

errores cometidos durante 30 años por la Comisión Europea, midiendo mal la contribución de la UE al avance en la frontera del conocimiento, que confunde y mezcla con los desarrollos incrementales. En el nivel disruptivo, la UE compite mal con EEUU y China, y los errores de medida están impidiendo el desarrollo de una política científica europea que corrija el retraso, especialmente en las tecnologías actualmente más importantes. Tomando como modelo España, la excesiva concentración de la ciencia europea en desarrollos incrementales se puede explicar por la política científica que lleva a los investigadores a evitar el riesgo de publicar poco. Cuando la investigación se dirige al avance de la frontera del conocimiento el riesgo es más alto, sobre todo en las ya mencionadas tecnologías importantes, donde la competencia es muy alta.

PALABRAS CLAVE: innovaciones disruptivas, investigación disruptiva, medidas de la ciencia.

ABSTRACT

Disruptive innovations are a crucial component of the economies of developed countries, originating from scientific breakthroughs produced by highly competitive research at the forefront of knowledge. In its first part, this article describes how to measure this competitive research, which is the first step toward developing scientific policies that lead to disruptive scientific breakthroughs. The second part explains the mistakes the European Commission has made over 30 years, misjudging the EU's contribution to advancing the frontier of knowledge, confusing and conflating it with incremental developments. At the disruptive level, the EU competes poorly with the USA and China, and measurement errors are impeding

the development of a European science policy that would correct the gap, especially in the currently most important technologies. Taking Spain as a model, the excessive concentration of European science on incremental developments can be explained by a scientific policy that leads researchers to avoid the risk of publishing little. When research is aimed at advancing the frontiers of knowledge, the risk is higher, especially in the aforementioned key technologies, where competition is very intense.

KEYWORDS: disruptive innovations, disruptive research, science metrics.

Número 36

CARTA DEL DIRECTOR

Por Pablo García Mexía

¿QUO VADIS PROTECCIÓN DE DATOS?

Quo vadis, data protection?

Por José Luis Piñar

TRANSPARENCIA Y PROTECCIÓN DE DATOS EN EL USO DE LA INTELIGENCIA ARTIFICIAL POR LA ADMINISTRACIÓN PÚBLICA

Transparency and data protection on the use of Artificial Intelligence by public administrations

Por Manuel Bellón Yturriaga

RESUMEN

Este trabajo tiene como objeto analizar el concepto multifacético de transparencia en relación con la inteligencia artificial del que ha venido haciendo uso la doctrina y ver en qué medida se puede ver reflejado en las normativas nacionales y europeas de transparencia y protección de datos personales, respectivamente. La conclusión alcanzada en el presente trabajo apunta a que la legislación española aún debe abordar la definición y establecimiento de garantías adecuadas respecto al uso de la inteligencia artificial en el ámbito de las Administraciones públicas.

PALABRAS CLAVE: protección de datos, inteligencia artificial, transparencia, explicabilidad, machine learning, deep learning, administración pública.

ABSTRACT

This paper aims to analyze the multifaceted concept of transparency regarding artificial intelligence, as discussed in scholarly literature, and to examine the extent to which it is reflected in national and european regulations on transparency and personal data protection, respectively. The conclusion reached in this study suggests that Spanish legislation must still address the definition and establishment of adequate safeguards regarding the use of artificial intelligence within public administrations.

KEYWORDS: data protection, artificial intelligence, transparency, explainability, machine learning, deep learning, public administration.

LA VALIDEZ DEL CONSENTIMIENTO OTORGADO EN LOS COOKIE PAYWALLS DESDE LA PERSPECTIVA DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

The validity of consent in cookie paywalls under data protection law

Por Antonio Emilio Borjas

RESUMEN

Durante el último año, diversos titulares de páginas web y aplicaciones han implementado modelos de consentimiento o pago para restringir el acceso a sus servicios. Estos modelos requieren que el usuario, para acceder a la página web o aplicación, acepte la instalación de cookies o tecnologías similares utilizadas para ofrecerle publicidad personalizada o, en su defecto, pague una tarifa que le permite acceder rechazando el uso de dicha tecnología. Este nuevo escenario, impulsado por recientes resoluciones europeas, genera incertidumbre sobre si el consentimiento otorgado por los usuarios en el marco de estos modelos cumple con la normativa de protección de datos personales.

Considerando este nuevo panorama de publicidad digital, el presente artículo analiza la validez del consentimiento otorgado en los modelos de consentimiento o pago y, en su caso, los requisitos que debe cumplir para que sea conforme con la normativa aplicable.

PALABRAS CLAVE: consentimiento, muros de cookies, publicidad comportamental, plataformas en línea de gran tamaño.

ABSTRACT

Over the past year, various website and app owners have implemented consent or pay models to restrict access to their services. These models require users to either accept the installation of cookies or similar technologies used to offer personalized advertising, or alternatively, pay a fee that allows access while rejecting the use of such technology. This new scenario, driven by recent European decisions, creates uncertainty about whether the consent given by users under these models complies with personal data protection regulations. Considering this new digital advertising landscape, this article assesses the validity of consent given under consent or pay models and, if applicable, the requirements it shall meet to comply with the relevant regulations.

KEYWORDS: consent, cookie paywalls, behavioural advertising, very large online platforms.

EL PACTO DIGITAL MUNDIAL DE LAS NACIONES UNIDAS **The United Nations Global Digital Compact**

Por Jorge Pérez Martínez

RESUMEN

En este artículo se analiza el Pacto Digital Mundial, recientemente aprobado en el seno de Naciones Unidas. El pacto es un conjunto de principios, objetivos y acciones, acordados por los Estados, que deben servir de guía a los gobiernos, empresas, sociedad civil y otros actores interesados, en la construcción de un futuro digital más equitativo y sostenible. Su importancia radica en que se trata del primer acuerdo firmado por todos los gobiernos soberanos del mundo, para la cooperación internacional en la gobernanza del ecosistema digital global. Para entender el pacto es

necesario analizar previamente la evolución del ecosistema digital que se construyó entre 2000 y 2017 en un contexto de confianza geopolítica. Esta confianza se vio truncada en 2017 con la elección de Donald Trump como presidente de Estados Unidos. Comprender estos antecedentes nos permitirá describir mejor el contenido del pacto y ofrecer una evaluación crítica del mismo.

PALABRAS CLAVE: Pacto Digital Mundial, gobernanza digital, ecosistema digital global, brecha digital.

ABSTRACT

This article analyzes the Global Digital Compact, recently approved within the United Nations. This compact is a set of principles, objectives, and actions agreed upon by states, intended to serve as a guide for governments, businesses, civil society, and other stakeholders in building a more equitable and sustainable digital future. Its importance lies in the fact that it is the first agreement signed by all sovereign governments in the world for international cooperation in the governance of the global digital ecosystem. To understand the compact, it is necessary to first analyze the evolution of the digital ecosystem, which was built between 2000 and 2017 in a context of geopolitical trust. This trust was broken in 2017 with the election of Donald Trump as President of the United States. Understanding this background will allow us to better describe the compact's content and provide a critical assessment of it.

KEYWORDS: Global Digital Compact, digital governance, global digital ecosystem, digital gap.

RECREACIONES PÓSTUMAS: SUS IMPLICANCIAS ÉTICAS Y JURÍDICAS

Posthumous Deepfakes: Their Ethical and Legal implications

Por Marcela Paz Sánchez Sarmiento y Diego Francisco Idrovo Torres

RESUMEN

El avance acelerado de la tecnología ha transformado la interacción humana en el ámbito digital. Uno de los fenómenos recientes es el surgimiento de las recreaciones póstumas, herramientas de inteligencia artificial que permiten manipular imágenes, videos, y audios para crear representaciones falsificadas de personas y situaciones. En este contexto, el uso de recreaciones plantea cuestionamientos sobre los límites entre lo real y lo ficticio, y la necesidad de establecer marcos regulatorios que protejan los derechos fundamentales de los individuos.

Este estudio examina las implicaciones jurídicas y constitucionales de las recreaciones, con un enfoque en la protección de la identidad digital, la honra, y el buen nombre, así como en los derechos a la intimidad y el consentimiento informado.

PALABRAS CLAVE: recreaciones póstumas, identidad digital, derecho a la honra, derecho a la intimidad, autodeterminación informativa.

ABSTRACT

The accelerated advancement of technology has transformed human interaction in the digital realm. One of the recent phenomena is the emergence of deepfakes, artificial

intelligence tools that allow images, videos, and audios to be manipulated to create falsified representations of people and situations. In this context, the use of deepfakes raises questions about the boundaries between the real and the fictional, and the need to establish regulatory frameworks that protect the fundamental rights of individuals. This study examines the legal and constitutional implications of deepfakes, with a focus on the protection of digital identity, honor, and good name, as well as the rights to privacy and informed consent.

KEYWORDS: posthumous deepfakes, digital identity, right to honor, right to privacy, informational self-determination.

EL URBANISMO ECOSISTÉMICO: SOSTENIBILIDAD Y REDUCCIÓN DE LA INCERTIDUMBRE

Por Roberto O. Bustillo Bolado y Paula Gamallo Carballude

ENCUESTA N° 36. PRIMERA GUÍA PRÁCTICA DE CIBERSEGURIDAD PARA LA ABOGACÍA

Por Mabel Klimt

EN RED N° 36

Año 2024

Número 35

CARTA DEL DIRECTOR

Por Pablo García Mexía

LA UNIVERSIDAD Y LA IA: EJEMPLO DE ESFUERZO, EMPUJE Y OPORTUNIDAD DE AVANCE. University and AI: Example of effort, drive and opportunity of advancement.

Por Pedro García Teodoro

PROTECCIÓN DE LAS PRODUCCIONES ALGORÍTMICAS EN LOS SISTEMAS COMMON LAW: CASOS ACTUALES Protection of algorithmic productions in Common Law Systems: current cases.

Por Rosa M.^a García Pérez

RESUMEN

Los modelos de inteligencia artificial generativa cuentan con capacidad para producir, de manera autónoma e independiente de la intervención humana, resultados o contenidos que formalmente encajan en el concepto de «obra». El avance tecnológico impulsado por la inteligencia artificial es profundo y estructural, constituyendo su impacto en el sector artístico todo un desafío en orden a determinar cómo conciliar la integración de estos modelos inteligentes en el proceso creativo con los actuales pilares normativos que sustentan el derecho *de autor*. Este trabajo se propone analizar la respuesta dada, principalmente, desde la perspectiva de los ordenamientos jurídicos de tradición «common law», a las solicitudes de reconocimiento y protección a través del derecho de autor de los resultados generados (outputs) por los modelos de inteligencia artificial. La elección de navegar por las

complejidades de los marcos regulatorios de los sistemas de copyright obedece a que, en estas jurisdicciones, la controversia sobre la materia se ha institucionalizado y judicializado, con mayor intensidad que en los sistemas de «droit d'auteur», de enfoque personalista más acusado. El estudio de los casos y de las demandas actualmente planteadas, sin duda, contribuirá a despejar incertidumbres y avanzar en la búsqueda de soluciones que respeten el equilibrio de los diversos intereses en conflicto.

PALABRAS CLAVE: Derecho de autor y obras generadas por inteligencia artificial: casos actuales controvertidos; Autoría y «prompts»; Titularidad de obras e inteligencia artificial generativa; Registro de producciones algorítmicas en sistemas «common law».

LA NUEVA DIRECTIVA DE PRODUCTOS DEFECTUOSOS EN EL CONTEXTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: ESPECIAL CONSIDERACIÓN AL PRODUCTO SANITARIO.

The new directive on defective products in the context of the artificial intelligence act: special consideration for medical device.

Por María Jorqui Azofra

RESUMEN

La nueva Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo, responde a varias cuestiones planteadas por las características específicas y riesgos de las nuevas tecnologías, incluida la inteligencia artificial, así como a los cambios derivados de los nuevos

modelos de negocio de la economía circular y de las cadenas de suministro mundiales. Este trabajo tiene como objetivo examinar los principales cambios introducidos por dicha Directiva. Se examinan también, a la luz de estos, algunas cuestiones que pueden plantearse cuando el producto es un sistema de inteligencia artificial de alto riesgo utilizado en personas con un fin médico específico; esto es, cuando es un producto sanitario.

PALABRAS CLAVE: Producto, sistema de inteligencia artificial, producto sanitario, evaluación de la conformidad, operador económico, responsabilidad por productos defectuosos, componente.

ABSTRACT

The new Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, addresses various issues raised by the specific characteristics and risks of new technologies, including artificial intelligence, as well as changes resulting from new business models in the circular economy and global supply chains. The objective of this study is to examine the main changes introduced by this Directive. It also examines, considering these changes, certain issues that may arise when the product is a high-risk artificial intelligence system used on individuals for a specific medical purpose; that is, when it is a medical device.

KEYWORDS: Product, artificial intelligence system, medical device, conformity assessment, economic operator, liability for defective products, component

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS ANTE LOS DESAFÍOS TECNOLÓGICOS: LA ARQUITECTURA DE LA RESPONSABILIDAD Y DE LA INDEMNIZACIÓN DEL DAÑO INMATERIAL EN CASO DE CIBERATAQUE *The General Data Protection Regulation and technological challenges: the architecture of responsibility and compensation of non-material damages in the event of a cyberattack.*

Por Simona Fanni

RESUMEN

El asunto VB c. Natsionalna agentsia za prihodite ha ofrecido al Tribunal de Justicia de la Unión Europea (TJUE) la oportunidad de pronunciarse sobre cuestiones cruciales como la responsabilidad del responsable del tratamiento y la indemnización de los daños y los perjuicios inmateriales en el evento de un ciberataque, en el marco del Reglamento General de Protección de Datos. El presente estudio analiza detenidamente la decisión del TJUE, y formula una serie de observaciones y propuestas críticas, sugiriendo también la posibilidad de enriquecer la visión desarrollada en la sentencia a través de un enfoque basado en los derechos y las libertades fundamentales, en virtud del diálogo judicial entre el TJUE y el Tribunal Europeo de Derechos Humanos.

PALABRAS CLAVE: Responsabilidad proactiva; daños inmateriales; ciberataque; principio de efectividad y principio de equivalencia; derechos y libertades fundamentales.

ABSTRACT

In the case VB vs. Natsionalna agentsia za prihodite, the Court of Justice of the European Union (CJEU) has had the opportunity to express its view on several crucial issues, such as the

responsibility of the data controller and the compensation for non-material damage in the event of a cyberattack, in the framework of the General Data Protection Regulation. This study thoroughly analyses the decision of the CJEU, in order to make some critical remarks and advance several critical proposals, by also suggesting that the adoption of a human rights-based approach, throughout judicial dialogue between the CJEU and the European Court of Human Rights, would help to enhance the results achieved in the ruling.

KEYWORDS: Proactive responsibility; non-material damages; cyberattack; principles of effectiveness and equivalence; fundamental rights and freedoms

EL CENTRO NACIONAL DE INTELIGENCIA: LÍMITES DERIVADOS DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES National Intelligence Center: limits arising from the fundamental right to the protection of personal data

Por Gonzalo Menéndez Margolles

RESUMEN

Las actividades de Inteligencia cobran cada vez más importancia debido al desarrollo tecnológico, reactivando el debate entre privacidad y seguridad. En España, el Centro Nacional de Inteligencia es la entidad responsable de proporcionar al Gobierno la información necesaria para prevenir y evitar ataques contra la Seguridad Nacional. Para ello, dicho Centro necesita, en muchos casos, tratar datos personales, afectando así al derecho fundamental que los protege y exigiendo efectuar una ponderación entre los

derechos e intereses en juego. Sin embargo, en ocasiones, la Seguridad Nacional ha sido utilizada como pretexto para actuaciones desproporcionadas y abusivas. En este sentido, el presente artículo estudia cuáles son las normas aplicables a los tratamientos de datos personales efectuados por el Centro Nacional de Inteligencia, identificando sus posibles especialidades derivadas de su particular naturaleza y sensibilidad y, en concreto, los límites que imponen a esos tratamientos para proteger a los ciudadanos frente a abusos.

PALABRAS CLAVE: Inteligencia, datos personales, Centro Nacional de Inteligencia, información clasificada.

ABSTRACT

Intelligence activities are becoming increasingly important due to technological development, reactivating the debate between privacy and security. In Spain, the National Intelligence Center is the entity responsible for providing the Government with the information required to prevent and avoid attacks against National Security. For that, in many cases, said Center needs to process personal data, causing an impact in the fundamental right that protects them and demanding a balancing test between the rights and interests at stake. However, National Security has sometimes been used as a pretext for disproportionate and abusive actions. In this regard, this article would examine which are the regulations applicable to the processing of personal data conducted by the National Intelligence Center, identifying their potential specialties arising from their particular nature and sensitivity, specifically the limits they impose to those processing activities in order to protect citizens from abuses.

KEYWORDS: Intelligence, personal data, National Intelligence Center, classified information.

POSIBLES VÍAS DE EVITAR LA APLICACIÓN DEL REGLAMENTO DE IA ¿VEREMOS UNA NUEVA “HUIDA” DEL DERECHO? Possible ways to avoid the application of the IA Act. Will we see a new "escape" from the law?

Por Carlos Fernández Hernández y Josu Andoni Eguiluz Castañeira

ENCUESTA N° 35. TECNOLOGÍA, REGULACIÓN Y PRIVACIDAD

Por José Javier Martínez Herraiz

EN RED N° 35

Número 34

CARTA DEL DIRECTOR

Por Pablo García Mexía

DEL REGLAMENTO EUROPEO DE LA IA HACIA LA NECESARIA GOBERNANZA GLOBAL From the European AI Regulation to the necessary global governance.

Por Carme Artigas

UNA DOBLE HISTORIA DE LA INTELIGENCIA ARTIFICIAL: AVANCE TECNOLÓGICO Y PROCESO DE REGULACIÓN EN EUROPA A double history of Artificial Intelligence: technological advance and regulation process in Europe.

Por Ana María de Marcos Fernández

RESUMEN

La gran convulsión que supuso el lanzamiento, en noviembre de 2022, de ChatGPT volvió a poner en el primer plano de la actualidad y del interés social tanto el concepto de inteligencia artificial como las implicaciones que el desarrollo de la misma tiene en todos los órdenes de la vida. Pero la presentación del chatbot conversacional de lenguaje natural de la compañía OpenAI, a pesar de su importancia e impacto, no fue más que un nuevo paso en la evolución de una disciplina, la inteligencia artificial, cuyos orígenes científicos y tecnológicos se encuentran en la primera mitad del siglo XX. La primera parte de este artículo resume la evolución de la inteligencia artificial a partir de entonces y hace mención de los principales hitos de la misma, que han ido desde los primeros y sencillos modelos de robots hasta los asistentes avanzados de la actualidad, pasando por la propia acuñación del concepto inteligencia artificial en los años 50, los algoritmos de aprendizaje automático, el aprendizaje profundo, los transformadores y los grandes modelos de lenguaje, entre otros avances fundamentales. La segunda parte del artículo se refiere al proceso de elaboración de la regulación de la inteligencia artificial por parte de las instituciones europeas, a partir de 2018, que culmina con la aprobación del Reglamento de la IA en la Eurocámara el 13 de marzo de 2024, y por el Consejo el 21 de mayo de 2024. Su publicación en el Diario Oficial de la Unión Europea se produce el 12 de julio de 2024, si bien su entrada en vigor tendrá lugar de forma escalonada según las distintas materias que son objeto de su regulación. La regulación europea de la IA se centra en la excelencia y la confianza, con el objetivo de impulsar la investigación y la capacidad industrial, garantizando al mismo tiempo la seguridad y los derechos fundamentales. Pretende conseguir el liderazgo mundial estratégico de Europa en relación con una

IA fiable, y centrada en el ser humano, que permita la innovación tecnológica y garantice la vigencia del Estado de Derecho y la democracia.

PALABRAS CLAVE: Inteligencia artificial (IA), aprendizaje automático, sistema experto, grandes modelos de lenguaje, Estrategia europea de inteligencia artificial, Ley de inteligencia artificial, Reglamento europeo de inteligencia artificial, Responsabilidad derivada de inteligencia artificial, Oficina europea de inteligencia artificial.

ABSTRACT

The upheaval caused by the launch, in November 2022, of ChatGPT brought back to the forefront of current affairs and social interest both the concept of artificial intelligence and the implications of its development for all aspects of life. But despite its importance and impact, the introduction of OpenAI's natural language conversational chatbot was just a new step in the evolution of a discipline - artificial intelligence - whose scientific and technological roots are to be found in the first half of the 20th century. The article contains two main parts, and the first one summarizes the evolution of artificial intelligence since then, and highlights its main milestones, ranging from the first simple robot models to current advanced assistants, with the very emergence of the artificial intelligence concept in the 1950s, machine learning algorithms, deep learning, transformers and large language models, among other fundamental steps, coming in between. The second part deals with the process of elaboration of the regulation of artificial intelligence by the European institutions, starting in 2018 and culminating in the adoption of the AI Regulation in the European Parliament on March 13, 2024, and by the Council on

May 21, 2024. The Regulation was published in the Official Journal of the European Union on July 12, 2024, although it will come into force on a step-by-step basis according to the different matters that are the subject of its regulation. The European regulation of AI focuses on excellence and trust, with the aim of boosting research and industrial capacity, while ensuring safety and fundamental rights. It aims to achieve Europe's strategic global leadership in trusted, human-centered AI, at the same time enabling technological innovation and ensuring the rule of law and democracy.

KEY WORDS: Artificial intelligence (AI) machine learning, expert system, large language models, European Artificial Intelligence Strategy, Artificial Intelligence Act, European Artificial Intelligence Regulation, Liability arising from Artificial Intelligence, European Office for Artificial Intelligence.

OBLIGACIONES DE LOS PROVEEDORES DE SISTEMAS DE IA Obligations of the AI Systems Providers.

Por Ricardo Rivero Ortega

RESUMEN

La regulación europea de la Inteligencia Artificial establece una serie de obligaciones informativas y técnicas para posibilitar el control de los proveedores de sistemas. Ante una normativa tan prolija, se hace necesario definir correctamente su alcance, límites y garantías favorables a la iniciativa e innovación de las empresas, así como precisar su aplicabilidad a los poderes públicos.

PALABRAS CLAVE: Regulación de la inteligencia artificial, obligaciones de los proveedores de IA, evaluación de conformidad.

ABSTRACT

The european regulation of AI establish information obligations of providers and techniques to enable its control. Given so much complex regulations, a correct definition of its scope, limits and favorable guarantees for the initiative and innovation of compa nies is necessary, as well as specifying its applicability to public powers.

KEYWORDS: AI Regulation; AI providers obligations; conformity assessment procedure.

USUARIOS DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL Y SUS OBLIGACIONES

Users of Artificial Intelligence systems and their obligations.

Por Mercedes Fuertes López

RESUMEN

La autora analiza en este estudio las obligaciones específicas que han de cumplir los usuarios de los sistemas de inteligencia artificial teniendo en cuenta las diversas categorías de riesgos que presentan tales sistemas y las moratorias para la efectiva aplicación del Reglamento europeo previstas.

PALABRAS CLAVE: Sistemas de Inteligencia Artificial. Usuarios de los sistemas de inteligencia artificial. Obligaciones de los usuarios. Responsables del despliegue de sistemas de inteligencia artificial. Obligaciones de los responsables del

despliegue. Sistemas de inteligencia artificial de riesgo alto. Moratoria del Reglamento.

ABSTRACT

In this study, the author analyses the specific obligations to be met by users of artificial intelligence systems, taking into account the various categories of risks posed by such systems and the expected moratoriums on the effective application of the European Regulation.

KEYWORDS: Artificial Intelligence Systems. Users of artificial intelligence systems. Obligations of users. Deployers of artificial intelligence systems. Obligations of those responsible for deployment. High-risk artificial intelligence systems. Moratorium on the Regulation.

SISTEMAS DE IA PROHIBIDOS, DE ALTO RIESGO, DE LIMITADO RIESGO, O DE BAJO O NULO RIESGO
Prohibited, high-risk, limited risk, or minimal or no risk ai systems.

Por Martín María Razquin Lizarraga

RESUMEN

La LIA regula los sistemas de IA desde la perspectiva del riesgo y por tanto los clasifica en sistemas de IA prohibidos, de alto riesgo o de bajo o nulo riesgo. Quedan prohibidas las prácticas de IA que supongan riesgos inadmisibles, salvo algunas excepciones. La categoría principal es la de sistemas de IA de alto riesgo, que vienen enumerados en función de su inclusión en normas sobre productos o en razón de criterios horizontales. Se permite su introducción en el mercado, comercialización y uso de los sistemas de IA de alto riesgo,

previo cumplimiento de diversos requisitos y obligaciones relevantes para los operadores. Por el contrario, los sistemas de bajo o nulo riesgo quedan sólo vinculados al cumplimiento voluntario de códigos de conducta.

PALABRAS CLAVE: Ley de Inteligencia Artificial, inteligencia artificial, sistemas de IA prohibidos, sistemas de IA de alto riesgo.

ABSTRACT

AIA regulates AI systems from a risk perspective and therefore reclassifies them into prohibited, high risk, or low or no risk AI systems. AI practices that suppose unacceptable risks are prohibited, with some exceptions. The main category is high-risk AI systems, which are listed based on their inclusion in products standard or based on horizontal criteria. High-risk systems are permitted to be introduced into the market, commercialized and used, subject to compliance with various relevant requirements and obligations for operators. On the contrary, minimal or no risk systems are only linked to voluntary compliance with codes of conduct.

KEY WORDS: Artificial Intelligence Act, artificial intelligence, prohibited AI systems, high-risk AI systems.

RIESGOS DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL GENERATIVA Y EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL EUROPEO

Risks of generative artificial intelligence systems and the European Artificial Intelligence Regulation

Por M^a Jesús Jiménez Linares

RESUMEN

La inteligencia artificial generativa permite la creación automática de contenido “original” en diferentes formatos (texto, audio, vídeo e imágenes). Un contenido que cada vez se acerca más al creado por los humanos. La inteligencia artificial generativa ofrece a la sociedad tantos beneficios como posibles riesgos. Se analizarán algunos como la confusión, la desinformación, los riesgos de los derechos de autor, a la seguridad, a la privacidad, la ciberdelincuencia, al derecho al honor, la intimidad y la propia imagen que pueden lesionarse con los deepfakes, la manipulación, los riesgos en el mercado laboral, los psicológicos, los sesgos...El nuevo Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) acoge la inteligencia artificial generativa dentro de la inteligencia de uso general, teniendo en cuenta la presencia, de posibles riesgos sistémicos y la exigibilidad de la ciberseguridad. Se analizará también la conexión de la inteligencia artificial generativa con la prohibida y la de alto riesgo. El Reglamento muestra especial preocupación ante las “ultrasuplantaciones”, deepfakes (donde es difícil distinguir entre lo real y lo irreal), y el necesario conocimiento de su origen artificial cuando las personas físicas interactúen con ellas, con la correspondiente obligación de transparencia. Todo ello, sin olvidar, la necesidad de hacer lo ético jurídico y de la alfabetización.

PALABRAS CLAVE: Inteligencia artificial generativa, riesgos, desinformación, seguridad, privacidad, ciberseguridad, transparencia, deep fakes, ultrasuplantaciones, riesgos sistémicos, ley de inteligencia artificial.

ABSTRACT

Generative artificial intelligence allows the automatic creation of "original" content in different formats (text, audio, video and images). Content that is getting closer and closer to that created by humans. Generative artificial intelligence offers society as many benefits as possible risks. Some will be analysed such as confusion, disinformation, copyright risks, security, privacy, cybercrime, the right to honour, privacy and self-image that can be injured by deep fakes, manipulation, risks in the labour market, psychological risks, bias... The new Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) welcomes generative artificial intelligence within general purpose intelligence, considering the presence of possible systemic risks and the enforceability of cybersecurity. The connection of generative artificial intelligence with prohibited and high-risk artificial intelligence will also be analysed. The Regulation shows special concern for "ultra-phishing", deep fakes (where it is difficult to distinguish between the real and the unreal), and the necessary knowledge of their artificial origin when natural persons interact with them, with the corresponding obligation of transparency. All this, without forgetting the need for legal ethics and literacy.

KEY WORDS: Generative artificial intelligence, risks, disinformation, security, privacy, cybersecurity, transparency, deep fakes, ultra spoofing, systemic risks, artificial intelligence law.

LA INNOVACIÓN EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

Por Pablo García Mexía

Número 33

CARTA DEL DIRECTOR

Por Pablo García Mexía

LEY DE DATOS, INNOVACIÓN Y COMPETITIVIDAD

Data Act, innovation and competitiveness.

Por Pilar del Castillo Vera

ANÁLISIS DE LA PROPUESTA DE REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL.

Analysis of the proposal for a European Regulation on Artificial Intelligence.

Por María Loza Corera

RESUMEN

Asistimos actualmente a una carrera por la regulación en materia de inteligencia artificial que Europa está firmemente decidida a liderar, consciente de sus limitaciones en materia de soberanía tecnológica. Europa ha tenido claro desde un inicio que debían marcarse unos límites para preservar la salud, seguridad y los derechos fundamentales de las personas frente al desarrollo de los sistemas de IA y ha elaborado una propuesta normativa horizontal para garantizar su protección. La propuesta de reglamento europeo de inteligencia artificial se articula sobre un enfoque basado en el riesgo y el sistema de evaluación de la conformidad proveniente de la normativa europea sobre seguridad de los productos, para establecer normas armonizadas que garanticen el marco jurídico único

necesario para el funcionamiento del mercado interior. A pesar de que solo el tiempo dirá si el enfoque europeo es lo suficientemente flexible para permitir la innovación a la par que conseguir dichos objetivos y de que el texto es mejorable en determinados aspectos, se trata de un buen punto de partida que previsiblemente tendrá un importante impacto a nivel mundial.

PALABRAS CLAVE: Inteligencia Artificial, reglamento, normas armonizadas, sistemas de inteligencia artificial, sistemas de alto riesgo.

ABSTRACT

We are currently witnessing a race to regulate artificial intelligence that Europe is firmly determined to lead, aware of its limitations in terms of technological sovereignty. Europe has been clear from the outset that limits must be set to preserve the health, safety and fundamental rights of individuals in the face of the development of AI systems and has drawn up a horizontal regulatory proposal to ensure their protection. The proposal for a European regulation on artificial intelligence is based on a risk-based approach and the conformity assessment system stemming from European legislation on product safety, in order to establish harmonised rules that guarantee the single legal framework necessary for the functioning of the internal market. Although only time will tell whether the European approach is flexible enough to allow for innovation while achieving these objectives and the text can be improved in certain respects, it is a good starting point that is likely to have a major impact at the global level.

KEY WORDS: Artificial Intelligence, regulation, harmonized rules, artificial intelligence systems, high risk systems.

LA GOBERNANZA Y LEGITIMIDAD DE LA INTELIGENCIA ARTIFICIAL Governance and Legitimacy of Artificial Intelligence.

Por Olga Gil

RESUMEN

Ante los desafíos para la humanidad de los desarrollos disruptivos de la inteligencia artificial, este trabajo plantea discusiones desde diferentes perspectivas, que permiten dialogar con científicos de diferentes campos, gobiernos, empresas y otros actores sociales sobre cuestiones relacionadas con la gobernabilidad y la legitimidad. El objetivo principal y el resultado del artículo es presentar un panel de control para el análisis de la gobernabilidad y la legitimidad de la inteligencia artificial, al que se denomina Gil Dashboard o Panel Gil. Este panel de control trata de resolver disputas de teoría política partiendo de enfoques clásicos para estudiar la gobernabilidad y la legitimidad. El panel de control también permite comparaciones de la gobernabilidad y la legitimidad de la IA en regímenes democráticos y no democráticos, en diferentes niveles de gobierno – tanto en los países Occidentales como en el Sur Global. Un resultado adicional es la aplicación del Panel al caso de China como estudio de caso. La aplicación del Panel de control permite 1) mostrar su valor como herramienta metodológica y analítica y 2) arrojar una nueva mirada interpretativa y sugerente a los datos existentes en el caso chino.

PALABRAS CLAVE: Inteligencia artificial; gobernanza; filosofía; ética; teoría política; China.

ABSTRACT

Amids challenges posed to humanity by artificial intelligence disruptive developments, this work is set to engage discussants from different perspectives -encompassing scientists in different fields, governments, firms and other social actors- on the topics of artificial intelligence, governance and legitimacy. The main aim and output of the paper is to present a dashboard for the analysis of governance and legitimacy of artificial intelligence. This Dashboard resolves disputes within the literature on political theory over classical approaches to study governance and legitimacy. The Dashboard has also the capacity to allow for comparisons in AI governance and legitimacy in democratic and non democratic regimes, at different government levels, both in Western Countries and in the Global South. An additional output is the application of the framework to the case of China as a case study. This analysis is carried out by applying the framework to take a fresh look at existing data in the Chinese case and showing its value as a methodological and analytical tool.

KEYWORDS: Artificial intelligence; governance; philosophy; ethics; political theory; China.

LA IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO CIVIL: RETOS Y OPORTUNIDADES

The Irruption of Artificial Intelligence in Civil Proceedings: Challenges and Opportunities.

Por Ana Garmendia Prieto

RESUMEN

El uso de Inteligencia Artificial por la administración de justicia puede agruparse fundamentalmente en dos grupos: el uso en

la tramitación procesal, y el derivado de la irrupción de la Inteligencia Artificial en el proceso civil, entendido como el instrumento fundamental para la demostración material de los hechos según ocurrieron o el establecimiento formal de los mismos para la resolución del litigio. Como pone de manifiesto el Reglamento IA, el uso de la Inteligencia Artificial en el seno de la administración de justicia y, en particular, el utilizado para asistir a la autoridad judicial o competente para resolver alternativamente la disputa, así como a quienes actúan en su nombre a investigar e interpretar los hechos y/o la ley así como en su aplicación a hechos concretos, es un uso de “algo riesgo”, donde la trascendencia de las implicaciones de la Inteligencia Artificial puede tener mayores repercusiones y donde las obligaciones que deben cumplir quienes las utilicen son de mayor calado (formal y material). No obstante, y a pesar de las dificultades que comporta, es evidente que la Inteligencia Artificial ha venido para quedarse, también en el seno de la Administración de Justicia y de la cotidianeidad de la función de los distintos operadores jurídicos. Esta realidad, nos obliga a todos los que formamos parte de este “baile” a cuestionarnos sobre los riesgos que ello implica, sobre la reacción y las dificultades que se plantean cuando esta tecnología choca con nuestra legislación actual y a encontrar soluciones que faciliten la convivencia legítima y pacífica de la actividad judicial con esta nueva herramienta.

PALABRAS CLAVE: Inteligencia Artificial, Inteligencia Artificial Generativa; justicia; Administración de justicia; proceso civil; prueba.

ABSTRACT

The use of Artificial Intelligence by the judiciary can be fundamentally grouped into two categories: its use in

procedural processing, and that arising from the advent of Artificial Intelligence in civil proceedings, understood as the fundamental instrument for the material demonstration of facts as they occurred or their formal establishment for dispute resolution. As highlighted by the AI Regulation, the use of Artificial Intelligence within the judiciary, particularly that used to assist the judicial or competent authority in alternative dispute resolution, as well as those acting on its behalf in investigating and interpreting facts and/or the law, and in their application to specific facts, is a “somewhat risky” use, where the significance of the implications of Artificial Intelligence can have greater repercussions and where the obligations to be fulfilled by those using it are of greater depth (both formal and material). However, despite the difficulties it entails, it is evident that Artificial Intelligence is here to stay, also within the Judiciary and in the daily routine of the various legal operators. This reality obliges all of us who are part of this “dance” to question the risks it entails, the reaction and difficulties that arise when this technology clashes with our current legislation, and to find solutions that facilitate the legitimate and peaceful coexistence of judicial activity with this new tool.

KEY WORDS: Artificial Intelligence; Generative Artificial Intelligence; Justice; Administration of Justice; civil procedure; evidence.

TECNOLOGÍAS DIGITALES PARA LOCALIZAR DE BIENES Y DERECHOS EMBARGABLES MÁS ALLÁ DE LA FUTURA REFORMA DEL PUNTO NEUTRO DE EMBARGOS.

Digital technologies to locate seizable rights and assets beyond the future reform of the Neutral Seizure Point.

Por Marina Serrat Romani

ENCUESTA N° 33

PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVA A LA RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS (2022/0302 [COD])

Proposal for a Directive of the European Parliament and of the Council on liability for defective products.

Por Joaquín Fernández

EN RED N° 33

Año 2023

Número 32

CARTA DEL DIRECTOR

Por Pablo García Mexía

La cartera de identidad digital europea y el principio de “Solo una vez” en el Derecho Español.

The European Digital Identity wallet and the «once-only» principle in Spanish Law

Por José María Delgado Báidez.

RESUMEN

La cartera de identidad digital europea prevista en la Propuesta de modificación del Reglamento eIDAS (conocida como Reglamento eIDAS 2) otorgará a los ciudadanos el control absoluto sobre los atributos de su identidad digital y sus datos

de carácter personal. Este revolucionario cambio de enfoque sobre el tratamiento de la información personal de los ciudadanos aconseja llevar a cabo un examen de las eventuales repercusiones que esta herramienta digital puede tener sobre la forma en la que el legislador español ha regulado el principio de “solo una vez” en nuestro Derecho.

ABSTRACT

The European digital identity wallet regulated by the Proposal for amending Regulation eIDAS (also known as Regulation eIDAS 2) will provide European citizens with absolute control over their online identity and personal data. This revolutionary approach to processing citizens' data needs an analysis of the potential repercussions it may have on traditional regulation of the “once only” principle in our Law.

Inteligencia artificial y Administración de Justicia. Artificial Intelligence and Administration of Justice

Por José Díaz Cappa

RESUMEN

Si existe una disciplina humana en la que la trascendencia de las implicaciones de la Inteligencia Artificial (IA) sobre la misma puede suponer grandes repercusiones a modo de cambios personales, sociales o políticos de gran calado, es la referida al ámbito de la aplicación de las leyes y de la justicia, en cuanto reflejo, por un lado, de uno de los tres poderes de cualquier Estado democrático (Poder Judicial) y como manifestación, por otro, de las decisiones últimas sobre los conflictos personales más importantes de las sociedades actuales mediante la aplicación e interpretación progresiva de las normas jurídicas que todos nos hemos dado. Por ello, el control, la regulación,

las estrategias de configuración y los límites de los futuros (y presentes) sistemas de Inteligencia Artificial que se generen por la Inteligencia Natural (seres humanos) en relación con la administración de justicia deben ser lo suficientemente rígidos para impedir que el uso inadecuado de aquella suponga la mediatización de los responsables de la aplicación de las normas (jueces y otros operadores jurídicos) ya sea mediante la imposición de sistemas de IA previamente condicionados por la selección de sus parámetros o mediante el condicionamiento posterior de los órganos judiciales a través del obligado uso de aquellos. La Inteligencia Artificial, al igual que la natural humana generadora de la misma, no siempre, por desgracia, se articulará para buscar buenos objetivos. En una frase a modo de resumen que se atribuye a Neil Jacobstein¹ : “no es la inteligencia artificial lo que me preocupa, es la estupidez humana”.

PALABRAS CLAVE: Inteligencia Artificial; sesgos; justicia; administración de justicia; ética digital; algoritmos; machine learning.

ABSTRACT

If there is a human discipline in which the significance of the implications of Artificial Intelligence (AI) can have personal, social, or political important changes, it is the one referred to the application of laws and justice. On the one hand, as a reflection of one of the three branches of any democratic state and, on the other, as a result of the final decisions on the most important personal conflicts of current societies through the application and progressive interpretation of the legal norms that we have all given ourselves for this purpose. Therefore, the control, regulation, configuration strategies and limits of

Artificial Intelligence systems that are generated by Natural Intelligence regarding the administration of justice must be sufficiently rigid to prevent a use aimed at the mediatization of those responsible for the application of the rules (judges and other legal operators) either through the imposition of previously conditioned parameters for artificial intelligence systems or through the subsequent conditioning of judicial bodies through them. It must also be the result of a social consensus in which respect for human rights, user information and the maintenance of the human referent as an essential part of the gear prevail. Artificial Intelligence, like the natural human intelligence that generates it, will not always, unfortunately, be articulated to seek good objectives. In a summary phrase attributed to Neil Jacobstein: "it's not artificial intelligence that worries me, it's human stupidity."

KEY WORDS: Artificial intelligence; bias; justice; administration of justice; digital ethics; algorithms; machine learning

El nuevo marco transatlántico de privacidad de datos Unión Europea-EEUU.

The new EU-US Transatlantic Data Privacy Framework.

Por Alfonso Ortega

RESUMEN

El nuevo Marco de Privacidad de Datos Unión Europea (UE)-EE. UU. introduce nuevas garantías vinculantes al objeto de dar respuesta a cada uno de los motivos de inquietud puestos de manifiesto por el TJUE, en su día, en las Sentencias «Schrems I» y «Schrems II». Entre estas garantías se encuentran la limitación del acceso por parte de los servicios de inteligencia estadounidenses a los datos de la UE y el establecimiento de

un Tribunal de Recurso en Materia de Protección de Datos, al que los ciudadanos de la UE tendrán acceso. Esperemos que con la aprobación de este nuevo Marco de Privacidad de Datos se pueda no sólo «cerrar», definitivamente, la falta de garantías señalada por el TJUE y que provocó la invalidez de los dos marcos de privacidad anteriores (Safe Harbor y Privacy Shield) sino, sobre todo, establecer un nuevo marco seguro y duradero, mediante el que se puedan realizar las transferencias de datos personales necesarias UE-EE.UU. Este trabajo se centra en el estudio de los diferentes esfuerzos llevados a cabo a nivel jurídico para establecer un marco regulatorio satisfactorio para las transferencias internacionales de datos de carácter personal UE-EE.UU., haciendo especial hincapié en el nuevo Marco transatlántico de Privacidad de Datos, recientemente aprobado.

PALABRAS CLAVE: transferencias internacionales, protección de datos, privacidad, marco transatlántico.

ABSTRACT

The new EU-US Data Privacy Framework introduces new binding safeguards to address each of the concerns raised by the CJEU in the 'Schrems I' and 'Schrems II' judgments. Among these guarantees are the limitation of access by US intelligence services to EU data and the establishment of a Data Protection Court of Appeal, to which EU citizens will have access. Hopefully, with the approval of this new Data Privacy Framework, it will be possible not only to "close", definitively, the lack of guarantees pointed out by the CJEU and which led to the invalidity of the two previous privacy frameworks (Safe Harbor and Privacy Shield) but, above all, to establish a new secure and durable framework, through which the necessary

EU-US transfers of personal data can be carried out, with special emphasis on the recently adopted new Transatlantic Data Privacy Framework.

KEYWORDS: international transfers, data protection, privacy, transatlantic framework.

Algunos interrogantes sobre la integración de la Inteligencia Artificial en la Administración Pública.

Some questions about the integration of Artificial Intelligence in the Public Administration.

Por Miren Sarasíbar Iriarte

ENCUESTA N° 32.

Ley de Inteligencia Artificial Europea

European Artificial Intelligence Act

Por Javier Torre de Silva L. de Letona

EN RED N° 32

Número 31

CARTA DEL DIRECTOR

Por Pablo García Mexía

Tribuna de honor. Importancia de los datos en inteligencia artificial

Importance of data in Artificial Intelligence

Por Francisco Ros

Transferencias internacionales de datos en los servicios cloud

International data transfers within cloud services

Por Víctor Julián Sánchez Calle

RESUMEN

El Cloud Computing ha emergido como un nuevo patrón tecnológico hacia el que muchas organizaciones están moviendo sus actividades y procesos para beneficiarse de una accesibilidad global, flexible e inmediata a la tecnología; para liberarse de la adquisición de sus propias herramientas de software y hardware; para reducir sus costes en tecnología a la vez que pueden escalar fácilmente cargas de trabajo y permitir una actividad de procesamiento y almacenamiento más especializada, centralizada y, frecuentemente, más segura. La idea de una infraestructura, plataforma o software como servicio (IaaS, PaaS and SaaS) se fundamenta en la ubicuidad y en la prestación remota de los servicios de computación; y ello conlleva una necesidad de analizar determinados requerimientos y problemáticas legales y regulatorias que tanto el responsable del tratamiento como los encargados del tratamiento están obligados a considerar cuando implanten sus estrategias sobre la tecnología cloud. El propósito de este artículo es proporcionar una perspectiva general acerca de una de las cuestiones sobre protección de datos que más frecuentemente aparece en la mayoría de las negociaciones de contratos de servicios cloud. La transferencia internacional de datos es un término clave para la operativa, disponibilidad, ejecución y seguridad de los servicios cloud; pero presenta amplios retos legales que han de ser tenidos en cuenta tanto cuando se presta el servicio cloud como cuando se adquiere. La idea de un servicio cloud público y global está vinculada a

las transferencias internacionales de datos en la medida en que los recursos para el alojamiento y operativa de tales servicios son, frecuentemente, diseñados bajo parámetros globales. El cumplimiento con el Reglamento general de protección de datos y su aplicación extraterritorial hacen necesaria la adopción de determinados fundamentos legales para llevar a cabo la transferencia internacional de datos y para crear un marco contractual de confianza donde la problemática sobre las restricciones a la transferencia a terceros países pueda ser resuelta de manera razonable para asegurar un nivel de protección adecuado en el marco de la prestación y uso de los servicios cloud.

PALABRAS CLAVE: transferencias internacionales, plataformas, servicios cloud, protección de datos.

ABSTRACT

Cloud computing has emerged as a new tech pattern towards which many organizations are moving their activities and processes to benefit from global, flexible and immediate accessibility to technology, to get rid of purchase of own software and hardware tools, to decrease IT costs while easily scaling workloads and to allow a more specialized, centralized and frequently secured processing and storage activities. The idea of infrastructure, platform, and software as a service (IaaS, PaaS and SaaS) is based on ubiquity and remote provision of computing services. And it ends up in a need of analyze the regulatory and legal issues and requirements that both controllers and processors must consider when implementing their cloud strategies. The purpose of this paper is to deliver an

overview of one specific privacy topic brought in most of cloud agreement negotiations. The international data transfer is a key term for the operation, availability, performance and security of the cloud services, but it shows broad legal challenges to be considered when performing and when purchasing the service. The idea of public and global cloud services is linked to international data transfers as the cloud hosting and operation resources are mostly designed under worldwide basis. Compliance with European Data Protection Regulation and its extraterritorial application require to meet some specific legal fundamentals for the transfer of personal information and to create a contractually trusted environment where third country restriction problems can be reasonably solved by ensuring adequate level of protection when providing and using cloud services.

KEY WORDS: international transfers, platforms, cloud services, data protection.

El impacto legal de la IA “Creativa”

The legal impact of "creative" AI

Por Vanessa Jiménez Serranía

RESUMEN

La IA lleva integrada en nuestras vidas desde hace décadas en distintas aplicaciones que nos acompañan cotidianamente. No obstante, en la actualidad nos encontramos, en principio, ante un cambio de paradigma: la IA no solo se utiliza como herramienta o instrumento de apoyo, sino que puede llegar a generar autónomamente textos, melodías y canciones, videos, etc. y reproducirlas sin necesidad de recurrir a autores, intérpretes o ejecutantes. Esta IA generativa o “creativa” genera

importantes cuestiones vinculadas a grandes ramas del derecho como son la protección de datos, la responsabilidad civil, la ciberseguridad y, por supuesto, la propiedad intelectual. Serán las implicaciones relativas a esta última las que abordaremos en este estudio, centrándonos en los dos principales caballos de batalla que se presentan y su alcance: por un lado, de qué modo obtiene la IA esos inputs que le permitan generar una producción de determinadas “creaciones” o, más bien, resultados; y, por otro, cómo van a estar protegidos —si es conveniente que estén protegidos— estos outputs o productos que va a generar esa IA “creativa”.

PALABRAS CLAVE: IA, prompt, propiedad intelectual, datos, mercados culturales, ChatGPT, Midjourney, titulares de derechos, competencia, ética.

ABSTRACT

AI has been in our lives for decades in various applications that accompany us daily. However, today we are facing a paradigm shift: AI is not only used as a tool or support instrument, but can also generate texts, melodies and songs, videos, etc. autonomously and reproduce them without the need for authors, interpreters or performers. This generative or “creative” AI raises important questions linked to major branches of law such as data protection, civil liability, cybersecurity and, of course, intellectual property. It will be the implications related to the latter that we will address in this study, focusing on the two main “battle horses” that arise and their scope: on the one hand, how AI obtains those inputs that allow it to generate the production of certain “creations” or, rather, results; and, on the other, whether these outputs or

products that this “creative” AI should be protected and eventually, how they will be protected.

KEYWORDS: AI, prompt, intellectual property, data, cultural markets, ChatGPT, Midjourney, rights holders, competition, ethics.

El reto de la Administración Algorítmica. Una reflexión coste-beneficio.

The challenge of algorithmic administration. A cost-benefit reflection

Por Óscar Cortés Abad

ENCUESTA N° 31. LA INTELIGENCIA ARTIFICIAL CREATIVA

Por Almudena Malla Manrique

EN RED N° 31

Número 30

CARTA DEL DIRECTOR

Por Pablo García Mexía

Tribuna de honor. Derecho e Inteligencia Artificial.

Law and Artificial Intelligence

Por Ricardo Rivero Ortega

La nueva regulación de los sistemas operativos y las tiendas de aplicaciones.

New regulation on operating systems and app stores

Por Natalia Gortazar Enrich y Juan J. Montero Pascual

RESUMEN

El nuevo Reglamento de Mercados Digitales de la Unión Europea impone obligaciones a los gestores de sistemas operativos y tiendas de aplicaciones considerados guardianes de acceso. Estas obligaciones derivan del conocimiento de estos mercados generado en casos de competencia como Google Android, Epic Games contra Apple y Spotify contra Apple. Las nuevas obligaciones pretenden por una parte incrementar la apertura en la gestión de estos servicios: obligación de permitir la instalación de apps, interoperabilidad, aplicaciones preinstaladas, neutralidad de red. Por otra parte, persiguen garantizar a los desarrolladores de apps acceso a las tiendas de aplicaciones en condiciones equitativas, razonables y no discriminatorias, lo que puede afectar a las comisiones que actualmente cobran las tiendas de aplicaciones.

PALABRAS CLAVE: plataformas digitales, Sistema operativo, tienda de aplicaciones, derecho de la competencia, regulación.

ABSTRACT

The European Union's new Digital Markets Regulation imposes obligations on both the managers of operating systems and the app stores that fall into the legal category of gatekeepers. These obligations derive from market knowledge acquired in competition cases such as Google Android, Epic Games v. Apple and Spotify v. Apple. On the one hand, these new obligations are aimed at boosting openness in the management of services: obligation to allow the installation of apps, interoperability, preinstalled applications, internet neutrality. On the other hand, they are also intended to guarantee app

developers access to app stores on fair, reasonable and non-discriminatory terms, which may in turn affect current fees charged by app stores.

KEY WORDS: digital platforms, operating system, app store, antitrust, regulation.

Implicaciones en materia de protección de datos personales en la creación y entrenamiento de modelos algorítmicos

Personal data protection implications when creating and training algorithmic models

Por Alicia Coloma Duato

RESUMEN

En los últimos años se ha producido un incremento considerable en la creación y entrenamiento de modelos algorítmicos para su utilización en el ámbito de distintas actividades. La creación, entrenamiento y utilización de dichos modelos algorítmicos conlleva, en la mayor parte de los casos, un tratamiento de datos personales que debe ser llevado a cabo en cumplimiento de la normativa aplicable a dicha materia en España. Las cuestiones que deben ser analizadas en la creación, entrenamiento y utilización de modelos algorítmicos desde la perspectiva de la normativa sobre protección de datos personales son muy diversas y el incumplimiento de las mismas pueden conllevar la imposición de sanciones por parte de las Autoridades de Protección de Datos Personales. De esta manera, a lo largo del presente artículo se analizarán las principales materias que deben ser tenidas en consideración desde la perspectiva de la normativa

aplicable en esta materia en el contexto de la creación, entrenamiento y utilización de modelos algorítmicos en España.

PALABRAS CLAVE: algoritmo, decisiones automatizadas, inteligencia artificial

ABSTRACT

During the last years the creation and training of algorithmic models to be used in the frame of different activities has been increase. The creation, training and use of such algorithmic models implies, in most of the cases, a personal data processing that shall be conducted in compliance with the applicable regulations in Spain to this matter. The matters that should be analysed within the creation, training and use of algorithmic models, from a personal data protection standpoint, are diverse and non-compliance with them may entail the application of sanctions by the Personal Data protection Authorities. Thus, through this article, the main matters that should be analysed taking into consideration the applicable regulations to the creation, training and use of algorithmic models in Spain will be analysed.

KEY WORDS: algorithm, automated decisions, artificial intelligence

Tratamiento de datos personales en el marco de las actividades de inteligencia corporativa. Consideraciones jurídicas y base de legitimación aplicable.

Processing of personal data within the framework of corporate intelligence activities. Legal considerations and applicable legal basis

Por Gonzalo Menéndez Margolles

RESUMEN

Tradicionalmente, las actividades de Inteligencia se han asociado al ámbito público y del Estado, como consecuencia de su intrínseca vinculación a la Seguridad Nacional. Sin embargo, desde hace tiempo, dichas actividades se han extendido al ámbito empresarial, dando origen a una rama denominada “Inteligencia Corporativa”, cada vez más integrada en la dinámica de las entidades del sector privado. Las actividades de Inteligencia Corporativa pueden comportar la utilización de datos personales, lo que conllevará la necesidad observar lo dispuesto en la normativa de protección de datos personales. En este sentido, el presente artículo analizará cuál podría ser la base de legitimación aplicable a los tratamientos de datos personales efectuados por entidades del sector privado ubicadas en España en el marco de sus actividades de Inteligencia Corporativa, teniendo en especial consideración que éstas se alimentan, principalmente, de información procedente de fuentes abiertas.

PALABRAS CLAVE: Inteligencia Corporativa, datos personales, base de legitimación, fuentes públicamente accesibles.

ABSTRACT

Typically, Intelligence activities have been associated to the public and State spheres, due to its inherent linkage with National Security. However, for some time now, such activities have spread to the business sector, giving rise to a field named “Corporate Intelligence”, increasingly integrated into the dynamic of private sector entities. Corporate Intelligence activities might entail the use of personal data, which results in

the necessity to comply with the provisions of the personal data protection regulations. In this regard, this article would analyse the legal basis that may be applicable the data processing activities carried out by private sector entities located in Spain within the framework of their Corporate Intelligence activities, taking into special consideration the fact that said activities mainly feed on information from publicly accessible sources.

KEYWORDS: Corporate Intelligence, personal data, legal basis, publicly accessible sources.

En prospectiva. Reflexiones sobre la disrupción de la inteligencia artificial desde la desinformación.

The European Union's Digital Services Act (DSA) and freedom of expresión

Por Francisco Pérez Bes

ENCUESTA N° 30.

Reglamento de servicios digitales

Por José Ignacio Herce Maza

EN RED N° 30

Número 29

CARTA DEL DIRECTOR

Por Pablo García Mexía

La innovación en España. Políticas públicas para una nueva etapa.

Innovation in Spain. Public policies for a new stage

Por Luis Fernando Álvarez-Gascón Pérez

La presencialidad como principio rector de la actividad parlamentaria. Un análisis de la función deliberante en la distancia.

Presence as a guiding principle of parliamentary activity. An analysis of the deliberant function in the distance

Por M.^a Teresa González Escudero

RESUMEN

La configuración del Parlamento como la reunión de los representantes de una nación o pueblo ha llevado a considerar la presencialidad como un elemento consustancial al ejercicio de la función representativa. Dicha función, que se manifiesta en la deliberación de los representantes democráticamente elegidos y en la adopción de acuerdos tras esa deliberación, se ha visto, sin embargo, alterada en los últimos tiempos adquiriendo cada vez más protagonismo formas de ejercicio a distancia, posibles gracias a los avances tecnológicos e impulsadas a consecuencia de la crisis de la COVID 19. Ahora bien, si el reconocimiento de la adopción de acuerdos en la distancia por el Parlamento — y que se manifiesta en el ejercicio del voto remoto— ha experimentado un importante desarrollo, tanto en su regulación como en su aplicación y, consecuentemente, ha sido ampliamente estudiada por la doctrina, el análisis del debate virtual en el Parlamento ha

quedado relegado a un segundo plano hasta hace solo unos pocos años, cuando el conflicto secesionista de la Comunidad Autónoma de Cataluña y, sobre todo, la crisis de la COVID 19, han traído a un primer plano la cuestión de un Parlamento que debate en remoto.

PALABRAS CLAVE: Debate virtual del Parlamento, quórum de presencia, mandato representativo, representación parlamentaria, sesiones por videoconferencia, voto en remoto.

ABSTRACT

The configuration of the Parliament as the assembly of representatives of a political nation or people has led to consider the attendance as an essential element to the exercise of the representative function. Said function, which is manifested in the deliberation of the democratically elected representatives and in the adoption of agreements after that deliberation, has, however, been altered in recent times, acquiring more and more prominence in forms of remote exercise, possible thanks to technological advances and promoted because of the COVID 19 crisis. However, if the recognition of adoption of agreements in the distance by Parliament — and that is manifested in the exercise of the remote voting — has experienced an important development, both in its regulation and in its application and, consequently, has been widely studied by the doctrine; the analysis of virtual debate in Parliament, has been relegated to the background until just a few years ago, in which the secessionist conflict of the Autonomous Community of Catalonia and, above all, the COVID 19 crisis, have brought to the fore the question of a Parliament that debates remotely.

KEYWORDS: Parliamentary representation, presence quorum, remote voting, representative mandate, sessions by videoconference, virtual debate of Parliament.

Implicaciones jurídicas del Metaverso

Legal implications of Metaverse

Por Eneko Delgado Valle

RESUMEN

La participación humana en cualquier ámbito, entorno o contexto lleva aparejada, desde su inicio, una serie de implicaciones jurídicas que serán más o menos relevantes cuanto más posibilidades de actuación en dicho entorno sea posible para los participantes del mismo. El Metaverso, y los metaversos que lo conforman (y aquellos que se les unan en el futuro) ofrece a sus usuarios un casi ilimitado rango de posibilidades de actuación, mayor incluso que las que tienen en el plano “físico” o real, al no verse limitados por aspectos territoriales o físicos más allá de los (pocos) límites que puedan encontrarse en un mundo de realidad virtual. En el presente estudio se analizarán, al menos de forma enunciativa, como el Metaverso, y la actuación de sus usuarios en él, se ven afectados jurídicamente tanto en el acceso a la propia herramienta o entorno como en la esfera personal y patrimonial de dichos usuarios.

PALABRAS CLAVE: Metaverso, NFT, avatar, realidad virtual, smart contract, propiedad intelectual e industrial, cibercriminosos.

ABSTRACT

Human participation in any area, environment or context, involves, from the very beginning, a series of legal implications that will be more or less relevant according to the more possibilities of action in that environment available to the participants of the same. The Metaverse, and the metaverses that conform it (and those that will join them in the future) offers its users an almost unlimited range of possibilities of action, even greater than those they have in the "physical" or real plane, since they are not limited by territorial or physical aspects beyond the (few) limits that can be found in a virtual reality world. This study will analyze, at least enunciatively, how the Metaverse, and the actions of its users in it, are affected from the legal point of view, both in terms of access to the tool or environment itself and in terms of the personal and patrimonial sphere of these users.

KEY WORDS: Metaverso, NFT, avatar, virtual reality, smart contract, IP, cybercrime

La transparencia en el uso de la inteligencia artificial en las subvenciones.

Transparency in the use of artificial intelligence in subsidies.

Por Martín María Razquin Lizarra

RESUMEN

El presente trabajo persigue explicar la importancia del principio de transparencia en las subvenciones, cuando se utilizan sistemas de inteligencia artificial. Las personas tienen derecho a acceder a la información pública que subyace en estos sistemas que se les aplican en las diversas fases de los procedimientos de concurrencia competitiva. Ello permitirá comprobar la observancia de los principios de igualdad y no

discriminación y de concurrencia, que rigen en las subvenciones.

PALABRAS CLAVE: transparencia, subvenciones, inteligencia artificial, derecho de acceso, información pública.

ABSTRACT

This paper explains the importance of the principle of transparency in public grants, when artificial intelligence are used. People have the right to access the public information that underlines these systems that are applied to them in the various phases of competitive bidding procedures. This will make it posible to verify compliance with the principles of the grants, as equality and non-discrimination and competition.

KEY WORDS: transparency, subsidies, artificial intelligence, right of access, public information.

A vueltas con la Ley de Servicios Digitales de la Unión Europea (DSA) y la libertad de expresión: a debate.

The European Union's Digital Services Act (DSA) and freedom of expression: a debate

Por Aurora María Vicandi Nebreda

ENCUESTA N°29

REGLAMENTO DE MERCADOS DIGITALES

Por Alejandro Negro

EN RED N° 29

Año 2022

Número 28

CARTA DEL DIRECTOR

Por Pablo García Mexía

Los datos de localización tecnológica en la investigación científica y los derechos de protección de datos de los participantes.

Technology location data in scientific research and the data protection rights of participants.

Por Lorena Pérez Campillo

RESUMEN

En estos momentos que vivimos es muy necesario entender la rápida evolución tecnológica de las herramientas y soluciones tecnológicas, también, en localización y su compatibilidad normativa para evitar todo freno en la innovación y desarrollo de la investigación en la lucha contra las enfermedades, mientras se respetan los derechos y dignidad de las personas con su uso. Algunos interrogantes que nos planteamos son: ¿cómo debe ser la información que se facilita a los participantes en una investigación con localización? ¿qué obligaciones deben cumplir los responsables y encargados? ¿qué medidas técnicas y organizativas pueden ayudar a cumplir el deber de información y la transparencia? ¿qué derechos tienen los participantes? ¿son absolutos? ¿cuál es el alcance del ejercicio de los derechos los participantes?

Se llegan a conclusiones tales como que, por un lado, se debe dar una cierta probabilidad de que los derechos -de acceso, de rectificación, limitación del tratamiento y portabilidad de los datos- imposibiliten o produzcan obstáculos graves para la consecución de los fines científicos, siendo necesarias estas excepciones para alcanzar las finalidades de la investigación científica. Y, por otro lado, un posible «ejercicio masivo» de los derechos de cancelación y oposición -por un gran número de personas- nos enfrentaría a un inevitable «efecto negativo en la investigación» ya que entorpecería la propia finalidad de la investigación. De hecho, en ocasiones, debe considerarse que, por ejemplo, el acceso inmediato a determinados tipos de datos sanitarios electrónicos personales puede ser perjudicial para la seguridad de las personas físicas, poco ético o inadecuado.

En cualquier caso, entendemos que donar datos personales anonimizados con fines de investigación científica podría ser el futuro de la medicina digital, ahora bien, debemos estar atentos en reprimir todo tipo de acceso ilegítimo, reidentificación y tráfico ilícito o mercadeo de esos datos.

PALABRAS CLAVE: datos de localización, investigación científica, derechos de participantes, RGPD, Espacio Europeo de Datos Sanitarios (EEDS)

ABSTRACT

In these times we live in, it is very necessary to understand the rapid technological evolution of technological tools and solutions, also in localisation, and their regulatory compatibility in order to avoid any brake on innovation and development of research in the fight against diseases, while respecting the rights and dignity of people with their use. Some of the

questions we ask ourselves are: what should the information provided to participants in localisation research be like? what obligations must those responsible and in charge fulfil? what technical and organisational measures can help to fulfil the duty of information and transparency? what rights do the participants have? are they absolute? what is the scope of the exercise of the participants' rights? The conclusions are that, on the one hand, there must be a certain likelihood that the rights - of access, rectification, restriction of processing and data portability - make it impossible or produce serious obstacles to the achievement of the scientific purposes, these exceptions being necessary to achieve the purposes of scientific research. And, on the other hand, a possible "massive exercise" of the rights of erasure and objection -by a large number of persons- would face an inevitable "negative effect on research" as it would hinder the very purpose of the research. Indeed, it must sometimes be considered that, for example, immediate access to certain types of personal electronic health data may be detrimental to the security of individuals, unethical or inappropriate. In any case, we understand that donating anonymised personal data for scientific research purposes could be the future of digital medicine, but we must be vigilant in repressing any kind of illegitimate access, reidentification and illicit trafficking or marketing of such data.

KEY WORDS: data localisation, scientific research, rights of personal data subjects, GDPR, European Health Data Space (EHDS).

La cibercriminalidad cambiante: el perfil del ciberdelincuente del Siglo XXI (respuestas penales a la sociedad del ciberespacio)

Changing cybercrime: the profile of the 21st century cyber offender (Criminal responses to the cyberspace society)

Por Ignacio Lledó Benito

ABSTRACT/RESUMEN

“El presente artículo explica los diferentes conceptos que se están empezando a implementar en el Derecho penal acerca de estos nuevos términos surgidos a raíz de la 4ª Revolución Industrial sobre la Robótica, IA, Cibercriminalidad y la ciberseguridad como herramienta de prevención en ataques a infraestructuras o personalidades sensibles del Estado español. Comenzamos definiendo la cibercriminalidad y la ciberdelincuencia como diferentes conceptos para la doctrina penal española, seguimos con un pequeño estudio sobre la ciberseguridad, los ciberdelitos más comunes, su implicación en el campo de la IA, el blockchain, los vehículos autónomos, los ciberataques que se dan en la UE, así como los más comunes ocurridos desde 2020 en España, con especial atención al caso Pegasus que puso en vilo la Seguridad del Estado entre abril y mayo de 2022”.

KEYWORDS/PALABRAS CLAVE: “IA, Cybercrime, cybersecurity, cyberattacks, ransomware, hacking, blockchain, spyware, pegasus”.

Ataques informáticos y ciberseguridad. Una respuesta para la amenaza del futuro.

Cyber-attacks and cyber-security. A response to the future's threat

Por Manuel Grueso Medina

RESUMEN

Nunca pasa de moda. El problema de la ciberseguridad y la continua preocupación por los Estados de garantizar un espacio de comunicación eficiente y libre de injerencias se ha vuelto un problema de primer orden. Estamos en el momento de la historia donde probablemente más conectados vivimos unos con otros. Eso se traduce en que la mayor parte de las conversaciones, hechos o transacciones que realizamos en nuestro día a día, está controlado por un soporte o instrumento digital. El texto abarca un repaso a la historia moderna de lo que consideramos la "era tecnológica", los principales problemas jurídicos que se plantean en torno a la figura del delito en los medios informáticos, y el gran papel que debe asumir el legislador para dar una respuesta eficaz y proporcional a una realidad proliferante y cada vez más difícil de abarcar.

PALABRAS CLAVE: ciberseguridad; daño informático; tecnología; sistema de información; virus; hackeo; secuestro; ciberdelincuencia; organización; criminalidad; infraestructura; Rusia; Ucrania; Anonymous

ABSTRACT

It never goes out of fashion. The issue of cybersecurity and the continuing concern of states to ensure an efficient and interference-free communication space has become a major problem. We are at the point in history where we are probably most connected to each other. This means that most of the conversations, events or transactions that we carry out in our daily lives are controlled by a digital medium or instrument. The text covers a review of the modern history of what we consider to be the "technological era", the main legal problems that arise

around the figure of crime in computer media, and the great role that the legislator must assume in order to provide an effective and proportional response to a proliferating reality that is increasingly difficult to cover.

KEY WORDS: cybersecurity; computer damage; technology; information system; virus; hacking; hijacking; cybercrime; organisation; criminality; infrastructure; Russia; Ukraine; Anonymous.

ENCUESTA N°28 REGLAMENTO DORA

Por Leopoldo González Echenique

EN RED N° 28

Número 27

CARTA DEL DIRECTOR

Por Pablo García Mexía

Del metaverso a la metajurisdicción: desafíos legales y métodos para la resolución de conflictos generados en realidades virtuales inmersivas.

From metaverse to metajurisdiction: legal challenges and methods for conflict resolution generated in immersive virtual realities

Por Federico Bueno de Mata

RESUMEN

El presente trabajo estudia los principales retos jurídicos que plantea el metaverso, con especial atención al impacto que el mismo tendrá sobre el derecho procesal y, más concretamente, sobre la jurisdicción y los métodos de resolución para resolver conflictos generados en esta realidad virtual. Del mismo modo, se realiza un análisis sobre las características del metaverso y se discute el modelo tecnológico con el que está iniciativa se desarrollará, al plantear el debate si nos encontramos ante un metaverso único o se potenciarán diversos multiversos a través de diferentes plataformas tecnológicas. En el punto central del trabajo se proponen diversos métodos para resolver conflictos entre avatares dentro del metaverso, así como aquellos que se produzcan entre plataformas oferentes del servicio o entre los usuarios y dichas plataformas. Por último, se reflexiona acerca de si debemos hablar de un “Derecho del metaverso” o de un “metaderecho”. Es decir, si las distintas áreas del derecho deben afrontar actualizaciones normativas para regular esta nueva realidad virtual o si por el contrario es necesario configurar un sistema jurídico nuevo y global para regular el metaverso.

PALABRAS CLAVE: Metaverso, jurisdicción, conflictos, plataformas digitales, procesal.

ABSTRACT

This paper studies the main legal challenges posed by the metaverse, with special attention to the impact it will have on procedural law and, more specifically, on jurisdiction and the methods of resolving conflicts generated in this virtual reality. Likewise, an analysis is made of the characteristics of the metaverse and the technological model with which this

initiative will be developed is discussed, by raising the debate as to whether we are faced with a single metaverse or whether various multiverses will be promoted through different technological platforms. The central point of the paper proposes different methods for resolving conflicts between avatars within the metaverse, as well as those that arise between platforms offering the service or between users and these platforms. Finally, it reflects on whether we should speak of a “metaverse law” or a “meta-law”. In other words, whether the different areas of law should face regulatory updates to regulate this new virtual reality or whether, on the contrary, it is necessary to configure a new and global legal system to regulate the metaverse.

KEY WORDS: Metaverse, jurisdiction, conflicts, digital platforms, litigation

El voto telemático parlamentario: suregluación y peculiaridades.

The telematic parliamentary vote: its regulation and peculiarities.

Por Montserrat Auzmendi del Solar

RESUMEN

Hay una mayoría de reglamentos parlamentarios de nuestro entorno que contemplan la posibilidad del voto parlamentario por vía telemática en situaciones excepcionales. Sin embargo, y aunque se ha puesto en práctica -de forma un tanto acelerada- durante la pandemia, sigue contemplándose esta modalidad con un cierto recelo. En el presente artículo se pretende dar un repaso a las diferentes regulaciones de esta figura, así como extraer una serie de conclusiones para que

esta forma de ejercer el voto tenga correcto acomodo en las exigencias constitucionales.

PALABRAS CLAVE: Voto parlamentario, indelegabilidad del voto, voto personal, representación parlamentaria, mandato representativo.

ABSTRACT

A majority of parliamentary regulations in our environment allow the possibility of parliamentary voting by telematic means in exceptional situations. However, and although it has been put into practice –in a somewhat accelerated way- during the pandemic, this modality continues to be viewed with some suspicion. This article intends to review the different regulations of this figure, as well as to draw a series of conclusions so that this way of exercising the vote has a correct accommodation in the constitutional requirements.

KEY WORDS: Parliamentary vote, non-delegability of the vote, personal voting, parliamentary representation, representative mandate.

Panorama actual de la incipiente regulación de la IA y la neurotecnología, con especial foto en la privacidad y autonomía humana.

Current regulatory framework with regards to artificial intelligence and neurotechnology, especially focus on privacy and human autonomy.

Por Adaya María Esteban Ruiz

RESUMEN

En los últimos años, se ha vivido un despliegue considerable en materia de algoritmos e inteligencia artificial, destacando a su vez los riesgos que estas tecnologías conllevan en la práctica. En el presente estudio, se hace un repaso general al panorama actual de la incipiente regulación de la IA, así como las iniciativas en materia de neurotecnología, con especial foco en los principios de privacidad y autonomía humana. El lector podrá recorrer los distintos hitos más relevantes en materia regulatoria de la IA, no solo a nivel nacional, sino principalmente a nivel europeo y también en algunos de los principales países que, actualmente, luchan en la carrera hacia una IA más confiable.

PALABRAS CLAVE: inteligencia artificial, neurotecnología, privacidad, autonomía humana, regulación, derecho comparado

ABSTRACT

In the last years, there has been an important increase in the development, deployment and use of algorithms in different spheres of our daily life. This article summarizes current regulatory framework with regards to artificial intelligence and preliminary initiatives in neurotechnology, with special focus on privacy and human autonomy principles. The reader can go through the most relevant milestones when it comes to the regulation of the IA, considering not only the Spanish perspective, but also (and mainly) the European regulatory initiatives and most relevant steps taken by some of the main countries in the race towards a trustworthy AI.

KEY WORDS: artificial intelligence, neurotechnology, privacy, human autonomy, regulation, comparative law.

Soluciones legal tech en los Registros de la Propiedad y Mercantiles Españoles.

Por María Rosario Jiménez Rubio

ENCUESTA N°27 EL METAVERSO.

Por Pablo García Mexía

EN RED N° 27

Número 26

CARTA DEL DIRECTOR

Por Pablo García Mexía

Retos jurídicos de la integración de los drones en la ciudad. Legal challenges of drone integration in the city

Por Fernando López Pérez

RESUMEN

La irrupción de los drones en los últimos años, junto con las previsiones económicas que prevén un espectacular desarrollo de sus operaciones, dibujan un escenario futurista, incluyendo la posibilidad de aeronaves no tripuladas dedicadas al transporte de personas y mercancías. Muchos de estos vuelos serán, previsiblemente, ejecutados sobre ámbitos urbanizados, lo que plantea algunos retos jurídicos sobre su integración en la ciudad. Así, se efectúa un análisis de la

regulación de drones europea y española, las competencias entre las diferentes administraciones, para, finalmente, abordar las principales cuestiones que el sobrevuelo de drones a una ciudad puede ocasionar. Sobre esto último, se examina, desde un punto de vista jurídico, la imposición de restricciones de vuelo sobre determinadas zonas, la implantación de una licencia o autorización municipal al vuelo de drones, la construcción de infraestructuras para su despegue o aterrizaje y la imposición de tributos municipales a su operación. Todo ello, desde la perspectiva del derecho local.

PALABRAS CLAVE: Ayuntamientos, Drones, Espacio urbano, Intervención administrativa, Seguridad Aérea, Tráfico Aéreo

ABSTRACT

The irruption of drones in recent years plus the economic forecasts concerning a spectacular growth in its operations point to a futuristic scenario that includes the employment of drones for passenger and freight transportation. The likelihood that many of these flights will be operated over urban areas pose some new legal challenges about their integration into the airspace. This paper addresses the main issues concerning drone overflight of urban areas from the perspective of local law. It first analyses the existing European and Spanish regulations and the distribution of competences between different administrations. Then, it analyses the imposition of flight restrictions on certain areas, the implementation of a municipal authorization for drone flights, the construction of infrastructures for drone take-off and landing, and the imposition of municipal taxes.

KEYWORDS: Municipalities, Drones, Urban areas, Administrative control, Air safety, Air traffic

La Blockchain de las cosas (el contrato Blockchain de las cosas), La necesidad de la tecnología Blockchain en el Internet de las cosas en materia de seguridad y privacidad. La nulidad de las cláusulas "AS IS"

The Blockchain of things (the Blockchain contract of things), the need for Blockchain technology in the internet of things in terms of security and privacy. The invalidity of the "as is" clause

Por María Jesús Jiménez Linares

RESUMEN

La unión del Internet de las cosas (IoT) y de la Blockchain (Blockchain de las cosas) en negocios jurídicos contractuales podría ser una modalidad del contrato Blockchain (contrato Blockchain de las cosas). Tras una breve configuración de estas dos tecnologías que se unen, se muestra como IoT encuentra en la Blockchain la posible solución a sus problemas de privacidad y seguridad apoyándose principalmente en su trazabilidad, confiabilidad, transparencia y descentralización, aunque para ello sea necesario que la propia tecnología Blockchain supere sus defectos en el entorno IoT, desarrollándose muchos proyectos en esta línea. Se analiza cómo los ataques cibernéticos DDoS son los que más sufre la Blockchain en el entorno IoT en sus smart contracts (software) y la posibilidad de prevenirlos. Por otra parte, tanto en la tecnología Blockchain como en el IoT entra en juego el software (independiente o embebido) y en los contratos de licencia de software se suele incluir la cláusula "as is" que excluye la

responsabilidad del desarrollador siendo nula al chocar con el Orden Público Europeo.

PALABRAS CLAVE: Internet de las cosas, Blockchain, Blockchain de las cosas, Contrato Blockchain de las cosas, ataques cibernéticos, cláusula “as is”, Orden Público Europeo

ABSTRACT

The union of the Internet of things (IoT) and the Blockchain (Blockchain of things) in contractual legal businesses could be a form of the Blockchain contract (Blockchain contract of things). After a brief configuration of these two technologies that come together, it is shown how IoT finds in the Blockchain the possible solution to its privacy and security problems, relying mainly on its traceability, reliability, transparency, decentralization. To achieve this it is nevertheless necessary that the Blockchain technology itself overcomes its own flaws in the IoT environment through the development of many projects in this line. It is analyzed how the DDoS cyberattacks are the ones that the Blockchain suffers the most in the IoT environment in its smart contracts (software) and the possibility of preventing them. On the other hand, the software (stand-alone or embedded) plays a role both in Blockchain technology and in the IoT and software license contracts usually include the clause “as is” that excludes the developer’s liability, becoming invalid when colliding with the European Public Order.

KEY WORDS: Internet of things, Blockchain, Blockchain of things, Blockchain contract of things, cyber attacks, clause “as is”, European Public Order.

Privacidad, protección de datos personales y derecho al olvido en la sociedad de Internet y de las redes sociales.

Privacy, protection of personal data and right to be forgotten in the internet society and social networks

Por Pablo Schiavi

RESUMEN

En plena voragine de la sociedad de la información y de internet, exacerbada con el uso exponencial de las redes sociales, y potenciada por la pandemia de la covid-19, se plantea la necesidad imperiosa de la protección de la privacidad y de nuestros datos personales, esto es, la protección de la información más sensible de una persona, esencia de su dignidad, cobrando especial relevancia los riesgos que conlleva un uso masivo, muchas veces irresponsable y sin control, pudiendo menoscabar o dañar nuestra dignidad como personas, en segundos y en forma irreparable. La viralización masiva de información y de contenidos que se nutre de datos personales de todo tipo se ha potenciado sin límites en el día de hoy con la existencia de los llamados “buscadores” o “motores de búsqueda” en internet, como por ejemplo “Google” nos plantea el dilema de una nueva generación de derechos, los llamados derechos digitales, entre ellos, el derecho al olvido.

PALABRAS CLAVE: Privacidad, intimidad, datos personales, derecho al olvido, regulación, desafíos.

ABSTRACT

In the midst of the vortex of the information society and the internet, exacerbated by the exponential use of social

networks, and enhanced by the covid-19 pandemic, the urgent need to protect privacy and our personal data arises. that is, the protection of the most sensitive information of a person, the essence of their dignity, taking on special importance the risks involved in massive use, often irresponsible and without control, which can undermine or damage our dignity as people, in seconds and in irreparable way. The massive viralization of information and content that feeds on personal data of all kinds has been promoted without limits today with the existence of so-called "search engines" or "search engines" on the Internet, such as "Google " presents us with the dilemma of a new generation of rights, the so-called digital rights, including the right to be forgotten.

EY WORDS: Privacy, intimacy, personal, data right to be forgotten, regulation challenges.

La gestión algorítmica de las redes sociales y su afectación a la libertad de expresión, al derecho a la información y a la no discriminación.

Algorithmic management of social networks and its impact on freedom of expression, the right to information and non-discrimination

Por Cecilia Celeste Danesi

RESUMEN

La irrupción de la inteligencia artificial en la vida de las personas trae como consecuencia que la mayoría de los ámbitos cotidianos sean gobernados por algoritmos. Uno de ellos es las redes sociales, donde aquellos operan como gestores del contenido. Esto significa que deciden qué vemos,

cómo y cuándo, dirigiendo el monopolio de la palabra. Bajo este escenario, en el presente trabajo nos proponemos evaluar las posibles consecuencias negativas de la gestión algorítmica en la libertad de expresión, el derecho a la información y a no ser discriminado. Asimismo, analizaremos la función preventiva de la responsabilidad civil como herramienta para prevenir esos posibles daños.

PALABRAS CLAVE: Inteligencia artificial. Algoritmos. Redes Sociales. Libertad de expresión. Derecho a la información. Derecho a la no discriminación. Responsabilidad civil. Función preventiva. Derecho de daños. Derecho del consumo. Derecho civil. Sesgos algorítmicos.

ABSTRACT

The AI irruption in human life has consequently led to most quotidian spheres being governed by algorithms. One of these spheres is social media, where algorithms operate as content moderators. In other words, they decide what we watch, how and when. This enables algorithms to maintain a monopoly over modern day free speech. In this context, we propose to examine if content moderator algorithms negatively affect freedom of expression, right to information, and right to non-discrimination. Moreover, we will analyse preventative function as a tool to prevent the potential consequences that may result from content moderator algorithms.

KEY WORDS: Artificial intelligence. Algorithms. Social Media. Freedom of expression. Right of information. Right to non-discrimination. Civil liability. Preventive function. Tort law. consumer law. Civil law. Algorithmic bias

ENCUESTA N°26 GOOGLE ANALYTICS

Por Katherine Pardo Ardila

Apuntes breves sobre el metaverso

Por José Andrés Jiménez Martín

EN RED N° 26

Número 25

CARTA DEL DIRECTOR

Por Pablo García Mexía

La carta de Derechos Digitales de España. Desafíos pendientes.

Spain's charter of digital rights. Challenges ahead.

Por Celia Fernández Aller

RESUMEN

El artículo analiza con detenimiento los diferentes derechos que se recogen en la Carta de Derechos Digitales de España, detectando áreas que necesitan desarrollo legislativo. Especialmente urgente resulta garantizar los derechos de los menores en el mundo digital, así como la regulación de la Inteligencia artificial, que presenta retos clave a través del uso generalizado de sistemas de decisión algorítmica.

PALABRAS CLAVE: Derechos digitales, privacidad, libertad de expresión, nuevas tecnologías

ABSTRACT

The article analyses in detail the different rights contained in Spain's Digital Charter of Rights, detecting areas which lack legislative development. It is particularly urgent to guarantee the rights of minors in the digital world, as well as the regulation of Artificial Intelligence, which presents key challenges through the widespread use of algorithmic decision systems.

KEYWORDS: Digital rights, privacy, new technologies

**La ética de los datos en las organizaciones e instituciones públicas y la gobernanza en el sector de la salud digital.
Data ethics in public organisations and institutions and governance in the digital health sector.**

Por Lorena Pérez Campillo

RESUMEN

Según el Supervisor Europeo de Protección de Datos (2015), la responsabilidad de dar solución al reto de la Era de la digitalización podría reposar en un ecosistema interdependiente de desarrolladores, empresas y reguladores. Nos encontramos con una oportunidad para llevar la ética a las organizaciones en forma, también, de responsabilidad social empresarial como contribución activa y voluntaria al mejoramiento social que tiene por objetivo mejorar la situación competitiva y valorativa de la empresa teniendo en cuenta el respeto del derecho fundamental de la protección de datos de las personas. Existen a priori algunos interrogantes que nos podemos plantear como; ¿de qué forma podría la ética de los datos solucionar los desafíos que se presentan con la transformación digital de la Industria? ¿se va a llevar la ética a las empresas (responsables y encargados de tratamiento) de

forma similar a lo que se conoce como responsable social empresarial? La ética de datos se considera como una nueva rama de la ética que profundiza sobre los problemas morales relacionados con los datos surgidos a raíz de tratamientos de datos. Su objetivo es formular soluciones como conductas correctas y señalando valores correctos. Pero ¿cómo podemos definir lo que es correcto de lo que no? ¿qué conductas de las organizaciones serán correctas? ¿y qué valores de las organización serán los correctos? ¿qué principios deberemos tener en cuenta en el escenario Covid-19? En la primera parte, abordaremos cómo la ética de los datos se integra en las organizaciones empresariales, repasando algunas herramientas que son utilizadas para ponerla en práctica, como los códigos de ética, los canales de denuncias internos, los comités de ética, las autoevaluaciones, las certificaciones y sellos de calidad, la ética desde el diseño y la privacidad como valor, además, veremos algunos casos de éxito. En segundo lugar, estudiaremos sobre la ética de los datos en el marco de las instituciones públicas y la gobernanza centrándonos en cuestiones como la investigación científica y el big data o la ciberseguridad. Por último, abordaremos la importancia de la ética de los datos en el escenario Covid-19, teniendo en cuenta el papel de ciudadano, la tendencia a la mercantilización de los datos, la limitación de las finalidades, la mejora de la legibilidad de las políticas de protección de datos, y los datos como “bien común” y el uso de checklists.

PALABRAS CLAVE: Data ethics; Data protection; Responsabilidad social empresarial; Ethics by Design; covid-19.

ABSTRACT

According to the European Data Protection Supervisor (2015), the responsibility for meeting the challenge of the digital age could rest with an interdependent ecosystem of developers, companies and regulators. This is an opportunity to bring ethics into organisations also in the form of corporate social responsibility as an active and voluntary contribution to social improvement that aims to improve the competitive and value situation of the company while taking into account respect for the fundamental right of data protection of individuals. A priori, there are some questions that can be raised, such as: how can data ethics solve the challenges posed by the digital transformation of the industry; Will ethics be brought to companies (data controllers and processors) in a similar way to what is known as corporate social responsibility? Data ethics is seen as a new branch of ethics that delves into data-related moral issues arising from data processing. It aims to formulate solutions as right behaviours and pointing out right values. But how can we define what is right and what is wrong, what organisational behaviours will be right, and what organisational values will be right, and what principles should we take into account in the Covid-19 scenario?

In the first part, we will address how data ethics is integrated in business organisations, reviewing some tools that are used to put it into practice, such as codes of ethics, internal whistleblowing channels, ethics committees, self-assessments, certifications and quality seals, ethics by design and privacy as a value, and we will also look at some success stories. Secondly, we will look at data ethics in the framework of public institutions and governance, focusing on issues such as scientific research and big data or cybersecurity. Finally, we will address the importance of data ethics in the covid scenario, taking into account the role of the citizen, the trend towards the

commodification of data, purpose limitation, improving the readability of data protection policies, and data as a “common good” and the use of checklists.

KEY WORDS: Data ethics; Data protection; Corporate social responsibility; Ethics by Design; covid-19

Las nuevas tecnologías aplicadas al ámbito legal: la tecnología blockchain y los Smart contracts como garantía jurídica en la propiedad intelectual. Especial mención a la aplicación de este tipo de tecnologías en la protección de la propiedad intelectual en la arquitectura y obra civil en los contratos del sector público.

Por Miguel de la Puente Pozo

RESUMEN

La aparición de nuevas tecnologías como la Blockchain ha revolucionado casi todos los sectores, desde los más industriales hasta los más tecnológicos. Por lo que no es de extrañar que finalmente el ámbito legal se haya visto afectando, requiriendo de una regulación concreta. Así pues, en el presente trabajo se va a exponer el punto de vista de la implementación de esta tecnología, concretamente su utilización a través de los contratos inteligentes o Smart Contracts. Se trata de un medio de modernización de las garantías jurídicas sobre las que se pueden apoyar los derechos de propiedad intelectual. Estos nuevos mecanismos aportarían un control más exhaustivo de las licencias relativas a la explotación de estos derechos y su autoría. Sobre todo, fortalecería el actual sistema anti-plagio y garantizaría un eficiente control del pago de los cánones y royalties a los

titulares de las licencias, evitando así, la actual fuga de riqueza del sector.

PALABRAS CLAVE. Blockchain, Cadena de bloques, Smart Contracts, Contratos inteligentes, Derecho de propiedad intelectual, tecnología disruptiva, ámbito legal.

ABSTRACT

The emergence of new technologies such as Blockchain has revolutionized almost all firm sectors, from the most industrial ones to startups. Thus, it is not surprising that it finally ends affecting the law, and therefore being in need of regulation. For this reason, this report will show a point of view of this technology implementation. More specifically, its use, through Smart Contracts, as a way of guarantying and updating intellectual property rights. Through these new mechanisms it is intended to carry out a more exhaustive control of the licenses that are granted for these rights common use, their authorship, and, above all, a copyright system much more efficient than the current one, as well as , a control of the payment of royalties to the licenses holders. This new method will avoid the current drain on money from the sector.

KEY WORDS. Blockchain, Smart Contracts, Royalties, Copyright, Law, IP Law, Intellectual Property, Disruptive technologies, Distributed Ledger Technologies (DLT).

El derecho de autodeterminación informativa ante los mecanismos de seguimiento y control presentes en el entorno digital.

The right to informational selfdetermination in the fase of tracking and control mechanisms present in the digital environment.

Por Santiago Grigera del Campillo

RESUMEN

En la actualidad transitamos una época de avances tecnológicos que superan el nivel de entendimiento y asimilación humana. La respuesta normativa no siempre resulta eficaz ante los vertiginosos cambios generados por la transformación digital. En este escenario complejo y globalizado abundan las normas, pero se carece de armonización a nivel internacional. Esta fragmentación normativa presenta desafíos en el control y cumplimiento legal. El usuario, interactúa con tecnologías que no siempre comprende. Tampoco es informado debidamente acerca de las implicaciones en la utilización de los dispositivos y programas de los que se vale en su vida cotidiana. Las tecnologías tienen repercusiones en los derechos y libertades de los usuarios.

En el presente trabajo se elabora una sistematización de tecnologías, técnicas y fenómenos presentes en el entorno digital, que tienen injerencias en el derecho fundamental de autodeterminación informativa. Se explicará de qué se tratan y también algunos aspectos legales que entrañan su utilización.

PALABRAS CLAVES: Libertad informática, autodeterminación informativa, tecnologías de seguimiento y control, privacidad, libertad.

ABSTRACT

Nowadays we are going through a time of technological advances that exceed the level of human understanding and

assimilation. Thereby, the delayed regulatory response is not always effective due to the vertiginous changes generated by the digital transformation. In this complex and globalized scenario, norms abound but international harmonization is lacking. This regulatory fragmentation presents challenges in legal compliance and enforcement. The user interacts with technologies that he does not always understand. In addition, it is not properly informed about the implications of using Internet connected devices and programs in daily life. Technologies have an impact on the rights and freedoms of users. The present work elaborates a systematization of technologies, techniques and phenomena existing in the digital environment, which interfere with the fundamental right of informational self determination. It will be explained what they are about and also point out some legal aspects that their use entails.

KEY WORDS: Computer freedom, informational self determination, monitoring and control technologies, privacy, freedom

La contractualización de la cesión de datos personales: hacia un nuevo paradigma.

The contractualization of personal data transfer: towards a new paradigm

Por Maite Sanz de Galdeano

El certificado COVID digital y el «EFECTO BRUSELAS» de corto recorrido.

Por Blanca Rodríguez-Chaves Mimbrero

EN RED N° 25

Año 2021

Número 24

CARTA DEL DIRECTOR

Por Pablo García Mexía

Inteligencia artificial y compliance.

Artificial Intelligence and compliance.

Por Nuria Díaz-Varela y Arrese

RESUMEN

Nos encontramos en un momento cambiante conocido como VUCA (volátil, incierto, complejo y ambiguo), la pandemia provocada por el COVID-19 ha desencadenado un impacto sin precedentes en el mundo y por ende, en la economía ahora tan globalizada, la cual se ha visto paralizada a nivel mundial. Se han derribado muchas barreras del avance de la digitalización en todos los niveles, incrementando el uso de la tecnología y acelerando el ritmo de los negocios, las relaciones económicas, las comunicaciones y las transacciones internacionales. Esta tendencia de cambio e innovación ha modificado las relaciones con los grupos de interés o stakeholders. El cambio cultural producido en los últimos años marcados por el impacto de las crisis económicas trae consigo la importancia de un comportamiento ético en las organizaciones cuya gestión debe estar alineada con los valores éticos asumidos voluntariamente. En este cometido, cada vez más complejo, la función de compliance desempeña un rol clave. El avance de la

tecnología de la Inteligencia Artificial supone una transformación digital global en todos los ámbitos de nuestra vida con consecuencias fuera del alcance de nuestra imaginación. La tendencia creciente de su utilización y el incierto entorno de cambio produce un impacto en las organizaciones que deben adaptarse al ritmo del mercado global para no perder la carrera. La Inteligencia Artificial ha surgido para inmiscuirse en nuestro entorno diario alterando nuestra forma de vida. Las organizaciones en busca de la eficiencia de sus recursos pueden sacar rendimiento de la utilización del Machine Learning en los sistemas de gestión de compliance para alcanzar sus objetivos de compliance. No sin olvidar los riesgos potenciales que conlleva su utilización, hay que identificarlos, evaluarlos y gestionarlos. El buen funcionamiento de los sistemas de gestión de compliance van acompañados de una actividad proactiva de las organizaciones estableciendo políticas de compliance con altos estándares éticos, desarrollando estrategias para utilizar una Inteligencia Artificial dentro de un marco ético hacia al que se dirigen las organizaciones para responder a las expectativas de la sociedad lo que redundará en un avance de la misma. La utilización de la Inteligencia Artificial de forma responsable y ética será el elemento diferenciador para el éxito o fracaso de las organizaciones. Su extraordinario valor se puede aprovechar para el desarrollo y la interiorización de la cultura de compliance al que están abocadas las organizaciones a incorporar en su día a día. Aquellas que no sepan aprovechar su potencial para transformar la organización de forma ética tenderán a desaparecer, por lo que la confluencia de la cultura de compliance y la Inteligencia Artificial aporta un valor añadido a las organizaciones como elemento diferenciador.

PALABRAS CLAVE: Compliance, Inteligencia Artificial, Machine Learning, stakeholders, ESG (Environmental, Social and Governance), compromisos, obligaciones, Código Ético, sistemas de gestión de compliance, VUCA (volátil, incierto, complejo y ambiguo), reskilling, upskilling, planteamiento AI First, offensive AI, ciberriesgos, análisis de riesgos, algoritmos, diseño de controles, gestión de riesgos, revisión documental, ciberseguridad, prevención y detección del fraude, formación, cultura de compliance, políticas de Compliance, gobernanza.

ABSTRACT

We are in a changing time known as VUCA (volatility, uncertainty, complexity and ambiguity), the pandemic caused by COVID-19 has unleashed an unprecedented impact on the world and therefore on the now globalized economy, which has been paralyzed worldwide. Many barriers have been broken down by the advance of digitalization at all levels, increasing the use of technology and accelerating the pace of business, economic relations, communications and international transactions. This trend of change and innovation has modified relations with stakeholders. The cultural change that has taken in recent years marked by the impact of the economic crises has brought with it the importance of ethical behavior in organizations whose management must be aligned with the ethical values they have voluntarily assumed. In this increasingly complex task, the Compliance function plays a key role. The advancement of Artificial Intelligence technology means a global digital transformation in all areas of our lives with consequences beyond the scope of our imagination. The growing trend of its uses and the uncertain environment of change produces an impact on organizations that must adapt to the pace of the global market in order not to lose the race.

Artificial Intelligence has emerged to intrude into our daily environment altering our way of life. Organizations looking for resource efficiency can benefit from the use of Machine Learning in Compliance Management Systems to achieve their Compliance objectives. However, the potential risks associated with its use must be identified, assessed and managed. The proper functioning of Compliance Management Systems is accompanied by a proactive activity of organizations establishing Compliance policies with high ethical standards, developing strategies to use Artificial Intelligence within an ethical framework towards which organizations are directed to respond to the expectations of society which results in its advance. The use of Artificial Intelligence in a responsible and ethical way will be the differentiating element for the success or failure of organizations. Its extraordinary value can be harnessed for the development and internalization of the Compliance culture that organizations are bound to incorporate in their day-to-day work. Those that do not know how to take advantage of its potential to transform the organization in an ethical way will tend to disappear, so the confluence of Compliance culture and Artificial Intelligence brings added value to organizations as a differentiating element.

KEY WORDS: Compliance, Artificial Intelligence, Machine Learning, stakeholders, ESG (Environmental, Social and Governance), commitments, requirements, Ethical Code, Compliance Management Systems, VUCA (volatility, uncertainty, complexity and ambiguity), reskilling, upskilling, AI First approach, offensive AI, cyber risks, risk assessment, algorithms, control design, risk management, document

review, cybersecurity, fraud prevention and detection, training, Compliance culture, Compliance policies, governance.

El derecho a una buena administración digital en la carta de los Derechos Digitales.

The right to good digital administration in the digital bill of rights

Por Concepción Campos Acuña

RESUMEN

La transformación digital de la gestión pública ha traído consigo nuevos retos frente a la utilización de las nuevas tecnologías y la protección de los derechos y libertades de la ciudadanía en un nuevo escenario: el digital. En este contexto los poderes públicos están promoviendo distintas iniciativas para garantizar la defensa de los mismos, en algunos casos a través de herramientas de soft law, como en el caso de España, con la aprobación de la Carta de Derechos Digitales. En este trabajo analizamos la proyección del derecho a una buena administración en la misma, su sentido, impacto y expectativas de futuro ante los retos que se presentan, sobre todo tras la crisis de Covid-19.

PALABRAS CLAVE: Transformación, Digital, Carta, Buena Administración

ABSTRACT

The digital transformation of public management has brought with it new challenges in the face of the use of new technologies and the protection of the rights and freedoms of citizens in a new scenario: digital. In this context, the public authorities are promoting different initiatives to guarantee

their defense, in some cases through soft law tools, as in the case of Spain, with the approval of the Charter of Digital Rights. In this work we analyze the projection of the right to good administration in it, its meaning, impact and future expectations in the face of the challenges that arise, especially after the Covid-19 crisis.

KEY WORDS: Transformation, Digital, Letter, Good Administration

El euro digital: ventajas, desafíos e implicaciones políticas. The Digital Euro: advantages, challenges and policy implications.

Por Marina Serrat Romaní

RESUMEN

El presente estudio pretende abordar las implicaciones legales y políticas de la creación de una divisa digital por parte del Banco Central Europeo: el euro digital. La popularización de las criptomonedas o criptoactivos y su lenta pero progresiva expansión en su uso ha causado que un gran número de países estén estudiando la posibilidad de lanzar sus propias divisas digitales, debidamente validadas por los respectivos bancos centrales, como medios de pago alternativos más rápidos y eficientes en el entorno de la economía digital. Este artículo aborda las principales características que definen una –CBDC– acrónimo en inglés de divisa digital emitida por los bancos centrales, cómo se diferencian de las criptomonedas y evalúa cuáles son las potenciales ventajas y los principales retos de la incorporación como moneda de curso legal de una divisa digital europea.

PALABRAS CLAVE. Euro digital; Divida digital de banco central; cripto monedas; Banco Central Europeo; privacidad; contra el blanqueo de capitales; política monetaria

ABSTRACT

This study aims to address the legal and political implications of the creation of a digital currency by the European Central Bank: the digital euro. The popularisation of cryptocurrencies or cryptoassets and their slow but progressive expansion in use has caused a large number of countries to consider launching their own digital currencies, duly validated by their respective central banks, as a faster and more efficient alternative means of payment in the digital economy. This article discusses the main characteristics that define a CBDC acronym for central bank-issued digital currency, how they differ from cryptocurrencies, and assesses what are the potential advantages and the main challenges of incorporating a European digital currency as legal tender.

KEY WORDS. Digital euro; Central Bank Digital Currency; Cryptocurrencies; European Central Bank; Privacy; Anti-Money Laundering; Monetary policy.

La plataforma “denaria”: razones y formas para proteger el uso del efectivo.

Por Javier Rupérez

Revisión sistemática de la jurisprudencia española sobre ciberseguridad y privacidad (1995-2020).

On the cybersecurity -and privacy- related cases in the Spanish Higher Courts: A systematic review

Por Fernando César Fernández González, Carlos de Fuentes G^a-Romero de Tejada, Lorena González Manzano y José María de Fuentes G^a-Romero de Tejada

RESUMEN

La expansión de las tecnologías de la información y la comunicación y el aumento de la conectividad, ha provocado el surgimiento de una gran cantidad de delitos como el grooming o la suplantación de identidad, por citar algunos. Sin embargo, no se ha evaluado la relevancia de esta materia en los tribunales españoles. Para superar esta limitación, en este trabajo realizamos un análisis sistemático de la jurisprudencia emanada bien del Tribunal Supremo, bien del Tribunal Constitucional, a través de 117 resoluciones desde 1995 hasta 2020. Nuestro análisis muestra las cuestiones jurídicas que son más frecuentes y revisa cómo han ido evolucionando los diversos conceptos jurídicos sobre ciberseguridad y privacidad.

PALABRAS CLAVE. Ciberseguridad; Privacidad; Protección de Datos; Autenticación; Tribunales españoles; Jurisprudencia.

ABSTRACT

With the explosion of information and communication technologies and the increase of connectivity, a plethora of offences have been identified such as grooming, personal data protection or impersonation, to name a few. Nevertheless, the relevance of this matter in Spanish courts has not been assessed. To overcome this limitation, in this paper we carry out a systematic analysis on 117 resolutions from 1995 to date. All of them belong to the Spanish Higher Courts, namely the Supreme Court and the Constitutional Court. This is particularly relevant as their resolutions can set a precedent that has to be

observed by lower courts. Our analysis shows the legal issues that are more often at stake as well as the trends in terms of legal doctrines and punishments.

KEY WORDS: Cybersecurity; Citizens privacy; Data security; Citizens authentication; Spain; Resolution; Higher Courts.

**LA ENCUESTA #24
EL EURO DIGITAL.**

Por Andrés Moisés Barrio

EN RED Nº 24

Número 23

CARTA DEL DIRECTOR

Por Pablo García Mexía

Regulación y supervisión en una economía digital globalizada.

Por Carlos Laguna de Paz

El acceso al legado digital: estudio de su regulación en España y en otros ordenamientos jurídicos.

Access rights to digital legacy: study of the regulation in Spain and other legal orders.

Por Andrea Romero-Lecrivain

RESUMEN

El devenir y la transmisibilidad de los bienes digitales tras el fallecimiento suscitan numerosas dudas. Este estudio se centra en el análisis de las dos leyes actualmente vigentes en España (ley autonómica y ley estatal) relacionadas con el legado digital de las personas físicas, para analizar los avances que suponen, evidenciar los elementos ambiguos y señalar sus posibles carencias, contrastando con otras tres disposiciones normativas (Francia, Italia, Portugal y Estados Unidos). Pretende aunar las observaciones y enfoques de los pocos estudios sobre estas normas, y complementarlos con reflexiones propias. Por razones de coherencia, el análisis estará enfocado exclusivamente al régimen sucesorio, quedando por tanto excluido del análisis lo específicamente relacionado con el de menores y personas incapacitadas.

PALABRAS CLAVE: Legado digital, sucesión, Cataluña, España, derecho comparado.

ABSTRACT

In Europe it is left to the Member States to provide for rules regarding the processing of the personal data of deceased. Accordingly, this paper proposes the evaluation of the solutions that the law provide to protect interests involved in digital inheritance in Spain. In this framework, we examine the different rules to analyze the progress they represent, highlight ambiguous elements and point out their possible shortcomings. In a second time, on the basis of comparative research, we examine the national legal rules in France, Italy, Portugal and United States with their specific measures regarding data protection for deceased persons. This paper combines the observations and approaches of the few studies on these norms, and complements them with own conjectures.

KEY WORDS: Digital inheritance, Catalonia, Spain, succession law, comparative law.

Salud versus privacidad: unos apuntes sobre el tratamiento de datos personas en la lucha contra la Pandemia por la Covid-19 desde los ámbitos de la regulación y la aplicación del Derecho.

Phealth versus privacy: a few notes on the processing of personal data in the fight against the Covid-19 pandemic from the areas of regulation and the application of law.

Por Blanca Rodríguez-Chaves Mimbrero

RESUMEN

Este trabajo tiene como objeto analizar las garantías del tratamiento de los datos de carácter personal realizados desde los desarrollos tecnológicos articulados para la gestión de la pandemia causada por la COVID-19. El análisis de dichas garantías se afronta desde dos perspectivas que terminan convergiendo. Desde la primera perspectiva, el estudio de las garantías del derecho a la protección de datos personales se realiza a partir de los documentos emanados tanto desde las instituciones europeas, especialmente el Comité Europeo de Protección de Datos, como desde la Agencia Española de Protección de Datos, que interpretan la aplicación del Reglamento General de Protección de Datos en esta situación de pandemia. El estudio se complementa con una segunda perspectiva en la que se analizan sistemáticamente las exigencias que conlleva el respeto a los derechos fundamentales, como es el derecho a la protección de datos de carácter personal, tomando como referencia la STC 76/2019, aún en situaciones de emergencia e incertidumbre científica.

Dicho análisis se realiza desde dos planos: el plano normativo y plano de aplicación del Derecho vigente.

PALABRAS CLAVE. Datos de salud, Aplicaciones de rastreo de contactos, limitación de derechos, ponderación, consentimiento.

ABSTRACT

The purpose of this work is to analyze the guarantees for the processing of personal data for the management of the pandemic caused by COVID-19, from the technological developments articulated for the control of the virus. The analysis of these guarantees is approached from two perspectives that end up converging. From the first perspective, the study of the guarantees of the right to the protection of personal data is carried out from the documents issued both from the European institutions, especially the European Data Protection Committee, and from the Spanish Agency for Data Protection, which interpret the application of the General Data Protection Regulation in this pandemic situation. The study is complemented with a second perspective in which the demands that the respect for fundamental rights entails, such as the right to the protection of personal data, are systematically analyzed, taking as reference STC 76/2019, even in emergency and scientific uncertainty situations. This analysis is carried out from two levels: the normative level and the application of current Law.

KEY WORDS. Health data, Contact tracing applications, Limitation on rights, weighting, consent

Aproximación al futuro marco normativo europeo de la inteligencia artificial.

The future european regulatory framework on artificial intelligence. An approach.

Por Carlos Fernández Hernández

RESUMEN

Análisis de la propuesta de Reglamento europeo sobre inteligencia artificial, presentado por la Comisión. Se ofrece un resumen del proceso que ha llevado hasta la elaboración de esta propuesta, para abordar a continuación sus contenidos más significativos, como su objeto, ámbito de aplicación; la clasificación de las diferentes prácticas de IA; las prácticas prohibidas; las prácticas de alto riesgo; las obligaciones impuestas a los distintos intervinientes en el diseño, comercialización o utilización de las mismas; los organismos europeos que prevé crear y el régimen de cumplimiento y sancionador que contempla.

ABSTRACT

Analysis of the proposal for a European Regulation on artificial intelligence, presented by the Commission. A summary of the process that led to the drafting of this proposal is presented, followed by an analysis of its most significant contents, such as its purpose and scope; the classification of the different AI practices; the prohibited practices; the high-risk practices; the obligations imposed on the different parties involved in the design, marketing or use of these practices; the European bodies that it plans to create and the compliance and sanctioning regime it envisages.

KEY WORDS: Artificial Intelligence. Data. Algorithms. Governance. High risk AI systems. Prohibited AI practices. Low risk AI systems. Penalties.

Ambivalencias de la sociedad virtual.

Por Héctor Romero Ramos

LA ENCUESTA #23

Proyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Por Francisco J. Hernández Guerrero

Número 22

CARTA DEL DIRECTOR

Por Pablo García Mexía

Una década de derecho al olvido de Internet

Por Artemi Rallo Lombarte

Algunas consideraciones sobre el derecho de autor de software de las application programming interface apis. Contenido y límite del derecho. La sentencia Oracle Inc. Vs. Google Inc.

Some considerations on the copyright of the Application Programming Interface API's software. Content and limit of the right. The Oracle inc. vs. Google inc.

Por Ana Felicitas Muñoz Pérez

RESUMEN

El estudio trata un tema de derechos intelectuales y desarrolla la temática ligada al caso jurisprudencial que enfrentó a Google Inc. con Oracle Inc. Con ocasión de este litigio se revisaron las particularidades del contenido de los derechos intelectuales cuando recaen sobre el software informático de las Application Programming Interface -APIS- en particular, por el contenido funcional del derecho y la capacidad de hacer interoperables los sistemas. En particular, la protección de derecho de autor sobre elementos funcionales de programas computacionales que hacen interoperable los sistemas Application Programming Interface (APIs). Al tiempo se analizan los límites al ejercicio de sus facultades contemplados en los denominados casos de "Fair use".

Palabras clave: Derechos intelectuales, APIs, uso justo.

ABSTRACT

The study deals with an issue of intellectual rights and develops a set of issues related to the jurisprudential case that confronted Google Inc. with Oracle. Inc. On the occasion of this litigation, the particularities of the content of intellectual rights were considered when they fall on computer software of the

Application Programming Interface -APIs due the functional content of the right and the ability to make systems interoperable. At the same time, the limits to the exercise of its powers contemplated in the so-called "Fair use" cases are analyzed.

Key words: Intellectual rights, APIs., "fair use".

Tratamientos de datos personales ex machina en plataformas de turismo colaborativo. Concienciación y previsibilidad a través de las políticas de privacidad.

Personal data processing ex machina in sharing tourism platforms. Awareness and foreseeability by means of privacy policies

Por María Estrella Gutiérrez David

RESUMEN

Las plataformas de turismo colaborativo constituyen un ecosistema genuino donde se desarrollan e implementan tecnologías innovadoras como el Machine Learning o el IoT. Estas tecnologías posibilitan el tratamientos masivos y altamente intrusivos de los datos personales de millones de usuarios, en tiempo real y con efectos individuales y sociales disruptivos. Es una afirmación común que los tratamientos de datos realizados por estas tecnologías especialmente, mediante el aprendizaje automático- permanecen, a menudo, "invisibles" para los interesados. Ello implica un alto riesgo de vulneración de los principios de lealtad y transparencia cuando los afectados no esperan tales tratamientos o el resultado de los mismos. Para evidenciar tales riesgos, trataremos de "visibilizar" las nuevas taxonomías de datos personales, observados e inferidos, así como los tratamientos específicos

realizados por las plataformas colaborativas (decisiones individuales automatizada y elaboración de perfiles). Para ello, rastreadremos la fraseología común utilizada en las políticas de privacidad (por ejemplo, «métodos automatizados», «tecnologías similares», «precios dinámicos individuales») tratando de “levantar el velo” sobre la verdadera naturaleza y alcance de dichos tratamientos de datos.

Palabras clave: Datos personales, Aprendizaje Automatizado, Decisiones Individuales Automatizadas, Perfilado, Políticas de Privacidad, Plataformas de Turismo Colaborativo.

ABSTRACT

Sharing tourism platforms constitute a genuine ecosystem where innovative technologies such as Machine Learning or IoT are developed and implemented. They enable massive, real time and highly intrusive processing of the personal data of millions of users, with disruptive individual and social effects. It is a common claim that underlying processing by these technologies -especially, by machine learning modelling- remains «invisible» to data subjects. This involves high risks of breaching the fairness and transparency principles when processing or any outcome resulting from it is not foreseen by individuals. To evidence such risks, we will seek to «make visible» the new taxonomies of observed and inferred personal data and the specific processing which takes place in sharing platforms (automated individual decision-making and profiling). In order to achieve this goal, we will trace the common wording used by privacy policies («automated methods», «similar technologies», «individual dynamic pricing» and so on) seeking to lift the veil on the true nature and scope of such data processing.

Key words: Personal Data, Machine Learning, Automated Individual Decision-Making, Profiling, Privacy Policies, Sharing Tourism Platform.

Las comunicaciones y redes de datos: revisión histórica y evolución en el contexto post-covid-19.

Communications and data networks: history and evolution in the post- COVID-19 context

Por José Morales Barroso

RESUMEN

La Red Telefónica Clásica (RTC), desarrollada para transportar las señales analógicas de voz, se utilizó como infraestructura básica para construir las Redes de Datos. Al ser este sistema caro y poco eficiente, se desarrollaron las técnicas de conmutación de paquetes, en las que se basa el funcionamiento de la actual Internet. ARPANET, que se puso en marcha en 1969, fue la red precursora de Internet. En Europa se desarrollaron las Redes Públicas de Conmutación de Paquetes, siendo la RETD española la primera del mundo que se puso en servicio.

Las comunicaciones sin hilos o inalámbricas comienzan en la década de 1920, pero hasta 1981 no se comercializa el servicio de telefonía móvil con la Primera Generación, que funcionaba en modo analógico. La Segunda Generación, liderada por el sistema europeo GSM, fue la primera que utilizó la tecnología digital. A partir de ahí, se ha experimentado una rápida evolución hasta la actual Quinta Generación o 5G, que está produciendo una revolución en las comunicaciones. En otro ámbito, la tecnología Wi-Fi, basada en los estándares 802.11 del IEEE para Redes Locales Inalámbricas, es actualmente el

sistema inalámbrico más utilizado, pasando por él la mayor parte del tráfico de Internet.

La pandemia del COVID-19 ha marcado un hito en la evolución de las Tecnologías de la Información y las Comunicaciones, pues ha provocado un crecimiento notable en su uso. Este rápido aumento de tráfico, y unos requerimientos de calidad más restrictivos, van a suponer cambios radicales en el funcionamiento de la red. En este sentido, la Comisión Europea ha presentado la Brújula Digital, basada en cuatro puntos que se analizan brevemente en el artículo. A continuación, se trata el importante tema de la denominada Revolución de la Era 5G y la cadena de bloques o Blockchain, en la que se basan, entre otras cosas, las criptomonedas y los contratos inteligentes. Para terminar, se reflexiona sobre la necesidad de simplificar, con objeto de encarar, con garantías de éxito, el futuro de las comunicaciones y las redes de datos.

Palabras clave: Comunicaciones, redes de datos, 5G, Blockchain, COVID-19

ABSTRAC

The Public Telephone Network (PSTN), developed to transport the voice analog signals, was used as the basic infrastructure to build the Data Networks. As this system is expensive and inefficient, packet switching techniques were developed, on which the operation of the current Internet is based. ARPANET, launched in 1969, was the forerunner of the Internet. In Europe, the Public Packet Switching Networks were built, the Spanish RETD being the first in the world to be put into service. Wireless communications began in the 1920s, but it was not until 1981 that mobile phone service was marketed with the First Generation, which operated in analog mode. The Second Generation, led by the European GSM system, was the first to

use digital technology. From there, there has been a rapid evolution until the current Fifth Generation or 5G, which is producing a revolution in communications. In another area, Wi-Fi technology, based on the IEEE 802.11 standards for Wireless Local Area Networks, is currently the most widely used wireless system, passing through most of the Internet traffic.

The COVID-19 pandemic has marked a milestone in the evolution of Information and Communication Technologies, as it has caused a remarkable growth in their use. This rapid increase in traffic, and more restrictive quality requirements, will lead to radical changes in the operation of the network. In this sense, the European Commission has presented the Digital Compass, based on four points that are briefly analyzed in the article. Next, the important topic of the so-called Revolution of the 5G Era and the Blockchain, on which cryptocurrencies and smart contracts are based, among other things, is discussed. Finally, it reflects on the need to simplify to face, with guarantee of success, the future of communications and data networks.

Key words: Communications, data networks, 5G, Blockchain, COVID-19

Implicaciones del modelo jurídico de implantación de la administración electrónica en personas mayores.

Consequences of the legal framework of establishment of E-Administration on elderly

Por Salvador Manzanera-Román y Francisco Eduardo Haz Gómez

RESUMEN

Este trabajo analiza el modelo jurídico para la implantación de la Administración Electrónica (procedimiento electrónico) y sus implicaciones sobre los derechos de las personas mayores. En

relación con la metodología empleada, se ha realizado un análisis documental de la normativa regulatoria del procedimiento electrónico y de las entrevistas a expertos realizadas a través de la técnica Delphi. Los resultados ponen de manifiesto la existencia de un modelo jurídico favorable a la equidad y la no discriminación de colectivos vulnerables. Sin embargo, este no se encuentra plenamente adaptado a las necesidades y exigencias de los mayores, lo que implica consecuencias como la exclusión digital (y social). Por lo que, urge llevar a cabo actuaciones para revertir esta situación.

Palabras clave: Sociedad digital; Administración Electrónica; Personas mayores; Modelo jurídico; Exclusión digital.

ABSTRACT

This work analyzes the legal framework for the implementation of Electronic Administration (online procedure) and its implications on the rights of the elderly. With regard to the methodology used, there were used a documentary analysis of the regulatory regulations of the electronic procedure and interviews with experts through the Delphi technique. The results point out the existence of a legal framework favorable to equity and non-discrimination of vulnerable groups. However, this is not fully adapted to the needs and demands of the elderly, which implies consequences such as digital (and social) exclusion. Therefore, some actions are urgently needed to reverse this situation.

Keywords: Digital society; E-Administration; Elderly; Legal framework; Digital exclusion.

Comentario crítico al Real Decreto Ley 9/2021. De 11 de mayo, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales.

Por Lucía Aragüez Valenzuela

La encuesta #22 El pacto digital para la protección de las personas

Por Pablo García Mexía

EN RED N° 22

Número 21

CARTA DEL DIRECTOR

Por Pablo García Mexía

Libertad de expresión, moderación de contenidos y neutralidad política de las plataformas en EEUU. La orden ejecutiva para la prevención de la censura en internet.

Freedom of speech, content moderation and online platforms neutrality in USA. The Executive Order on Preventing Online Censorship.

Por Alejandro Puerto Mendoza

RESUMEN

El debate sobre la responsabilidad de las plataformas en EEUU por las decisiones de moderación de los contenidos que difunden no ha hecho más que intensificarse desde que, en mayo de 2020, la red social Twitter etiquetó, por primera vez,

un mensaje del presidente Donald Trump advirtiéndolo de que su contenido era potencialmente falso y que debía ser objeto de comprobación. Esta polémica se ha reavivado significativamente tras el suceso de la ocupación del Capitolio, el 7 de enero de 2021, que desencadenó, entre otras consecuencias, la expulsión temporal o definitiva de Trump de varias redes sociales y la cancelación unilateral por Apple, Google y Amazon de los servicios de intermediación que venían prestando a la red social Parler, al considerar que vulneró sus respectivas condiciones de uso por el continuo incremento del contenido incitando a la violencia que se difundía a través de esta aplicación. A estos hechos se suman otros no menos preocupantes derivados de la gran cantidad de contenidos dañinos e ilícitos que se distribuyen a través de las plataformas y que, en buena medida, suponen una amenaza para las libertades y el desarrollo de internet. De esta manera, se viene cuestionando si el régimen legal aplicable desde hace 25 años a las plataformas en EEUU sigue siendo válido o, por el contrario, la evolución de los mercados digitales exigen su reforma ante el enorme poder que estas disfrutaban sobre el ejercicio del derecho a la libertad de expresión e información de los ciudadanos y el aparente desinterés mostrado en combatir eficazmente los contenidos indeseables. La principal respuesta a estas problemáticas ha venido de la mano de diferentes propuestas de modificación de la regulación con el fin de reducir la amplia exención de responsabilidad que gozan las plataformas actualmente y, en concreto, de la revisión de la Sección 230 (c) de la Ley de Decencia de las Comunicaciones de 1996. La Sección 230 (c) viene constituyendo una pieza indispensable para el mantenimiento y desarrollo del actual entorno de internet, pues gracias a ella, las plataformas y otros servicios basados en la difusión de contenidos de terceros se

benefician de un escudo legal casi absoluto respecto de los daños que esos contenidos pueden llegar a ocasionar, incluso en los casos en que intervienen de forma activa a través de su moderación. Entre las numerosas propuestas de modificación se encuentran las efectuadas a nivel gubernamental a través de la Orden Ejecutiva para la Prevención de la Censura en Internet, dictada por Trump en mayo de 2020 con el objetivo de imponer la neutralidad política en las redes, y el proyecto de ley elaborado por el Departamento de Justicia de septiembre de ese mismo año. Sin embargo, todas las propuestas de modificación del citado régimen legal deben hacer frente a diversos retos, como la cobertura que la actual interpretación de la Primera Enmienda otorga a las plataformas para decidir qué contenidos desean difundir o moderar, o el derivado del reciente cambio en la presidencia de los EEUU.

Palabras clave: libertad de expresión, neutralidad, plataformas de internet, moderación de contenidos, redes sociales, responsabilidad de intermediarios, Sección 230.

ABSTRACT

The debate about liability of social media platforms in the United States over their decisions on content moderation has increased in intensity since, in May 2020, Twitter tagged a post from President Donald Trump as potentially false and claimed its content should be verified. This controversy was significantly rekindled after the events surrounding the US Capitol riots of 7 January 2021, which, among other consequences, triggered the suspension of Trump's accounts in several platforms, as well as the unilateral cancellation of the intermediary services provided by Apple, Google and Amazon to the social network

Parler. This was based on the claim that the content distributed on the platform incited to violence and breached their terms of service. These facts add up to the rather worrying amount of harmful and illicit contents shared online, which entail a threat to freedom and to the development of the internet. Thus, it is questioned whether the legal framework that has been applicable to US platforms for the last 25 years is still valid today or, conversely, the evolution of digital markets requires their reform given the enormous power that platforms wield in exercising the right to freedom of expression and information, along with their apparent lack of interest in effectively countering illicit and harmful contents. The main answer to these predicaments came in the form of proposals to modify the applicable legal framework, aiming to reduce the ample liability exemptions enjoyed by the platforms and, more specifically, revisiting Section 230 (C) of the Communications Decency Act of 1996. Section 230 (c) has become an essential element in the development and maintenance of the current internet environment. It is said to render online platforms and other third-party content sharing services an almost absolute legal shield against potential liabilities, even in cases where they perform active content moderation. Among its many proposed amendments, there are two government-sponsored initiatives: The Executive Order on Preventing Online Censorship, dictated by President Donald Trump in May 2020, and the Department of Justice's bill dating from September of the same year. However, all proposed amendments to this legal framework must face a number of challenges, like the protection that the First Amendment gives to online platforms to moderate content; and the challenges derived from the recent change in administration of the US.

Key words: freedom of speech, online platform neutrality, content moderation, social media, intermediary liability, Section 230

Trading and settlement of crypto-assets.

Por Gonzalo Navarro Ruiz

ABSTRACT

This article focuses on analysing various regulatory topics regarding the crypto-securities in order to give the reader a general view of the concept of them and the regulatory framework applicable to them. In order to do that, the definition of crypto-securities, the application of the financial regulatory framework to them, the regulatory concerns related to the development of crypto- securities trading platforms will be studied throughout the article among other legal issues. The article is divided into several major sections along which the subjects referred to above are addressed in a systematic way. The article concludes with a section devoted to the conclusions, in which, as a closing, we expose in an orderly and succinct way the ideas that we consider essential on the different topics addressed throughout it. The content of the article is based on European and non-European regulation on the securities markets and Blockchain technology; publications and reports of international supervisory authorities and associations (i.e. Bank International Settlements, Asia Securities Industry & Financial Markets Association, UK Financial Conduct Authority, Autorité des Marchés Financiers, Swiss Capital Markets and Technology Association, International Organization of Securities Commission); and publications, specialized works and doctrinal opinions on the subjects under study.

Key words: Blockchain, centralized platforms, crypto-securities, crypto-securities trading platforms, decentralized platforms, ITO, security tokens, tokenised securities.

La responsabilidad de los prestadores de servicios de intermediación de nombres de dominio por infracciones de terceros: especial referencia a derechos exclusivos marcarios.

Liability information society services providers domain names infringement: special reference to intellectual property rights.

Por Pilar Íñiguez Ortega

RESUMEN

Los prestadores de servicios de intermediación pueden “contribuir” a las infracciones que se cometen en Internet. En este artículo examinaremos las diferencias y las coincidencias en la atribución de responsabilidad a los ISP por la prestación de servicios de acceso y mera transmisión de hosting y de caching, así como la jurisprudencia generada en los distintos países europeos, valorando las exenciones de responsabilidad dentro de los nuevos modelos de negocio en Internet, a tenor de la Directiva 2000/31, de 8 de junio de 2000 sobre comercio electrónico en aras a la prevención de actividades ilícitas, con especial referencia a los derechos de propiedad intelectual.

Palabras clave: nombres de dominio, prestadores de servicios de la sociedad de la información, responsabilidad, propiedad intelectual, puerto seguro.

ABSTRACT

The information society services providers can “contribute” to the infringements committed by users over the Internet. In this paper will examine the differences and coincidences in the allocation of liability on ISP for providing services of access and transmission, of hosting and caching, as well as the different case law from European countries, analyzed the exemptions from liability to the new Internet business models in the Directive 2000/31 of 8 June 2000 on electronic commerce, in relation to prevent illicit activities, with special reference to intellectual property right.

Keywords: domain names, information society services providers, liability, intellectual property right, safe harbours.

LA ENCUESTA #21

La nueva regulación del trabajo a distancia.

Por Lucía Aragüez Valenzuela, Pablo Viedna Cabrera y Carmen Aránguez Sánchez

Un nuevo horizonte para las plataformas difitales del sector VTC en la Comunidad de Madrid.

Por Alfonso Codes Calatrava

EN RED Nº 21

Año 2020

Número 20

CARTA DEL DIRECTOR

Por Pablo García Mexía

Una brújula para regular la Inteligencia Artificial

Por Alessandro Mantelero

Privacidad y Covid-19

Privacy and Covid-19

Por Ramón Miralles López

RESUMEN

La pandemia provocada por el coronavirus causante de la COVID-19 ha puesto en evidencia muchas debilidades, pero también diversas fortalezas, ya no de nuestra sociedad, incluso de nuestra civilización, y hemos percibido con claridad lo vulnerables que somos, tanto individual como colectivamente. El sistema de derechos de que disfrutamos pretende protegernos de todo tipo de vicisitudes, pero en ocasiones hay que limitar su alcance, precisamente para seguir protegiendo el interés general; los derechos fundamentales y libertades públicas están ahí para garantizarnos unos mínimos de convivencia y cohesión social, que cuando de algún modo se ven perturbados, requiere que se actúe sobre esos derechos, limitándolos en base a medidas que deben ser, en todo caso, proporcionadas a la gravedad de la situación que pretende gestionarse, y de las que deben obtenerse como resultado final, más beneficios que perjuicios.

Las tecnologías en general y, en particular, las de la información y

la comunicación, son herramientas útiles e imprescindibles para combatir la pandemia, y para ello precisan tratar datos relativos a las personas, pero ese tratamiento de datos

personales, y en particular aquellos relativos a la salud, están protegidos por un derecho fundamental, que en Europa tienen un origen, que no es otro que evitar daños y perjuicios sobre las personas como consecuencia del tratamiento de sus datos personales. Este estudio trata sobre cómo el derecho fundamental a la protección

de datos se ha mantenido vigilante y firme durante la situación de pandemia, y trata de los instrumentos jurídicos que refuerzan esa protección de las personas, incluso en situaciones de extrema

gravedad, sin que por ello se haya limitado o impedido la adopción de todo tipo de medidas, tendentes a aportar soluciones a la grave crisis derivada de la pandemia.

Palabras clave: COVID-19, coronavirus, SARS-CoV-2, pandemia, datos personales, datos de salud, tecnologías, derechos fundamentales, app, móviles, investigación científica, salud pública, estado de alarma, autoridades de protección de datos, vulneración de derechos, privacidad, intimidad, evaluación de impacto, licitud, crisis sanitaria, tecnologías que deterioran la privacidad.

ABSTRACT

The COVID-19 pandemic caused by the coronavirus has revealed many weaknesses, but also various strengths, no longer of our society, even of our civilization, and we have clearly perceived how vulnerable we are, both individually and collectively.

The system of rights that we enjoy aims to protect us from all kinds of vicissitudes, but sometimes its scope must be limited, precisely to continue protecting the general interest; Fundamental rights and public freedoms are there to

guarantee us a minimum of coexistence and social cohesion, which when they are disturbed in some way, requires action on those rights, limiting them based on measures that must be, in any case, proportionate to the seriousness of the situation that is to be managed, and of those that must be obtained as a final result, more benefits than damages. Technologies in general and, in particular, those of information and communication, are useful and essential tools to combat the pandemic; they need to process data related to people, but that processing of personal data, and in particular those related to health, are protected by a fundamental right, which in Europe has an origin, which is none other than to avoid damages to people as a result of the processing of their personal data. This study deals with how the fundamental right to data protection has remained vigilant and firm during the pandemic situation and deals with the legal instruments that reinforce that protection of people, even in extremely serious situations, without the adoption of all kinds of measures, aimed at providing solutions to the serious crisis derived from the pandemic, has been limited or prevented. Some legal forecasts for the future are also made, based on different indications and on the observation of much of what has happened, and is happening, around COVID-19.

Key words: COVID-19, coronavirus, SARS-CoV-2, pandemic, personal identifiable information, health data, technologies, fundamental rights, app, mobile phones, scientific research, public health, state of alarm, data protection authorities, violation of rights, privacy, privacy impact assessment, legality, health crisis, technologies that decrease privacy.

La pandemia como punto de inflexión, de hecho y derecho, en el trabajo a distancia.

Pandemic as a factual and legal breaking point in remote working

Por Camino Ortiz de Solórzano Aurusa

RESUMEN

Debido a la pandemia, España, así como otros muchos países, declare el estado de alarma. Una de las principales consecuencias fue la promoción del trabajo a distancia – particularmente el teletrabajo– como instrumento para aunar las restricciones de movilidad y la actividad económica. Esto ha derivado en un significativo incremento del teletrabajo en nuestro país, incluso cuando ya había concluido la primera ola de la pandemia; y ambos, empresas y trabajadores, podrían apostar en el futuro por esta forma más flexible de trabajo. La aprobación de un nuevo marco jurídico para el teletrabajo debería proveer mayor seguridad jurídica para su implantación una vez que la crisis sanitaria haya terminado. La negociación colectiva será una herramienta necesaria en el desarrollo de dicho marco jurídico para desarrollar los derechos y deberes de empresarios y trabajadores en este ámbito.

Palabras clave: Trabajo a distancia, teletrabajo, Covid-19, confinamiento, negociación colectiva, privacidad y seguridad de datos.

ABSTRACT

Due to the pandemic, Spain, as well as many other countries, declared the state of alarm. One of the major consequences was the promotion of remote working –particularly teleworking– as a tool to bring together restrictions to mobility

and economic activity. This has led to a significant increase of teleworking in our country, even when the first wave of the pandemic was already over; and both, companies and workers, might bet for this more flexible way of working in the future. The approval of a new legal framework for teleworking should provide higher legal certainty for its implementation, once the health crisis is over. Collective bargaining will become a necessary tool in the development of such legal framework as the way to stipulate the rights and duties of employers and employees in this field.

Key words: Remote working, Teleworking, Covid-19, confinement, collective bargaining, privacy and data security

La protección de los datos personales en las empresas. Análisis de las normas aplicables y principios protectores. The protection of personal data in companies. Analysis of the applicable rules and protective principles.

Por Claudia Victoria San Martín Rodríguez

RESUMEN

Un completo análisis sobre la normativa y los principios generales

aplicables en materia de Protección de Datos personales para las

empresas en España permitirá alcanzar una reflexión sobre la adecuación de estas herramientas legales disponibles que garantizan el derecho fundamental a la intimidad. A pesar de su relativa juventud, es manifiesta la inculcación de estos principios en la sociedad y en el tejido productivo y su probada efectividad en la resolución de las mayores amenazas que las nuevas tecnologías provocan sobre los datos personales. La

acelerada velocidad de estas últimas, sin embargo, supera la capacidad de adaptación que tiene el derecho a los cambios que provocan y, por tanto, es preciso abordar actualizaciones y mejoras constantes tanto de estas normativas como de sus sistemas de control.

Palabras clave: Protección de datos, intimidad, contexto legal, datos personales laborales, privacidad en la empresa.

ABSTRACT

A complete analysis of the regulations and general principles applicable to the Protection of Personal Data for companies in Spain will allow to reflect on the adequacy of these available legal tools that guarantee the fundamental right to privacy. Despite their relative youth, the inculcation of these principles is manifest in society and in the productive fabric and their proven effectiveness in solving the greatest threats that new technologies cause on personal data. The accelerated speed of the latter, however, exceeds the adaptability that the right has to the changes they cause and, therefore, constant updates and improvements must be addressed both in these regulations and in their control systems.

KEY WORDS: Data protection, privacy, legal context, personal work data, privacy in the company.

Riesgos jurídicos del uso de datos intermediados: el caso de la plataforma de intermediación de datos.

Legal risks of the use of mediated data: the case of the data mediated platform

Por Eva Martín Ibáñez

RESUMEN

El uso de datos intermediados está cada vez más extendido en los trámites administrativos. Es resultado de la implantación de medios electrónicos en las Administraciones Públicas. Las plataformas de intermediación de datos facilitan el derecho de los ciudadanos a no aportar documentos. Además permiten que las Administraciones Públicas validen los datos de forma automatizada. Sin embargo, la utilización de servicios de datos intermediados también puede tener otras consecuencias que es necesario evaluar con un enfoque de riesgos jurídicos.

Palabras clave: Datos; datos intermediados; riesgo; riesgo jurídico; Administración digital

ABSTRACT

The use of intermediated data is increasingly growing in administrative procedures. This is a one of the many outcomes of the implementation of electronic means in the Public Administration. The intermediated data platforms enable citizen's right to not submit documents. Furthermore, it makes possible for the Public Administration to automate data validation. Nevertheless, the usage of intermediated data services can also lead to consequences that need to be assessed on a legal risk-based approach.

Key words: Data; intermediated data; risk; legal risks; eGovernment

La encuesta #20 GOOGLE y la eliminación cookies de terceros.

Por Nuria Díaz-Varela Arrese

El sudor como muestra analítica y sus posibilidades en el marco clínico y legal.

Sweat as analytical sample and its possibilities in the clinical and legal fields.

Por Feliciano Priego Capote

RESUMEN

El sudor es un biofluido corporal que está recibiendo un interés creciente debido a su potencial en aplicaciones clínicas y forenses. Sin embargo, su utilización aún requiere una estandarización con el fin de poder reproducir resultados entre diferentes laboratorios. Entre sus ventajas destaca el muestreo no invasivo, la diversidad de posibilidades de muestreo, su composición relativamente sencilla y su fácil manejo. Estos factores hacen que su análisis pueda aportar información sobre parámetros bioquímicos, como pueden ser la osmolaridad o el pH, que pueden asociarse, por ejemplo, con el nivel de hidratación, y sobre la presencia y concentración de metabolitos endógenos y exógenos. Esta última opción permite la utilización

del sudor como fuente de biomarcadores clínicos y forenses para la detección de patologías, exposición a agentes tóxicos, o para la elucidación de la causa de muerte en situaciones en las que obtener información con otras muestras convencionales no aporten la información deseada.

Palabras clave: Sudor; análisis clínico; análisis forense; toxicología; metabolómica.

ABSTRACT

Sweat is a body biofluid that is receiving increasing interest due to its potential in clinical and forensic applications. However, its

use still requires standardization in order to be able to reproduce results between different laboratories. Its advantages include non-invasive sampling, the diversity of sampling possibilities, its relatively simple composition and its easy handling. These factors support the análisis of sweat to provide information on biochemical parameters, such as osmolarity or pH, which can be associated, for example, with the level of hydration, and on the presence and concentration of endogenous and exogenous metabolites. This last option allows the use of sweat as a source of clinical and forensic biomarkers for the detection of pathologies, exposure to toxic agents, or for the elucidation of the cause of death in situations in which obtaining information with other conventional samples does not provide the information. desired.

Key words: Sweat; clinical analysis; forensic analysis; toxicology; metabolomics.

EN RED N° 20

Número 19

CARTA DEL DIRECTOR

Por Pablo García Mexía

¿Gobbernaza de Big Data?

¿Big Data governance?

Por Domingo Sugranyes Bickel

**Lingüística computacional y tecnologías del lenguaje.
Computational linguistics and language technologies.**

Por Carmen Torrijos Caruda

RESUMEN

La lingüística computacional es un campo poco conocido de la Inteligencia Artificial que tiene como particularidad la hibridación de dos mundos: por un lado, la lingüística teórica y aplicada y, por otro, la ingeniería informática o computación. Este artículo realiza una revisión del estado del Procesamiento del Lenguaje Natural (PLN) fundamentalmente en España, resumiendo el avance técnico de la disciplina en los últimos años y la configuración de nuevos perfiles y equipos técnicos. A lo largo del artículo se expone la importancia de la lingüística computacional en la sociedad digital, del mismo modo que se realiza una aproximación metodológica al funcionamiento de los sistemas de PLN, desde las herramientas automáticas de análisis lingüístico y las fases básicas de procesamiento hasta las últimas tecnologías de vectorización contextual. Se analiza cuáles son las aplicaciones de PLN más demandadas actualmente por empresas e instituciones, como el análisis del sentimiento, la clasificación masiva de texto, la traducción automática o las respuestas automáticas a preguntas. La descripción de estas tareas servirá también para reflexionar sobre qué significa «comprensión» o «aprendizaje» en el ámbito de las máquinas. Finalmente, se revisan los nuevos perfiles profesionales en torno a la figura del lingüista computacional, los últimos cambios en la formación universitaria, el acceso al mercado laboral y su integración en equipos tecnológicos.

Palabras clave: Lingüística computacional, Procesamiento del Lenguaje Natural, PLN, Inteligencia Artificial, Big Data,

Ingeniería Informática, Tecnología de la Información,
Lingüística, Tecnología.

ABSTRACT

Computational linguistics is a not very well-known field of Artificial Intelligence that has as a particularity the hybridization of two worlds: on the one hand, theoretical and applied linguistics and, on the other hand, computer engineering or information technology (IT). This article reviews the state of Natural Language Processing (NLP) mainly in Spain, summarizing the technical progress of the discipline in recent years and the configuration of new profiles and technical teams. Throughout the article, it is explained the importance of computational linguistics for our digital society, as well as a methodological approach to the functioning of NLP systems, from automatic linguistic análisis tools and basic processing stages to the latest contextual embeddings technologies. The most demanded NLP applications by companies and public institutions are exposed, such as sentiment analysis, massive text classification, machine translation or automatic question answering. The description of these tasks will also lead to a reflection on what it means “understanding” or “learning” when talking in terms of machines. Finally, the new professional profiles around computational linguistics are reviewed, as well as the latest changes in university training, access to work positions and computational linguists integration in technological teams.

Key words: Computational Linguistics, Natural Language Processing, NLP, Artificial Intelligence, Big Data, Computer Engineering, Information Technology, Linguistics, Technology.

Puertas traseras, criptografía y teléfonos móviles; o el conflicto entre privacidad e investigación policial.

Backdoors, cryptography and mobile phones; or the conflict between privacy and police investigation

Por Javier Junquera

RESUMEN

La adopción masiva de la telefonía móvil ha tejido una enorme red, de la cual es posible extraer cantidades ingentes de información. Cada uno de los dispositivos que la conforman es un auténtico dossier sobre su dueño, en el que puede estar registrado desde sus hábitos de sueño hasta sus intereses más privados. La divulgación de este contenido tan sensible supondría una vulneración de la intimidad del usuario, de una magnitud inimaginable hace tan solo diez años. Es por ello que, tanto los propios usuarios como la industria, han centrado sus esfuerzos en crear medidas de protección cada vez más robustas. Sin embargo, estas medidas pueden suponer un obstáculo infranqueable cuando se cruzan en el camino de una investigación policial.

La carrera por el control de la información ha trascendido, si es que alguna vez ha estado limitado a él, el plano técnico; y son cada vez más las iniciativas que, aduciendo velar por la seguridad nacional, abogan por poner cotas a la criptografía, o establecer regulaciones que permitan sortear las medidas de seguridad: es decir, puertas traseras. En este artículo se expondrá por qué las puertas traseras son nocivas para la seguridad de la ciudadanía, y de qué maneras puede encontrarse un compromiso entre privacidad y cumplimiento de la ley.

Palabras clave: puertas traseras, ciberseguridad, criptografía, privacidad.

ABSTRACT

The massive adoption of mobile telephony has made an enormous network from which it is possible to extract large amounts of information. Each device in this network is a dossier of its owner, where could be registered from his sleep habits to his most private interests. The divulgation of such sensitive information could suppose trespassing into the users' privacy of a magnitude unimaginable just ten years ago. Therefore, both users and industry have been putting their efforts on the creation of new robust protection techniques. Nevertheless, these measures could be an obstacle for crime investigations.

The career for the information control has transcended the technical dimension if has ever been limited to it. There are more and more governmental initiatives advocating for the limitation of cryptography, or even looking to regulate the creation of mechanisms for overcoming those security measures: in other words, for creating backdoors. This article aims to prove why back-doors are a dangerous idea for the security of the people, and how could be found a compromiso between privacy and compliance.

Key words: backdoors, cybersecurity, cryptography, privacy.

El turismo en la economía de los datos y la economía de plataformas en la UE. Especial referencia al reglamento UE 1150/2019

Turism in the platform economy and the data economy in the EU.

Special attention to EU Regulation 1150/2019

Por José Antonio Castillo Parrilla

RESUMEN

El sector turístico es un importante activo en la economía digital, que se ha transformado en lo que se conoce como economía de plataformas. La mayor parte de empresas (hoteles, restaurantes, guías) relacionadas con el sector turístico ofrecen sus servicios en internet, y especialmente a través de plataformas especializadas y conocidas por todos. En la medida en que la gran mayoría de la oferta se produce a través de plataformas o motores de búsqueda, los empresarios acaban ocupando una posición de debilidad contractual que genera una excesiva indefensión. Esta indefensión se debe por una parte a esta debilidad contractual, pero también a la opacidad de los algoritmos que gobiernan los índices de prelación de ofertas y a la escasez de normas que los puedan proteger frente a comentarios negativos en internet.

El Reglamento UE 1150/2019 pretende ser un primer paso para solucionar estos problemas, que deben encuadrarse en un context en que los datos como activo económico adquieren cada vez más valor; debido, entre otras razones, a que son la materia prima con que se extrae la información útil que permite a las plataformas y motores de búsqueda aconsejar de manera personalizada a cada usuario sobre lo que está buscando.

Palabras clave: Turismo, economía de plataformas, economía de datos, Reglamento UE 1150/2019, transparencia de los algoritmos, usuarios profesionales, protección de la parte débil.

ABSTRACT

The tourism sector is an important part of the digital economy, and the digital economy cannot be understood without the idea of “platform economy”. The vast majority of tourist businesses offer their products and services through platforms and search engines. Since it is so, those businesses are weak before the platforms and the search engines. This weakness is related to their contract weakness, but also to the lack of algorithms transparency (since algorithms govern the offer classification indexes), and the lack of rules protecting businesses against bad comments by users. EU Regulation 1150/2019 pretends to be a first step to solve these problems. Finally, data have revealed as a very important economic asset. Among other reasons, data are the raw material to build up useful knowledge to microtargeting and the offers classification in the platform economy.

Key words: Tourism, platform economy, data economy, EU Regulation 1150/2019, algorithm transparency, business users, protection of the weaker party.

El camino al infierno está empedrado de buenas intenciones: reflexiones sobre el ONLINE HARMS White paper y la libertad de expresión en Internet

The road to hell is paved with good intentions: considerations on the online harms white paper and freedom of expression on the internet

Por José Ignacio Herce Maza

RESUMEN

El "Online Harms White Paper" es un documento británico que propone establecer una regulación de los contenidos nocivos en la Red. Si bien es cierto es una propuesta bienintencionada y destinada al servicio al interés general puede colisionar con algunos derechos y libertades inherentes a Internet. En este trabajo se estudiará sus posibles colisiones con el derecho fundamental a la libertad de expresión.

Palabras clave: Regulación – Internet – Daños en Línea – derechos Fundamentales – Buena Administración.

ABSTRACT

"Online Harms White Paper" is a British document that proposes to establish a regulation of harmful content on the Internet. Although it is true, it is a well-intentioned proposal and aimed at serving the general interest, it may collide with some inherent rights and freedoms in Internet. This work will study its possible collisions with the fundamental right to freedom of expression.

Key words: Regulation – Internet – Online Damage – Fundamental Rights – Good Administration.

La encuesta #19 freno a libra

Por Santiago Navarro de Andrés

Covid 19 y protección de datos, breve comentario a los informes de las Autoridades Española y Europea.
COVID 19 and data protection. Brief commentary on the reports of the spanish and european authorities

Por Luis Felipe López Álvarez

EN RED N° 19

Número 18

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

A modo de ensayo urgente: la seguridad y privacidad en las aplicaciones tecnológicas vinculadas a la Pandemia COVID-19.

Tracing COVID-19: privacy and security issues.

Por Ángel Gómez de Ágreda y M^a Belén Andreu Martínez

COVID 19, Interés general y Derechos Fundamentales.

COVID 19, general interest and fundamental rights.

Por Jaime Rodríguez-Arana

El Passenger name record (PNR) en la Unión Europea para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y delincuencia grave, como instrumento de cooperación.

The Passenger Name Record (PNR) in the European Union for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, as an instrument of cooperation

Por Nicolás del Solar Duarte

RESUMEN

El trabajo de investigación analiza el Sistema de registro de nombres de los pasajeros (Passenger Name Record) como mecanismo para la prevención del terrorismo y otras formas de delincuencia grave, y las dificultades que tuvo su implementación en la UE. No obstante, su aprobación mediante la Directiva (UE) 2016/681, el sistema europeo PNR mantiene muchos de los cuestionamientos formulados previos a su adopción, en particular, aquellos respecto a su relación con los derechos fundamentales de las personas dadas las características intrusivas y represivas propias del mecanismo. Se analiza en particular el caso español (único país que no ha traspuesto la directiva) como ejemplo de los criterios y alcances que puede sufrir el Sistema en la práctica y se reflexiona sobre las decisiones tomadas por dicho estado a la luz de los principios de necesidad y proporcionalidad.

PALABRAS CLAVE: Registro de Nombres de Pasajeros, PNR, Privacidad, Proporcionalidad, Necesidad, Seguridad.

ABSTRACT

The research work analyses the Passenger Name Record (PNR) system as a mechanism for the prevention of terrorism and other forms of serious crime, and the difficulties encountered in its implementation in the EU.

However, its approval through Directive (EU) 2016/681, the European PNR system maintains many of the questions raised

prior to its adoption, in particular, those regarding its relationship with the fundamental rights of persons given the intrusive and repressive characteristics of the mechanism.

In particular, the Spanish case (the only country that has not transposed the directive) is analysed as an example of the criteria and scope that the system may suffer in practice and the decisions taken by this state are reflected upon in the light of the principles of necessity and proportionality.

KEY WORDS: Passenger Name Record, PNR, Privacy, Proportionality, Necessity, Security

Blockchain and National Security.

Blockchain y seguridad nacional

Por Vicente Moret Millás

ABSTRACT

Blockchain technology is becoming a disruptive element in the digital environment according to the high expectations it is generating. Although its real impact is particularly evident in relation with crypto currencies, applications that are already being developed and will be developed in the future, mean that this technology is called to have a real impact on issues related to the States national security. The implications of Blockchain for national security are known today, but they are only a part of the many derivatives that will emerge as this technology develops in the coming years. New opportunities will arise to increase our security and increase our economic and social development, but also next to these brilliant new digital milestones will arise new risks, as has been common throughout the History in relation with technological innovations.

KEY WORDS: Blockchain, national security, cybersecurity, cryptocurrencies, financial security, cybercrime, online fraud, ransomware, money laundering, supply chains.

RESUMEN

La tecnología Blockchain se está convirtiendo en un elemento disruptivo en el entorno digital de acuerdo con las altas expectativas que está generando. Aunque su impacto real es particularmente evidente en la aparición de criptomonedas, las utilidades y aplicaciones que ya se están desarrollando y se desarrollarán en el futuro, significan que esta tecnología va a tener un impacto real en cuestiones relacionadas con la seguridad nacional de los Estados. Hoy se conocen las implicaciones del Blockchain para la seguridad nacional, pero son solo una parte de las muchas derivadas que surgirán a medida que esta tecnología se desarrolle en los próximos años. Surgirán nuevas oportunidades para aumentar nuestra seguridad y aumentar nuestro desarrollo económico y social, pero también junto a estos nuevos hitos digitales brillantes surgirán nuevos riesgos, como por otra parte, ha sido común a lo largo de la Historia de la Humanidad.

PALABRAS CLAVE: Blockchain, seguridad nacional, ciberseguridad, criptomonedas, seguridad económica, ciberdelitos, fraude online, ransomware, blanqueo, cadenas de suministro.

El cuarto poder independiente. Ejercicio de la responsabilidad en el Gobierno Inteligente: regulación de la inteligencia artificial, tecnologías basadas en software y big data.

A fourth government branch. Accountability in smart government development: The regulation artificial intelligence, software-enabled technologies and big data

Por Olga Gil

RESUMEN

El siguiente trabajo defiende que las ideas, como cemento de las sociedades, hacen problemático consagrar la gobernanza de la inteligencia artificial al mundo de los dispositivos, y explica porqué. El trabajo también defiende que las características de la inteligencia artificial suponen una oportunidad para revisar las prioridades de los gobiernos desde una perspectiva multinivel, desde el nivel local hasta niveles supranacionales. En términos éticos, el trabajo enfatiza la tensión existente entre impulsar un mayor y más rápido avance de la tecnología centrado en la innovación, y el bienestar humano -donde este bienestar no está garantizado automáticamente por defecto. Esta tensión podría resolverse mediante un juego positivo en el que los actores participantes ganan, un resultado que a día de hoy no se ha producido ni se ha resuelto, ni en el ámbito de la investigación ni en el desarrollo de instituciones o instrumentos de gobierno públicos y privados. Finalmente, el artículo propone el desarrollo democrático de una cuarta rama gubernamental independiente, dotada para garantizar que los algoritmos de las democracias se ajusten a los principios de las Constituciones. El propósito de esta cuarta rama del gobierno en las democracias modernas sería consagrar la responsabilidad del desarrollo de la inteligencia artificial, incluidas las tecnologías habilitadas por software, y la implementación de políticas basadas en grandes datos, dentro de un contexto de régimen democrático más amplio.

PALABRAS CLAVE: Inteligencia artificial, big data, transparencia, responsabilidad, democracia, políticas públicas, regulación

ABSTRACT

The following work argues that ideas, being the cement of society, create obstacles for integrating governance of artificial intelligence into the world of devices. This work also posits that the features of artificial intelligence provide an opportunity to revise government priorities from a multilevel perspective. On ethical grounds, this work identifies the trade-off today that results from the simultaneous push for greater and faster technological advancement and innovation, and human wellbeing, which is not, by default, guaranteed. This trade-off, however, could be achieved in the future but is currently unresolved due to the current state of research, as well as the limits on the development of practical and applied private and public policy instruments. Finally, the article proposes a fourth independent government branch that would be endowed to ensure that algorithms in present democracies conform to constitutional principles. The purpose of adding this fourth governmental branch within modern democracies would be to enshrine the accountability of artificial intelligence development, including software-enabled technologies, and the implementation of policies based on big data within the context of a wider democratic regime.

KEY WORDS: artificial intelligence, big data, accountability, governance, democracy, public policies, regulation.

BLOCKCHAIN: securities regulation.

BLOCKCHAIN: regulación de valores.

Por Alfonso Codes Calatrava

RESUMEN

Por medio del presente artículo, el autor realiza un análisis general de las posibles consecuencias que Blockchain puede tener en la regulación de los mercados de valores, desde una perspectiva global. Por ello, se se ha decidido enfocar este capítulo desde una perspectiva conceptual básica y general que permita extraer unas conclusiones introductorias en cuanto a la relación blockchain y mercados de valores, sobre las que luego puedan cimentarse estudios específicos que surjan a medida que se vayan profundizando los análisis técnicos experimentales realizados por las propias entidades públicas y privadas, protagonistas de estos mercados. De lo contrario, se caería en la improductiva tentación de convertir este capítulo en un intento visionario de vaticinar lo que aún no se ha desarrollado; o lo que es peor, en la poco pragmática labor de descender al estudio pormenorizado de aspectos conceptuales y funcionales que aún está por saber si serán, o no, definitivos.

ABSTRACT

In this article, the author performs a general analysis of the possible consequences that Blockchain may have on the regulation of the securities markets, from a global perspective. All this means that, in the opinion of this author, it is more didactic to approach this chapter from a basic and general conceptual perspective that allows introductory conclusions to be drawn regarding the relationship between blockchain and securities markets, on which specific studies can then be based as the experimental technical analyses carried out by the public and private entities themselves, the protagonists of these

markets, become more in-depth. Otherwise, there would be the unproductive temptation to turn this chapter into a visionary attempt to predict what has not yet been developed; or worse, the little pragmatic work of descending to the detailed study of conceptual and functional aspects that it remains to be seen whether or not they will be definitive.

PALABRAS CLAVE: Blockchain, mercado de valores, regulación de valores (Blockchain, securities markets, securities regulation).

**El COVID-19, información sanitaria y “fake News”.
COVID-19, health information and “fake news”.**

Por Francisco Javier Sanz Larruga

**La encuesta #18 La limitación del ancho de banda
consecuencia de la saturación de Internet por COVID-19.**

Por José Morales Barroso

EN RED N° 18

Número 17

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

El creciente interés en los datos personales de los conductores de vehículos conectados.

Growing interest in personal data of drivers of connected.

Por Lucia Aragües Valenzuela

RESUMEN

Actualmente existe cierto aumento del número de dispositivos que utilizan los servicios de comunicación mediante “objetos inteligentes”, no siendo operados directamente por el ser humano, sino que, en realidad, se encuentran implantados en los objetos que los mismos utilizan, como pudiera ser un vehículo de conducción. Sin embargo, la utilización de estos dispositivos puede diseñarse con cierta intencionalidad al almacenar datos privados de los usuarios, permitiéndose incluso hackear el vehículo conectado de forma inalámbrica. Esta situación determina una cierta vulnerabilidad de los conductores ante incluso posibles amenazas de seguridad cibernética, ocasionando en cualquier caso dicha hiperconectividad un cierto riesgo en los datos personales de los conductores. Resulta imprescindible reflexionar sobre estos términos y, más concretamente, sobre si dichos vehículos conectados cumplen -o no- con las previsiones del Reglamento General Europeo de Protección de Datos.

Palabras clave: Datos, vehículos, protección, conectividad, Internet

ABSTRACT

Currently there is a certain increase in the number of devices that use communication services through “intelligent objects”, not being directly operated by human beings, but actually implanted in the objects they use, such as a private driving vehicle. However, the use of these devices can be designed with some intention to store users’ private data, even allowing

hacking the connected vehicle in a wireless way. This situation results in a certain vulnerability of drivers to even potential cybersecurity threats, with such hyper-connectivity causing a certain risk to drivers' personal data. It is essential to reflect on these terms and, more specifically, on whether or not these connected vehicles comply with the provisions of the European General Data Protection Regulation.

Key words: Data, vehicles, protection, connectivity, Internet.

La transparencia algorítmica en el tratamiento de los datos personales.

Algorithmic transparency in the processing of personal data.

Por Gonzalo Rodríguez Martínez

RESUMEN

En el presente trabajo se realiza un análisis sobre la transparencia exigida en las decisiones individuales automatizadas que produzcan efectos jurídicos sobre las personas o les afecte significativamente de modo similar. Debido a los riesgos inherentes este tipo de tratamientos, el Reglamento (UE) 2016/679, General de Protección de Datos establece una protección especialmente reforzada, imponiendo a los responsables del tratamiento, unas estrictas obligaciones de información cuyo contenido y alcance resulta controvertido, no sólo por los límites derivados de otros derechos contrapuestos, como la propiedad intelectual y los secretos comerciales de los algoritmos utilizados a tal efecto por aquellos, sino también por los límites técnicos derivados de la complejidad de los mismos. Además, a tales derechos de

información se añaden otras garantías mínimas que los responsables deberán respetar en todo caso.

Palabras clave: Datos personales. Transparencia algorítmica. Derecho a una explicación.

ABSTRACT

In this paper, an analysis is made of the transparency required in automated individual decisions that produce legal effects on individuals or significantly affect them in a similar way. Due to the inherent risks of this type of processing, Regulation (EU) 2016/679, General Data Protection, establishes a particularly reinforced protection, imposing on the data controllers strict information obligations whose content and scope is controversial, not only because of the limits derived from other conflicting rights, such as intellectual property and trade secrets of the algorithms used for this purpose by the data controllers, but also because of the technical limits derived from the complexity of the algorithms and, in particular, in those based on automatic learning systems. In addition to these rights to information, there are other minimum guarantees that those responsible must respect in all cases.

Key words: Personal Data. Algorithmic transparency. The right to an explanation.

La instauración por parte de los Ayuntamientos de sistemas de control de jornada laboral basados en el registro de los datos de dactiloscópicos de sus empleados. The implementation by city councils of supervisory systems of working times based on the fingerprint data of its employees.

Por Ángela H. Martínez López

RESUMEN

El presente estudio aborda la cuestión de la instauración por parte de los Ayuntamientos en España de sistemas de control de jornada laboral basados en el registro de los datos dactiloscópicos de sus empleados. Se procederá en primer lugar a analizar si los citados sistemas son ajustados a Derecho, de conformidad con la normativa correspondiente. Se expondrán a continuación las obligaciones que recaen sobre los Ayuntamientos en lo concerniente al registro de los datos dactiloscópicos de sus empleados, así como las implicaciones que para éstos tiene dicho registro. Por último, se finalizará el estudio con unas breves conclusiones.

Palabras clave: protección de datos, datos biométricos, datos dactiloscópicos, huellas digitales, Reglamento Europeo de Protección de Datos, LOPD, Ayuntamientos, Administración Pública.

ABSTRACT

The present study delves into the intricacies of the implementation by Town Halls in Spain of registration systems based on biometric fingerprint data for the purpose of controlling the working times of their employees. At the outset, the legal basis for such a system will be explored. Further on, the obligations of the Town Halls vis-à-vis their employees in what concerns the registration of the latter's fingerprint data will be presented, as well as what this implies for the said employees. Finally, the analysis will be closed with a number of conclusive remarks.

Key words: Data protection, biometric data, fingerprints, GDPR, LOPD, Town hall, Municipality, Public Administration.

Hacia la excelencia del dictamen pericial en materias tecnológicas en una sociedad digitalizada.

Towards the excellence of the expert report about technological subjects a digitized society.

Por Antonio Luis Flores Galea.

RESUMEN

Vivimos en una sociedad cada vez más digitalizada, donde tanto ciudadanos como empresas recurren a las nuevas tecnologías para ejecutar sus tareas diarias y procesos de negocio, respectivamente. En este escenario, es esperable un proporcional crecimiento en el número de conflictos y demandas judiciales donde las TIC jueguen un papel primordial y, por ende, una mayor demanda de informes periciales. Paralelamente, debido a la complejidad que presenta la elaboración de los mismos, dada la elevada complejidad de los ecosistemas tecnológicos y su enorme variabilidad con el tiempo, se puede esperar también una mayor necesidad de calidad y eficacia, con un doble objetivo: (1) comprender correctamente y en detalle la cuestión del conflicto, y (2) convencer, de manera clara, concisa y con el mínimo coste económico y en tiempo, de la realidad de los hechos, con el fin de facilitar un mejor acuerdo entre las partes o ayudar al juez a dictar una sentencia lo más razonada y ajustada posible a la realidad juzgada.

En este artículo se ofrece una serie de recomendaciones, procedentes de estándares emitidos por organizaciones internacionales de reconocido prestigio y también por la experiencia y conocimientos del propio autor, para que el

jurista tenga más y mejores herramientas para seleccionar al mejor perito para cada caso y evaluar su trabajo de manera objetiva.

Palabras clave: Perito, pericial, metodología, dictamen, prueba, perito tecnológico, informe pericial.

ABSTRACT

We live in an increasingly digitised society, where citizens and companies use new technologies to execute their daily tasks and business processes, respectively. In this scenario, we may expect proportional growth in the number of conflicts and lawsuits where ICT takes centre stage and, therefore, a greater demand for expert reports is also expected. In parallel, due to the complexity of producing these reports, given the high complexity of technological ecosystems and their enormous variability along time, a greater need for quality and efficiency can be presumed, with a double objective: (1) to understand correctly and in detail the question of the conflict, and (2) to convince, in a clear, concise manner and with the minimum economic cost and time, of the reality of the facts, in order to facilitate a better agreement between the parties or help the judge to issue a sentence as reasoned and adjusted as possible to the reality that is judged.

This article offers a series of recommendations, based on standards issued by internationally recognised organisations and also on the author's experience and knowledge, so that the jurist has more and better tools to select the best expert for each case and evaluate his work, objectively.

Key words: Expert, judicial expert, methodology, expert opinion, expert report, proof, technology expert.

**El Derecho, de lo analógico a lo digital.
The law, switching from analog to digital.**

Por Manuel González-Meneses

EN RED N° 17

ENTREVISTA A JOSÉ MIGUEL MARTÍNEZ SANCHIZ

Año 2019

Número 16

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

Dilemas de la Sociedad Digital: ¿Nos salvarán las leyes de nosotros mismos?

Por Rafael Fernández Campos

Los retos de ser persona en el Mundo Digital

Por Pablo García Mexía

La vida del reglamento general de protección de datos: aclaraciones interpretativas prácticas de las disposiciones de RGPD.

Por Maite Valdecantos

Caso Huawei: ¿hacia una “Trampa de Tucídides” Digital? “Huawei Case”: Towards a digital thucydides’ s trap?

Por Alfonso Cuenca Miranda.

RESUMEN

El conocido como “caso Huawei” se inscribe en la pugna por el dominio de la tecnología 5G entre Estados Unidos y China, manifestación ésta de la lucha geopolítica entre ambos colosos. El ascenso de China al estatus de cohegemon mundial, y los planes de expansión de su ámbito de influencia, cuyo epítome es el Proyecto One Belt-One Road, ha provocado la reacción estadounidense. En el ámbito digital se asiste a una feroz competencia por dominar una tecnología clave para el devenir mundial, que podría provocar finalmente la división en bloques tecnológicos.

PALABRAS CLAVE: China, Estados Unidos, geopolítica, 5G, Huawei.

ABSTRACT

The so called “Huawei case” is framed within the struggle for the 5G worldwide supremacy between the United States and China, as a proof of the geopolitical fight between these two colossus. The rise of China to the status of global hegemon and the projects to extend its influence, whose most important evidence is the One Belt and One Road Plan, have caused the American reaction. In the digital field there is a fierce competition in order to dominate a key technology for the world’s future. Finally, this rivalry can cause a division in two technological blocks.

Key words: China, United States, geopolitics, 5G, Huawei.

El marco civil de internet y la regulación de internet en Brasil.

“Marco civil de internet” and internet regulation in Brazil.

Por María Rita Braga de Siqueira Neiva

RESUMEN

En las últimas décadas se ha vivido la ascensión de la denominada sociedad de información, una revolución social y tecnológica que ha causado profundas transformaciones en la manera como se establecen las relaciones sociales, económicas y políticas. Los cambios generados por las nuevas tecnologías, especialmente por internet, ponen de relieve la importancia de adaptar el derecho a esta nueva realidad, a través de la creación de normas que fomenten la innovación y el desarrollo de la sociedad de información. En ese sentido, la aprobación de la Ley 12.965/2014, conocida como Marco Civil de Internet (MCI), representa un gran logro de Brasil, esencial para el proceso de adaptación del ordenamiento jurídico a los avances tecnológicos. El presente trabajo busca reflexionar sobre los principios consagrados en el Marco Civil de Internet, en concreto: el principio de la privacidad, el principio de neutralidad de red y el principio de la libertad de expresión. Este último principio consiste en el fundamento del sistema de responsabilidad civil de los proveedores de internet construido en el MCI, aspecto que también merecerá especial atención en este trabajo.

Palabras clave: Internet, sociedad de información, Brasil, Marco Civil de Internet.

ABSTRACT

In the last decades there has been the ascension of the called information society, a social and technologic revolution that has caused deep transformations in the way the social, economic and politic relationships are established. The changes caused by the new Technologies, especially by the internet, bring up the importance of a needed adaptation of the law to this new reality, together with the fixation of norms that incentive innovation and the development of the information society. In this sense, the approval of Law 12.965/2014, known as Marco Civil de Internet (MCI), represents a great achievement of Brazil, essential for the process of adapting the legal system to technological advances. This work aims to reflect on the principles enshrined in Marco Civil de Internet, specifically: the principle of privacy, the principle of net neutrality and the principle of freedom of expression. This last principle is based on the civil liability system of Internet providers built in the MCI, which will also deserve special attention in this work.

Key words: Internet, information society, Brazil, Marco Civil de Internet.

La nueva estrategia nacional de Ciberseguridad 2019. National Cybersecurity Strategy 2019.

Por Carola Cadenas Sicilia

RESUMEN

La elección del tema del presente trabajo viene determinada por el interés que para la historia en tiempo presente¹ tienen los últimos acontecimientos acaecidos en el mundo que se iniciaron con los terribles atentados del 11 de septiembre en EEUU contra las Torres Gemelas y el Pentágono que originaron

un giro vertiginoso a la hora de abordar el fenómeno del terrorismo y el trato debido a los detenidos acusados de realizar tales actos. “La Administración estadounidense quiere intentar mantener a salvo internet de los ciberterroristas. El FBI ha lanzado una alerta contra el terrorismo cibernético, y el Senado norteamericano ha aprobado una serie de medidas que dan más facilidades a la policía para pinchar internet” 2. Ese día se produjo “un suceso sísmico de consecuencias incalculables”, así se refirió el académico Gilles Kepel al referirse al momento en que, como señaló la comisión de investigación de dichos atentados, “cambió el mundo”. Este trabajo, a partir de fuentes secundarias, tiene como objetivo analizar trabajos y estudios que han profundizado en el análisis de las nuevas amenazas a la seguridad que han nacido paralelas a los grandes avances tecnológicos. Las nuevas tecnologías informáticas, especialmente Internet, han sido también utilizadas frecuentemente, no solo por lo que pueda aportar al análisis historiográfico sino también en la búsqueda de fuentes documentales de la época.

Comenzaremos por una exposición de las nuevas amenazas a la seguridad y la consagración del ciberespacio como un nuevo espacio donde se desarrollan los conflictos para después profundizar en los antecedentes de la nueva Estrategia de Ciberseguridad Nacional y en la estructura, y líneas de actuación de esta última

Por último a modo de conclusiones se aportan las ideas más relevantes extraídas de la lectura de la diversa documentación y sitios de internet consultados.

Palabras clave: Ciberespacio, ciberseguridad, Estrategia de Seguridad Nacional, Estrategia Global de Seguridad de la Unión Europea.

ABSTRACT

The choice of this issue is determined by the concern of nowadays history, which began after the terrible attacks occurred on September 11 against the Twin Towers and the Pentagon. Those attacks originated a vertiginous change when it comes to tackling the terrorist phenomenon and the handling of detainees accused of carrying out those crimes. On that very date "a seismic event of incalculable consequences" occurred, according to the academic Gilles Kepel, referring to the moment when, as the commission of investigation pointed out, the world changed.

This study, based on secondary sources, aims to analyze works and studies that have deciphered in depth the new security threats which had their origin at the same time that new technologies develop. New computer technologies, especially the internet, have also been used frequently, not only because of its contribution to historiographic analysis, but also in order to search documentary sources of that time.

We will begin with an explanation of new security threats and ciber operation as a new war phenomenon, focusing on the antecedents of the new National Ciber Security Strategy and briefly defining the strategy and the lines of action. Finally, the most relevant ideas extracted from the reading of assorted documentation and main websites consulted are provided.

Key words: Cyberspace, cybersecurity, National Security Strategy, European Cyber-security Strategy.

LA ENCUESTA #16 INE Y EL RASTREO DE DATOS TELEFÓNICOS

Por Jorge Villarino Marzo

Entrevista 16 a Oferlia Tejerina

Número 15

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

Implicaciones de la transformación digital del Derecho y de la Abogacía.

Por Rodolfo Tesone Mendizábal

Sesgos y perspectiva cultural en el enfrentamiento de los algoritmos de inteligencia artificial.

Biases and cultural perspective in the training of the models of Artificial Intelligence algorithms.

Por Ángel Gómez de Ágreda e Idoia Ana Salazar García

RESUMEN

La implementación de sistemas de inteligencia Artificial supone un notable incremento de la eficiencia en general en cuanto a la gestión de los datos y la extracción de su valor. De hecho, los algoritmos son meros mecanismos de optimización de procesos. Sin embargo, los datos de los que se alimenta la máquina o los procesos que emplea en su entrenamiento pueden tener sesgos intencionados y/o no intencionados que condicionan definitivamente la toma de decisiones. Este hecho puede suponer un impacto social y/o profesional negativo cuando se emplean este tipo de tecnologías. El contexto

geográfico/cultural, e incluso temporal introduce condicionantes adicionales que pueden descontextualizarse en su aplicación. El objetivo del presente artículo es analizar los posibles sesgos no deseados en los algoritmos, así como identificar los diversos aspectos culturales que se deben de tener en cuenta en la vigilancia de dichos datos y procesos, para que la efectividad en su toma de decisiones venga acompañada de beneficios equivalentes para las personas.

Palabras clave: Inteligencia Artificial, datos, toma de decisiones, tecnología, ética, cultura.

ABSTRACT

The implementation of Artificial Intelligence systems poses a remarkable increase of the efficiency in general in terms of the management of the data and the extraction of its value. In fact, algorithms are mere mechanisms of process optimization. However, the data on which the machine feeds can have intentional and / or unintentional biases that definitively condition decision making. Awareness of this fact is fundamental to avoid a negative social and / or professional impact when using this type of technology.

The geographic / cultural context -even the temporal one- introduces additional factors which may decontextualize its application. The objective of this article is to analyze the possible undesired biases in the data used by the algorithms, as well as to identify the different cultural aspects that should be taken into account in the monitoring of said data and processes, so that the increase in their effectiveness in decision making brings along equivalent benefits for individuals.

Key Words: Artificial Intelligence, Big Data, decisión-making, technology, Ethics, culture

Energía y entorno digital.

Energy and digital environment.

Por Pablo García-Manzano Jiménez de Andrade

RESUMEN

La energía y la digitalización han estado en la raíz de todas las revoluciones económicas, y lo están también en la de la llamada cuarta revolución industrial. Los cambios acelerados y convergentes en uno y otro sector hacen posible que la energía, marcada históricamente por los altísimos costes de construcción y de operación y mantenimiento, afronte la llamada transición energética hacia una economía baja en carbono, segura y eficiente con un gran apoyo en las tecnologías digitales. Estas no solo hacen posible transformar la demanda o las aplicaciones finales (cuyo ejemplo más obvio es el vehículo eléctrico), sino que revolucionan también las formas de producción (generación distribuida) y suponen un reto para el jurista, que se enfrenta a nuevas formas de titularidad y contractuales bajo un esquema regulatorio por definición incompleto.

Palabras clave: Energía eléctrica, gas natural, digitalización, Blockchain, inteligencia artificial (IA), relaciones jurídicas.

ABSTRACT

Energy and digitalization have been at the root of all economic revolutions, and they are also at the root of the so-called fourth industrial revolution. Accelerated and converging changes in both sectors make it possible for energy, historically marked by

very high construction and operation and maintenance costs, to tackle the so-called energy transition to a low-carbon, secure and efficient economy with strong support from digital technologies. These not only make it possible to transform the demand or the final applications (the most obvious example of which is the electric vehicle), but also profoundly change the forms of production (distributed generation) and pose a challenge for the jurist, who is faced with new forms of ownership and contracts under a regulatory scheme by definition incomplete.

Key words: Electricity, natural gas, digitalization, Blockchain, artificial intelligence (AI), transactions.

La propiedad sobre el dato. ¿Cabe una vertiente patrimonial de la protección de datos?

Por Carmen Perete Ramírez y Pablo García Mexía

Aplicación de la tecnología Blockchain a emisiones de valores negociables.

Application of blockchain technology to issuances of tradeable securities.

Por Gonzalo Navarro Ruiz

RESUMEN

El presente artículo centra su interés en analizar si la eventual aplicación de la tecnología Blockchain o DLT al registro de emisiones de valores admitidos a negociación en mercados secundarios oficiales o sistemas multilaterales de negociación, y de las transacciones realizadas sobre los mismos, podría encontrar encaje normativo en la regulación actual o si, por el

contrario, sería necesario llevar a cabo una modificación de dicha regulación. Parece apropiado señalar en este punto el motivo que nos ha llevado a escribir un artículo sobre este tema tan actual, que no es otro que la enorme y creciente importancia que ha adquirido y está adquiriendo la tecnología Blockchain, siendo así que el Foro Económico Mundial estima que, para el año 2027, el 10% del producto interior bruto a escala mundial estará representado por esta tecnología. El referido análisis exige entender los orígenes relativos a la forma de representación de dichos valores negociables; orígenes que se configuran por la teoría de la incorporación del derecho al título, que da lugar al nacimiento de los títulos físicos, y su posterior evolución a la anotación en cuenta; con el fin de disponer de las herramientas conceptuales necesarias para delimitar, en este ámbito, el significado de uno de los elementos centrales de esta tecnología Blockchain, el Token. Es por ello por lo que el artículo se estructura en cuatro grandes apartados a lo largo de los cuales se abordan, de una forma sistemática, las materias anteriormente referidas, comenzando por la teoría de la incorporación del derecho al título; estudiando, a continuación, la anotación en cuenta como forma de representación que surge a consecuencia de la crisis del título-valor; deteniéndonos, seguidamente, en el régimen jurídico actual regulador de la anotación en cuenta y del registro contable; para, finalmente, dedicar el último bloque al estudio de la tecnología Blockchain, a la que concebimos como una consecuencia de la evolución de las anteriores formas de representación impulsada por los avances tecnológicos. En este último bloque dedicamos el apartado final a plasmar nuestras consideraciones normativas sobre un futuro registro contable basado en el uso de la tecnología Blockchain.

El artículo concluye con un apartado dedicado a las conclusiones, en las que, a modo de cierre, exponemos de forma ordenada y sucinta las ideas que consideramos esenciales sobre los distintos temas abordados a lo largo del mismo. El contenido del artículo está fundamentado en normativa nacional y comunitaria sobre el mercado de valores; publicaciones e informes de autoridades relevantes en el ámbito del mercado de valores (CNMV, Banco de España); y publicaciones, obras especializadas y opiniones doctrinales sobre los temas objeto de estudio.

Palabras clave: Anotación en cuenta, Blockchain, ICOs, depositarios centrales de valores, intermediarios, registro contable, títulos-valores, Token, valores negociables.

ABSTRACT

This article focuses on analyzing whether the possible application of the Blockchain or DLT technology to the registration of issuances of securities admitted to trading in official secondary markets or multilateral trading systems, and of the transactions carried out on them, could find a regulatory compliance in the current regulation or if, on the contrary, it would be necessary to carry out a modification of the referred regulation. It seems appropriate to point out, at this point, the reason that led us to write an article on this trending topic, which is the enormous and growing importance that Blockchain technology has acquired and is acquiring. In this sense, the World Economic Forum estimates that by the year 2027, 10% of the gross domestic product on a global scale will be represented by this technology. The aforementioned analysis requires understanding the origins of the form of representation of said negotiable securities; origins that are

configured by the theory of the incorporation of the right to the title, which gives rise to the birth of the physical titles, and its subsequent evolution to the account entry; in order to have the necessary conceptual tools to delimit, in this area, the meaning of one of the central elements of this Blockchain technology, the Token. That is why the article is divided into four major sections along which the subjects referred to above are addressed in a systematic way, starting with the theory of the incorporation of the right to the title; studying, then, the account entry as a form of representation that arises as a result of the crisis of the title-value; stopping next in the current legal regime regulating the book entry and the accounting registry; to finally devote the last block to the study of Blockchain technology, which we conceive as a consequence of the evolution of the previous forms of representation driven by technological advances. In this last block we devote the final section to reflect our regulatory considerations on a future accounting registry based on the use of Blockchain technology. The article concludes with a section devoted to the conclusions, in which, as a closing, we expose in an orderly and succinct way the ideas that we consider essential on the different topics addressed throughout it. The content of the article is based on national and community regulations on the securities market; publications and reports of relevant authorities in the field of the securities market (CNMV, Bank of Spain); and publications, specialized works and doctrinal opinions on the subjects under study.

Key words: Account entry, Blockchain, ICOs, central securities depositories, intermediaries, accounting registry, title-value, Token, tradeable securities.

EN PROSPECTIVA

¿Y ahora que? Tras la sentencia de inconstitucionalidad sobre la recopilación por los partidos de las opiniones políticas de los ciudadanos.

Por Borja Adsuara Varela

La encuesta #15 SPAM ELECTORAL

Por Elena Gil González y José García Herrero

Entrevista 15 a Victoria Ortega Benido

En Red nº 15

Número 14

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

Ciberseguridad, ciberdelincuencia y empresa: la respuesta Penal

Por Eloy Velasco Núñez

**Novedades regulatorias en materia de juegos de azar online: se refuerzan las obligaciones de compliance.
Regulatory developments in the on line gambling sector: compliance obligations are bolstered.**

Por Carmen Perete Ramírez

RESUMEN:

En los últimos meses se han aprobado una serie de normas de distinto rango que afectan de forma directa al sector de los juegos de azar, especialmente al del juego online, y que suponen un incremento sustancial de las obligaciones de cumplimiento normativo (compliance) de los operadores de juego. Estas normas establecen nuevas obligaciones en materia de identificación de jugadores, prevención del blanqueo de capitales y la financiación del terrorismo y lucha contra el fraude. Además, existen otras normas todavía en fase de tramitación que establecerán, asimismo, nuevas obligaciones en materia de publicidad y juego responsable. En este artículo se analizan las obligaciones que dichas normas comportan para los operadores de juego regulados por la Ley 13/2011, de 27 de mayo, de regulación del juego y se ponen encima de la mesa algunas dudas que plantea su aplicación.

Palabras clave: juegos de azar, lotería, compliance, cumplimiento normativo, prevención del blanqueo de capitales, fraude, menores de edad, interdicción, publicidad, comunicaciones comerciales, juego responsable.

ABSTRACT

In the last few months, a series of norms of different rank have been approved that directly affect the gambling sector, especially the online gambling sector, and which entail a substantial increase in the compliance obligations of gambling operators. These rules establish new obligations regarding the identification of players, the prevention of money laundering and the financing of terrorism and the fight against fraud. In addition, there are other rules still in the process of being approved that will also establish new obligations in the fields of advertising and responsible gaming. This article analyzes the

obligations that these rules entail for gaming operators regulated by Law 13/2011, of May 27, and puts forward some doubts that their application raises.

Key words: gaming, gambling, lottery, compliance, anti-money laundering, fraud, minors, self-prohibition, advertisement, commercial communications, responsible gaming.

Última voluntad digital, testamento digital, heredero digital: el mundo virtual de la transmisión hereditaria en el derecho español.

Digital last will, digital testamentary, digital heir: virtual word of hereditary transmission in Spanish law.

Por Francisca Ramón Fernández

RESUMEN

El mundo digital afecta al ámbito jurídico. La regulación actual de la sucesión dista considerablemente de las nuevas tecnologías de la información y comunicación (TICs) y no se admiten fórmulas digitales para la transmisión hereditaria. Se trata de analizar cómo el ámbito digital puede tener influencia en la transmisión hereditaria, así como a los problemas que pueden plantear la identidad digital, el soporte y la protección de datos de carácter personal. Se atenderá por un lado, la influencia de las nuevas tecnologías de la información y comunicación (TICs) en la figura básica de la sucesión mortis causa, en especial el caso del testamento ológrafo; y por otro lado, a la sucesión en los elementos digitales.

Palabras clave: Voluntad digital; normativa nacional; testamento; tecnologías de la información y comunicación (TICs); herencia.

ABSTRACT

The digital world concerns the legal field. The current regulation of the succession is considerably far away from the new Information and communication technologies (ICTs) and digital forms are not allowed for the hereditary transmission.

The aim is

to analyze how the digital domain can have an influence on hereditary transmission, as well as the problems that digital identity can pose, the support and protection of personal data. It will address on the one hand, the influence of the new information and communication technologies (ICTs) on the basic figure of the succession mortis causa, especially the case of the holographic will; on the other hand, the succession in the digital elements.

Keywords: Digital last will; national regulation, testament; information and communication technologies (ICTs); inheritance.

La nueva regulación sobre Ciberseguridad de Redes y Sistemas de Información en España: Preguntas y respuestas sobre el Real Decreto-ley 12/2018, de transposición de la Directiva NIS.

The new regulation on cybersecurity of networks and information systems in Spain: Questions and answers on the royal decreelaw 12/2018, of transposition of the NIS directive.

Por Francisco Javier Donaire Villa

RESUMEN

El presente artículo analiza la transposición de la Directiva 2016/1148, sobre Seguridad de Redes y Sistemas de Información (Directiva NIS), llevada a cabo en España por el Real Decreto-ley 12/2018. En él se trata de identificar y responder a los principales interrogantes que plantea, en relación con su contenido y con la constitucionalidad de la opción por un Decreto-ley como forma de transposición de la mencionada Directiva en el ordenamiento jurídico español.

Palabras clave: Ciberseguridad, Redes y Sistemas de Información, Directiva NIS, Real Decreto-ley 12/2018.

ABSTRACT

This paper deals with the implementation of Directive 2016/1148 on Security of Networks and Information Systems (NIS Directive) carried out in Spain by Royal Decree-Law 12/2018, trying to pose and answer the main questions it raises as regards its content, as well as on the constitutionality of the choice of a Decree-Law as the suitable source of law to implement the aforementioned Directive within the Spanish legal system.

Keywords: Cybersecurity, Information Networks and Systems, NIS Directive, Royal Decree-law 12/2018.

EN PROSPECTIVA

Reglamento General de Protección de Datos y Real Time Bidding.

Por Lorena Rivera Novillo

La encuesta #14 EDUCACIÓN Y NUEVAS TECNOLOGÍAS

Entrevista 14 a Oriol Pujol Vila

En Red nº 14

Número 13

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

Transición de la fuerza a la palabra, premisa de la nueva era

Por Federico Mayor Zaragoza

La neutralidad de la red: contexto jurídico y modelo de ejecución técnica.

Network neutrality: legal framework and technical implementation.

Por Margarita Robles Carrillo, Gabriel Maciá Fernández y Pedro García Teodoro

RESUMEN

La neutralidad de la red es un principio inscrito originariamente en el desarrollo de Internet y asociado a los fundamentos del ciberespacio. El estudio del desarrollo normativo de la neutralidad en el marco internacional y en el plano interno permite advertir las carencias en su articulación jurídica derivadas de la diversidad de regulaciones y de la progresiva limitación de su alcance y contenido. El análisis del modelo

técnico actual de gestión de la neutralidad pone de manifiesto la existencia de un conjunto de problemas que afecta tanto a operadores como a usuarios. La propuesta de un nuevo modelo de ejecución técnica tiene como objetivo resolver esa problemática ajustándose a los requerimientos tanto técnicos como jurídicos necesarios para dar efectividad a un concepto operativo de neutralidad.

PALABRAS CLAVE: Neutralidad de la red. Régimen jurídico. Aplicación técnica.

ABSTRACT

Network neutrality is a principle closely linked to the origins of the Internet and associated with the foundations of cyberspace. The study of international and national regulations on neutrality reveals certain lacks and dysfunctions. There are two main reasons for this situation: the diversity of regulations and the progressive limitation of the scope and content of neutrality. The analysis of the current technical model of neutrality management illustrates the existence of a set of problems affecting both operators and users. The proposal for a new technical execution model aims to solve this problem. The objective is to reconcile the adequate and necessary technical and legal requirements to give effectiveness to an operative concept of neutrality.

KEY WORDS: Network Neutrality. Legal framework. Technical implementation.

La Emergencia de las Redes Comunitarias y del Principio de Autodeterminación de Red: un Ejemplo de Gobernanza de

Internet.

The rise of community networks and of the network self-determination principle: an example of internet governance.

Por Luca Belli

RESUMEN

Este artículo argumenta que cualquier individuo debe gozar del derecho de “autodeterminación de red” y que tal principio, a esar de no ser todavía reconocidode jure, ya está siendo implementado de facto, gracias al desarrollo de redes comunitarias y a los proceso de gobernanza de Internet que estas redes alimentan. La autodeterminación de la red debe ser considerada como el derecho de asociarse libremente para definir, de forma democrática, el diseño, desarrollo y gestión de la infraestructura de redes comunitarias, a fin de buscar, transmitir y recibir informaciones e innovaciones libremente. Las redes comunitarias, en cuanto a ellas mismas, son infraestructuras de red basadas en la colaboración y se establecen de forma bottom-up para los miembros de las comunidades locales que las desarrollan y gestionan como un bien común. La primera sección de este artículo defiende que el principio de autodeterminación de red encuentra sus bases conceptuales en el derecho fundamental a la autodeterminación de las personas, así como en el derecho a la autodeterminación informacional. El estudio enfatiza que la autodeterminación de la red desempeña un papel fundamental, permitiendo que los individuos se asocien y junten esfuerzos para superar las brechas digitales de manera colaborativa. En esta perspectiva, la segunda sección del artículo examina una selección de redes comunitarias, destacando las externalidades positivas desencadenadas por

tales iniciativas que favorecen el establecimiento de nuevas estructuras de gobernanza participativa y el desarrollo de nuevos contenidos, aplicaciones y servicios que atienden las necesidades de las comunidades locales, empoderando a individuos previamente desconectados. El estudio ofrece evidencias que el desarrollo de redes comunitarias puede inducir varios beneficios, creando oportunidades de aprendizaje, estimulando el emprendimiento local, promoviendo la creación de nuevos empleos y revigorizando las conexiones sociales de las comunidades, a través de asociaciones multistakeholder, que acercan a instituciones locales con los empresarios y los miembros de las comunidades.

Palabras clave: Acceso a Internet; redes comunitarias; libertad de expresión; derechos humanos; autodeterminación.

ABSTRACT

This paper argues that every individual should enjoy a right to “network selfdetermination” and such principle, in spite of not being recognised de jure, is already implemented de facto, thanks to the development of Community Networks (CNs) and the processes that such initiatives nurture. Network self-determination should be seen as the right to freely associate in order to define, in a democratic fashion, the design, development and management of network infrastructure as a common good, so that all individuals can freely seek, impart and receive information and innovation. CNs are crowd-sourced networks, built, deployed and organised in a bottom-up fashion by the local community that manages them as commons. The first section of this paper argues that the right to network self-determination finds its basis in the fundamental

right to self-determination of people as well as in the right to “informational self-determination” that, since the 1980s, has been consecrated as an expression of the right to free development of the personality. The paper emphasises that, network self-determination plays a pivotal role allowing individuals to associate and join efforts to bridge digital divides in a bottomup fashion, freely developing common infrastructure. In this perspective, the second section of this paper examines a selection of CNs, highlighting the positive externalities triggered by such initiatives, with regard to the establishment of new governance structures as well as the development of new content, applications and services that cater for the needs of the local communities, empowering previously unconnected individuals. The paper offers evidence that the development of CNs can prompt several positive external-effects that considerably enhance the standards of living of individuals, creating learning opportunities, stimulating local entrepreneurship, fostering the creation of entirely new jobs, reviving social bounds amongst community members and fostering multistakeholder partnerships.

Keywords: Internet Access; Community Networks; Human Rights Freedom of Expression; Self-determination

Las redes sociales en las administraciones públicas: ¿una oportunidad perdida?

Social networks in public administration: a missed opportunity?

Por Mercedes Díaz García

RESUMEN

Las redes sociales han “revolucionado” nuestras vidas y también a nuestras Administraciones. Por ello, este artículo pretende mostrar cómo las Administraciones Públicas no pueden ser indiferentes a los cambios que traen consigo las tecnologías, cómo las redes sociales han cambiado las formas de comunicarnos, no solo a nivel individual sino también con las Administraciones y cómo estas han de incorporarlas a sus procedimientos habituales. Las redes sociales han venido para quedarse, pero, ¿es consciente de ello nuestro legislador? La evolución normativa, de la que hacemos un repaso, ha sido un cúmulo de oportunidades perdidas hasta la reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales. El primer paso está dado y, tal como se reconoce en el preámbulo de la citada Ley, internet se ha convertido en una realidad omnipresente en nuestras vidas que el derecho no puede ignorar.

PALABRAS CLAVES: Administración Públicas, redes sociales, derechos digitales, protección de datos, privacidad.

ABSTRACT

Social networks have “revolutionized” our lives and also our administrations. Therefore, this article aims to show how Public Administrations cannot be indifferent to the changes brought about by technologies, how social networks have changed the ways of communicating, not only individually but also with Administrations and how they have to incorporate them into their usual procedures. Social networks have come to stay, but is our legislator aware of this? The normative evolution, of which we review, has been an accumulation of lost opportunities until the recent Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the

Guarantee of Digital Rights. The first step has been taken and, as recognised in the preamble to the aforementioned Law, the Internet has become an omnipresent reality in our lives that the law cannot ignore.

KEYWORDS: Public Administration, social networks, digital rights, data protection, privacy.

EN PROSPECTIVA

Minería de datos en plataformas de entretenimiento de cara al RGPD.

Data mining in entertainment platforms facing the GDPR.

Por Valentina Moreno Zambran

RESUMEN

El ciberespacio se ha convertido en uno de los grandes espacios de socialización, aprendizaje y ocio, en el que el lector ha desarrollado un nuevo modelo de interacción con la información, enfrentándose a nuevos códigos y lenguajes (Díaz Noci, 2004). Estos nuevos códigos muchas veces escapan de los límites y consideraciones de la legislación, lo que ha obligado a las autoridades a adaptar el marco jurídico. Con el aumento de la actividad digital, ha surgido también una creciente preocupación por el tratamiento de los datos personales de los internautas, cuyas acciones en la red son monitorizadas y analizadas continuamente. En este marco, surge en Europa el Reglamento General de Protección de Datos (RGPD), que brinda al usuario la posibilidad de limitar e indagar sobre el uso se le da a sus datos personales y acciones, en la red y fuera de ella. En este artículo analizaremos el impacto de la RGPD en la

minería de datos en entornos de entretenimiento, como los massive multiplayer online role player games (MMORPGs) y las plataformas de vídeo bajo demanda. Una de las grandes posibilidades de estos entornos es el análisis no sólo de los gustos o comportamientos, sino de las competencias o elecciones de los usuarios en entornos lúdicos.

Palabras clave: Datamining, MMORPG, GDPR.

ABSTRACT

Cyberspace has become one of the great spaces for socialization, learning and leisure, in which the reader has developed a new model of interaction with information, confronting new codes and languages (Díaz Noci, 2004). These new codes often escape the limits and considerations of legislation, which has forced the authorities to adapt the legal framework. With the increase in digital activity, there has also been growing concern about the treatment of personal data of Internet users, whose actions on the network are continuously monitored and analyzed. Within this framework, the General Data Protection Regulation (GDPR) arises in Europe, which provides the user with the possibility of limiting and inquiring about the use given to their personal data and actions on the network, and outside of it. In this article, we will analyze the impact of the GDPR on data mining in entertainment environments, such as massive multiplayer online role player games (MMORPGs) and video on demand platforms. One of the great possibilities of these environments is the analysis, not only of the tastes or behaviors, but of the competences or choices of the users in playful environments.

Keywords: Datamining, MMORPG, GDPR.

La encuesta #13 a Juan Bestard Perelló
Salud y nuevas tecnologías

Entrevista a María Eugenia Gay

En Red nº 13

Año 2018

Número 12

CARTA DEL DIRECTOR

Por Pablo García Mexía

Tribuna de honor

La Internet Abierta, o Internet a secas.

Por João Damas

Perspectivas sobre el transhumanismo.

Por José Andrés Jiménez Martín

RESUMEN

Este artículo trata de compendiar los fundamentos básicos del transhumanismo, esbozando sus características fundamentales y la diversidad de las manifestaciones de este, así como el papel de la literatura de ciencia-ficción como instrumento predictivo para poder determinar su futuro, trazando también una breve perspectiva de su evolución

histórica y su estado actual, las posiciones de los intelectuales al respecto, así como un planteamiento de los tres principales pilares en los que se basan los potenciales desarrollos del transhumanismo: la manipulación genética de los seres humanos, la inteligencia artificial y la hibridación hombre-máquina. También se presentan una serie de cuestiones abiertas en las que se trata de analizar brevemente las perspectivas que plantean una serie de temas potencialmente controvertidos y las soluciones que serían aplicables. Finalmente, en las conclusiones versan sobre el cambio de paradigma que supondrá la aplicación de los ideales del transhumanismo.

Palabras clave: Transhumanismo, ingeniería genética, inteligencia artificial, nanotecnología.

ABSTRACT

This article tries to summarize the basic fundamentals of transhumanism, outlining its fundamental characteristics and the diversity of its manifestations, as well as the role of science fiction literature as a predictive tool to determine its future, also drawing a brief perspective on its historical evolution and its current state, the postures of the intellectuals in this regard, as well as an approach to the three main pillars on which the potential developments of transhumanism are based: the human genetic manipulation, artificial intelligence and man-machine hybridization. A series of open questions are also presented in which it is a question of briefly analyzing the perspectives posed by a series of potentially controversial topics and the solutions that would be applicable. Finally, the conclusions deal with the paradigm shift that the application of the ideals of transhumanism will entail.

Keywords: Transhumanism, Genetic Engineering, Artificial Intelligence, Nanotechnology.

Crypto-currencies: current regulation, challenges and proposals.

Por Vicente Moret Millás y Riccardo Mülchi Miera

RESUMEN

Para dar seguridad a la nueva realidad de las cripto-monedas, la regulación tiene un papel fundamental que jugar. No obstante, esa regulación siempre debe tener en cuenta el impacto que tiene en los mercados; un equilibrio que debe sopesarse constantemente. Este análisis de los aspectos legales actuales de las criptomonedas hace una serie de propuestas para los aspectos no regulados con el fin de preservar la integridad y la estabilidad financiera de España y el resto de la zona euro. Para que sea posible, es necesario crear nuevas cripto-monedas apoyadas por las autoridades monetarias. Existe una forma en que los gobiernos podrían aprovechar los beneficios de la tecnología blockchain: emitir su propia moneda. Para ello, la Unión Europea tendría que emitir una cripto-moneda con el mismo valor convertible que el euro, la cual podría denominarse CryptoEuro.

Palabras clave: criptomonedas, regulación, tecnología legal, blockchain, impuestos.

ABSTRACT

In order to give security to the brave new reality of crypto-currencies there is a critical role for regulation, but regulation should always take into account the impact that it has on

markets, a balance that must be constantly weighed. This analysis of the current legal aspects of cryptocurrencies presents a proposed policy for the unregulated aspects of cryptocurrencies for the purpose of preserve the integrity and the financial stability of Spain and rest of the Euro region. To make it possible

it is necessary to create new cryptocurrencies supported by monetary authorities. There is a way in which governments could take advantage of the benefits of the blockchain technology: Issuing their own currency. In order to that, the European Union would need to issue a cryptocurrency with the same convertible value as the Euro. It could be called the CryptoEuro.

Keywords: cryptocurrencies, regulation, legal tech, blockchain, taxation.

La Ciberseguridad en las Empresas

Por Francisco Navarro

RESUMEN

Mientras que la seguridad tradicional es principalmente una preocupación a nivel nacional, la seguridad cibernética es fundamentalmente una cuestión de interés internacional. Es esencial tener en cuenta que gran parte de lo que ocurre en un país puede originarse fuera de sus fronteras, lo que hace que la colaboración internacional sea vital.

Sin embargo, la seguridad cibernética no solo es una amenaza para la seguridad nacional e internacional, sino también un negocio en crecimiento. Los ataques cibernéticos causan pérdidas económicas, pero también presentan una oportunidad para desarrollar nuevos negocios. El sector de la

ciberseguridad es un mercado que crece a un 11-13% en todo el mundo. En los últimos años, ha modificado completamente la industria de la seguridad, creando roles completamente nuevos a un ritmo acelerado y demandando profesionales con nuevas habilidades para cumplir esos roles. Esto presenta una oportunidad única para que nuestro país y nuestras empresas desarrollen sus negocios en este nuevo sector.

Palabras Clave: Agencia Española de Protección de Datos (AEPD). Centro Criptológico Nacional (CCN). Centro Nacional de Inteligencia (CNI). Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). Ciberamenazas. Ciberarmas. Ciberataques. Cibercrisis. Ciberespacio. Cibernético. Cibersecuestro. Ciberseguridad. Crisis. Espacio Asimétrico. Global Commons. INCIBE (Instituto Nacional de Ciberseguridad de España). IOT (Internet of Things). Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). Malware. Mando Conjunto de Ciberdefensa (MCCD). Ransomware. Reglamento General de Protección de Datos (RGPD). Riesgos

ABSTRACT

Whereas traditional security is mainly a concern at a national level, Cybersecurity is fundamentally a matter of international concern. It is essential to bear in mind that, much of what happens in one country may originate outside its borders, thus making international collaboration vital. However, Cybersecurity is not only a threat to national and international security, but also a growing business. Cyber-attacks cause economic losses, but they also present an opportunity to develop new businesses. The cybersecurity sector is a market that grows at 11-13% worldwide. In the past years, it has

completely reshaped the security industry, creating completely new roles at fast pace and demanding professionals with new skills to fill those roles. This presents a unique opportunity for our country and our companies to develop their business in this new sector.

Keywords: Spanish Agency for Data Protection (AEPD). National Cryptologic Center (CCN). National Intelligence Center (CNI). National Center for the Protection of Critical Infrastructures (CNPIC). Cyber threats. Cyber weapons. Cyber-attacks. Cyber crisis. Cyberspace. Cybernetic. Virtual Kidnapping. Cybersecurity Crisis. Asymmetric space. Global Commons. INCIBE (National Cybersecurity Institute of Spain). IOT (Internet of Things). Organic Law on Data protection and Guarantee of Digital Rights (LOPDGDD). Malware. Joint Cyber Defense Command (MCCD). Ransomware. General Regulation of Data Protection (RGPD). Risks.

Reflexiones en torno a las ciudades inteligentes y el reglamento general de protección de datos

Por Dr. Daniel Federico Quesada Monge

RESUMEN

En la actualidad, el análisis sobre las ciudades inteligentes se podría describir como tecnocentrista. Es decir, se encuentra mayoritariamente enfocado desde la perspectiva y beneficios tecnológicos, olvidando el factor humano y la injerencia que tiene una ciudad inteligente en el ámbito de la privacidad y la protección de datos de carácter personal de sus ciudadanos. Este artículo se plantea como reflexión sobre algunas de las obligaciones de las ciudades inteligentes a la luz del

Reglamento General de Protección de Datos, como parámetro y garantía de dicho derecho.

Palabras Clave: ciudades inteligentes, protección de datos de carácter personal, privacidad, Reglamento General de Protección de Datos, consentimiento, tratamiento de datos, ciberseguridad, privacy by design, principio de transparencia, seudonimización de datos de carácter personal, derechos y libertades fundamentales.

ABSTRACTt

As of today, smart cities analysis can be described as technocentrist, meaning that it is primarily focused on the technology perspective and its benefits, forgetting the human factor in a smart city and the interference of technologies in the privacy and data protection of the citizens. This paper aims to provide a thought on the obligations that smart cities have under the General Data Protection Regulation as a parameter of effective data protection.

Keywords: smart cities, data protection, privacy, General Data Protection Regulation, consent, data processing, cybersecurity, privacy by design, transparency, pseudonumisation, fundamental rights and freedoms.

EN PROSPECTIVA

Sobre la necesidad de ser más rápidos

Por Xavier Alamán Roldán

La encuesta #12 Reglamento e-privacy

Entrevista a Enrique Castellón

En Red nº 12

Número 11

CARTA DEL DIRECTOR

Por Pablo García Mexía

Tribuna de honor

China y la revolución digital. China and the digital revolution.

Por Eugenio Bregolat Obiols

"Neutralidad de la Red: cambio y corto." "Net Neutrality: over and out."

Por Ofelia Tejerina Rodríguez.

RESUMEN

Tras años de debate, desde la aparición de Internet hasta 2016, cuando Europa y Estados Unidos recorrían caminos de similar sentido en la regulación de la neutralidad de la red, la llegada de Donald TRUMP a la Casa Blanca, junto con las primeras pruebas de la tecnología 5G, han supuesto un "cambio y corto" en los acontecimientos. Los principios básicos de no discriminación, no bloqueo, no priorización por pago, transparencia, no interferencia injustificada y no ralentización, se han puesto en tela de juicio frente a las posibilidades de esta nueva tecnología, según parece,

para reinterpretar ese tradicional objetivo de la gestión razonable del tráfico de la red, de utilización eficiente de los recursos optimizando la calidad global de las transmisiones.

PALABRAS CLAVE: neutralidad, Internet, discriminación, regulación, transparencia.

ABSTRACT

After years debating, from the appearance of the Internet until 2016, when Europe and the United States followed similar lanes regulating the net neutrality, the arrival of Donald Trump to the White House, and the first 5G technology experiments, they have supposed a “over and out” in the circumstances. The basic principles: non-discrimination, blocking, no prioritization by payment, transparency, unfair interference and no throttling, have been questioned against the possibilities of this new technology, as it seems to be, to reinterpret the traditional objective of the network traffic management, the efficient use of resources optimizing the overall quality of transmissions.

KEY WORDS: neutrality, Internet, discrimination, regulation, transparency.

Fake news, monopolios y democracia. Cómo controlar el poder de GAFA Fake news, antitrust and democracy. How to control the power of GAFA.

Por Paloma Llana González

RESUMEN

Los GAFA (acrónimo Google, Apple, Facebook y Amazon) han aumentado su poder como monopolios convirtiéndose, para algunos, en obstáculos para la innovación al abusar de su

posición de dominio en el mercado bien comprando a la competencia, bien anulándola. No solo eso; la concentración del mercado en pocos prestadores que recaban millones de datos, junto con el uso intensivo que de los mismos hacen, supone un riesgo para la intimidad de los ciudadanos y para su desarrollo personal pleno. El diseño de algoritmos para analizar a los usuarios y servirles la publicidad personalizada a su carácter, ha sido explotado con la finalidad de ofrecer informaciones, en muchos casos falsas, como parte de campañas de desinformación en procesos electorales tan trascendentes como el Brexit o la elección del presidente de los EEUU. Diversos sectores sociales han comenzado a solicitar a la administración estadounidense un cambio de rumbo mediante la aplicación, entre otras, de estrictas reglas anti monopolio a estas entidades, de responsabilidades por los contenidos que curan y ofrecen de manera individualizada, todo ello con la finalidad de preservar la competencia, la innovación y el acceso universal justo y abierto a los servicios de internet.

Palabras clave: GAFA, Privacidad, Competencia, Antitrust, fake news, filtro burbuja, responsabilidad por contenidos, innovación.

ABSTRACT

The GAFA (acronym Google, Apple, Facebook and Amazon) have increased their power becoming monopolies that abuse of their position of dominance, being an obstacle to innovation by buying the competitors or blocking their growth. Further, they are in an unique position to collect millions of data as the internet market is concentrated in their hands. This poses a risk for the privacy of the citizens and for their full personal

development. The algorithms designed in principle to analyse users' behaviour in order to serve them personalized advertising, have been perverted to disseminate information, in many cases false, as part of disinformation campaigns in electoral processes as important as the Brexit or the US Presidential elections. Stakeholders (consumers, think tanks, etc...) have requested a change of direction from the US administration in order to preserve competition, innovation, and fair and open universal access to internet services. They ask for a strict application of anti-trust rules to GAFA, making them, all the way, accountable for the information they cure and serve.

Key Words: GAFA, Privacy, Competition, Antitrust, Fake news, Bubble filter, Content Accountability. Innovation.

La amenaza tecnológica en los procesos electorales. Una respuesta jurídica. The threat of technology in the electoral process: A legal response

Por Rafael Rubio Núñez

RESUMEN

El proceso electoral está siendo objeto de diferentes ataques a lo largo del mundo. Estos ataques, de base tecnológica, seroducen en momentos del proceso como la inscripción en el registro, la conformación de candidaturas, la campaña electoral, la votación o el recuento y buscan incidir en las votaciones, alterar los resultados y generar incertidumbre y desconfianza. La novedad del problema requiere nuevas respuestas en el plano de la seguridad y la defensa, la educación, la cooperación entre distintos actores que forman parte del proceso, nacional e internacional, y el derecho. La

respuesta jurídica, escasa hasta el momento, deberá afrontar los cambios que se están produciendo en el proceso electoral en los canales, los actores, los contenidos, los tiempos y la protección de los datos de carácter personal.

Palabras claves: Elecciones, campañas electorales, tecnología, ciberataques.

ABSTRACT

The electoral process is currently under attack across the world. These technology- based attacks come about at particular moments in the process, such as registration in the electoral register, the election of candidates, the electoral campaign, voting and recounts, and they find a way to interfere in votes, alter results and generate incertitude and mistrust. The fact that the problem is so new and unparalleled means that new responses are needed in security and defense, education, cooperation between different actors that form part of the national and international process, and in the law. The legal response, which up until now has been scarce, needs to confront the changes that are arising in the channels, actors, content, timeframe and personal data protection, of the electoral process.

Keywords: Elections, electoral campaigns, technology, Cyberattacks

La Protección de Datos Personales y el caso Facebook: una cuestión transnacional. Data protection and the Facebook case: a transnational issue.

Por Diego López Garrido

EN PROSPECTIVA

Internet y jurisdicción: cómo ejercitar nuestros derechos en un mundo global.

Por Jorge Rodríguez-Zapata Pérez

La encuesta #11 Blockchain y privacidad

Entrevista a Alex Preukschat

En Red nº 11

Número 10

CARTA DEL DIRECTOR

Por Pablo García Mexía

Incibe como entidad de referencia para el desarrollo de la ciberseguridad en España

Por Alberto Hernández

Robótica, inteligencia artificial y derecho

Robotics, artificial intelligence and law

Por Rafael de Asís Roig

RESUMEN

La proyección de la Inteligencia Artificial y la Robótica en el Derecho es un hecho. Este trabajo examina algunos de los retos que esa proyección plantea tanto en el campo de la metodología de los operadores jurídicos cuanto en el campo de la regulación de la responsabilidad. En el campo de la metodología se proponen algunos rasgos comunes del

razonamiento jurídico, que deben ser respetados por los sistemas de Inteligencia Artificial. En el campo de la responsabilidad se da cuenta de las distintas fórmulas propuestas para regular la presencia de los robots en la sociedad. El trabajo termina haciendo referencia a los principios que deben guiar la proyección de la Inteligencia Artificial y la Robótica en el Derecho.

Palabras Clave: Inteligencia Artificial, Robótica, Argumentación Jurídica, Responsabilidad, Derechos Humanos

ABSTRACT

The projection of Artificial Intelligence and Robotics in the Law is a fact. This paper examines some of the challenges that this projection poses both in the field of the methodology of legal operators and in the field of regulation of responsibility. In the field of methodology, some common features of legal reasoning are proposed, which must be respected by Artificial Intelligence systems. In the field of responsibility, account is given of the different formulas proposed to regulate the presence of robots in society. The paper ends with a reference to the principles that should guide the projection of Artificial Intelligence and Robotics in the Law.

Keywords: Artificial Intelligence, Robotics, Legal Argumentation, Responsibility, Human Rights

Implicación de los trabajadores en el desarrollo de la creación de la marca digital de la empresa: la cesión de gestión de perfiles en redes sociales.

Participation of the employers in the company's digital brand development: assignment of the social media profile management.

Por M^a Isabel Carmona González, y Eva Sánchez Polidoro

RESUMEN

Las estrategias de posicionamiento de la marca y desarrollo de la reputación online de las empresas inciden de forma relevante en el ámbito de las relaciones laborales especialmente cuando integran directamente a los empleados en ellas para convertirlos en “embajadores de la marca”. Últimamente está aumentando la celebración de acuerdos en virtud de los cuales los trabajadores le ceden a su empresa la gestión de su cuenta personal en redes sociales para que aquella utilice dicha cuenta en el marco de su estrategia de marketing social. Este tipo de acuerdos presenta una serie de importantes consecuencias jurídicas que deben ser cuidadosamente consideradas ya que afectan significativamente, entre otros, al ámbito de los derechos fundamentales del trabajador y su privacidad.

Palabras clave: “Redes sociales” “trabajadores” “cesión” “derechos fundamentales” “privacidad”

ABSTRACT

Companies are carrying out brand positioning and online reputation strategies which affect, in a relevant way, their relations with their employees specially when the employees collaborate directly with these strategies and become “brand ambassadors”. Lately it is growing the number of agreements by which the employees sign over their personal accounts in social networks to the Company to be included in the company

social media and marketing strategy. This kind of agreements face important legal effects that have to be considered carefully given that they concern, among others, fundamental rights of the employees as well as their privacy.

Keywords: "social network" "employees" "assignment" "fundamental rights" "privacy"

La regulación de las plataformas colaborativas **The regulation of the sharing economy**

Por Juan José Montero Pascual

RESUMEN

La regulación de la economía colaborativa debe construirse a partir del reconocimiento de un nuevo modelo de organización industrial: los mercados multilaterales en los que una plataforma electrónica hace posible la interacción de prestadores de servicios y usuarios de los mismos. Las plataformas no tienen vocación de prestar los servicios subyacentes. Por el contrario, las plataformas prestan servicios de mediación o corretaje, aunque de gran valor añadido, ya que crean una oferta estructurada en red a partir de los servicios de prestadores individuales y fragmentados. La regulación, reconociendo este punto de partida, puede hacer frente a retos como el poder de mercado de las plataformas, las potencialmente desequilibradas relaciones entre plataformas y prestadores de servicios, la protección de los consumidores, etc.

Palabras clave: economía colaborativa, plataforma, mercados multilaterales, Uber

ABSTRACT

The regulation of the sharing economy has to acknowledge a new model of industry organization: multilateral markets in which an electronic platform makes possible the interaction between service providers and users. Electronic platforms have no ambition to provide the underlying services. On the contrary, they merely intermediate between third parties, but such intermediation offers a lot of added value, as it creates a new offer with a network structure from a pool of previously isolated and fragmented service providers. If regulation acknowledges this reality, it can meet challenges such as the market power of the platforms, unbalanced relationships between service providers and the platforms, as well as between consumers and platforms, etc.

Keywords: sharing economy, platform, multisided markets, Uber

La gobernanza de internet

Internet governance

Por Moisés Barrio Andrés

RESUMEN

Las singularidades del entramado institucional de Internet aparecen ya señaladas en la propia denominación, que se refiere a la «gobernanza» y no al «gobierno» de la Red. En este artículo se analizan la naturaleza, caracteres y tipología de la estructura orgánica que rige el ciberespacio, así como sus problemas e insuficiencias, ya que está siguiendo una evolución cuyos perfiles no acaban de fraguar pacíficamente. Además, el proceso de reforma de la ICANN culminado en 2016-2017 se ha traducido en el establecimiento de unos

objetivos y unos valores esenciales y en la constitución de una estructura orgánica que responden al modelo de organización multipolar o multistakeholder con escasa representación de los Estados-nación, lo cual parece estar dando origen a una república de la Red por medio de una fragmentación o balcanización de Internet.

Palabras clave: gobernanza de Internet, ICANN, IANA, Cumbre Mundial de la Sociedad de la Información, Foro para la Gobernanza de Internet.

ABSTRACT

The uniqueness of the institutional structure of the Internet is already indicated in the name itself, which refers to “governance” and not “government” of the Net. This paper analyzes the very nature, characteristics and typology of the organic structure that governs the cyberspace, as well as its problems and inadequacies, since it’s following an evolution whose profiles haven’t been yet established peacefully. In addition, the ICANN reform process completed in 2016-2017 has resulted in the establishment of essential objectives and values and the constitution of an organizational structure that respond to the multipolar or multistakeholder organizational model with low representation of nation-states, which seems to be giving rise to a republic of the Net through fragmentation or balkanization of the Internet.

Keywords: Internet governance, ICANN, IANA, World Summit on the Information Society, Internet Governance Forum.

EN PROSPECTIVA

Los datos personales. ¿Una propiedad o un derecho fundamental?

Por Paula Ortiz López

La encuesta #10 plataformas tecnológicas y derechos Laborales

Entrevista a Ignacio Astarloa Huarte-Mendicoa

En Red nº 10

Número 9

CARTA DEL DIRECTOR

Por Pablo García Mexía

¿Qué implica ser liberal progresista en la era digital?

Por Vicente Ten

“Tecnología y nuevo derecho: autorregulación regulada y soft law. A propósito del reglamento europeo de protección de datos”

Por José López Calvo

RESUMEN

Las nuevas tecnologías, en especial Internet, han sometido a un test de stress al sólido Estado de Derecho tradicional que contempla la eclosión de nuevas técnicas como autorregulación y soft law. La autorregulación emplaza a la intermediación de normas y controles privados que poseen relevancia para el Derecho público. En el soft law los poderes

públicos ejercen en plenitud su capacidad normativa, pero incapaces de descender al grado de especificidad exigible se refugian en la tautología, en conceptos jurídicos indeterminados y en flexibilidad y abstracción El Reglamento Europeo de Protección de Datos, llamado a regular la privacidad en Internet, es un claro exponente de la utilización de tales figuras. Este artículo analiza los principales supuestos y ejemplos

PALABRAS CLAVE: autorregulación, soft law, internet, Reglamento de Protección de Datos

ABSTRACT

The new technologies, especially Internet, have submitted to a test of stress to the solid and traditional rule of law, who must contemplate the emergence of new techniques such as self-regulation and soft law Self-regulation reaches private norms and controls that are relevant to public law. In the soft law, public powers fully exercise their normative capacity, but unable to fall to the degree of enforceable specificity they take refuge in the tautology, in undetermined juridical concepts and in flexibility and abstraction The European Regulation on Data Protection, called to regulate privacy on the Internet, is a clear example of the use of such figures. This article analyzes the main cases and examples.

KEY WORDS: self regulation, soft law, internet, General Data Protection Regulation

Los efectos del bloqueo geográfico sobre el bienestar económico

Por Joaquín Blanco García-Lomas

RESUMEN

La Comisión Europea, en el marco del Mercado Único Digital, se ha marcado como uno de sus principales objetivos la reducción del bloqueo geográfico. La estrategia comercial de segmentación el mercado europeo en función de la nacionalidad o del lugar de residencia de los consumidores llevada a cabo por parte de muchas empresas con presencia online, tiene un impacto negativo sobre el bienestar agregado de la sociedad. Un reducido acceso transfronterizo a los bienes y a los servicios de otros países, una disponibilidad de los contenidos todavía limitada en algunos sectores, y una discriminación de precios en función del lugar de residencia explican que las medidas legislativas orientadas a reducir el bloqueo geográfico pueden tener efectos positivos sobre el bienestar de los ciudadanos europeos.

Palabras clave: Bloqueo geográfico; Discriminación de precios; Mercado Único Digital; Efectos sobre el bienestar.

ABSTRACT

The European Commission, within the Digital Single Market strategy, includes the reduction of geo-blocking as one of the main aims to tackle. The commercial strategy of segmentation of the European market based on nationality or place of residence carried out by many companies with online presence, has a negative impact on society. A reduced cross-border access to goods and services from other countries, a limited availability of contents in some sectors, and a price differentiation by place of residence explains that legislative

measures aimed at reducing the geographical geo-blocking may have positive effects on the welfare of European citizens.

Keywords: Geo-blocking; Price discrimination; Digital Market Union; Welfare effects.

Contratación pública electrónica como medicina a la corrupción

Por Sergio Alberto Martin Esquivel

RESUMEN

La economía de los países ha obligado a diversificar los esquemas de contratación de bienes, servicios y proyectos de infraestructura, hacer más con menos y hacer uso de estrategias e innovación, mejorar sustancialmente los márgenes y reducir costos, la creciente transformación tecnológica y el trabajo de estándares a nivel internacional han transformado la Contratación Pública convencional y se requiere implementar tanto tecnologías como procesos innovadores. En todos los países la capacidad de contratación de los Gobiernos es la más importante, es por ello, que la Contratación Pública es atractiva para las empresas nacionales e internacionales, e inclusive, muchas de ellas dependen prácticamente de sus ventas a Gobierno, por lo que, la Contratación Pública no sólo es el conducto para conseguir en una parte el cumplimiento de políticas públicas y programas sociales, sino que también, puede ser el mecanismo de desarrollo a micro, pequeñas y medianas empresas. Podemos ilusionarnos con pensar que puede ser real una Administración Pública Electrónica, porque la globalización está marcando una tendencia muy importante en el uso y crecimiento de las tecnologías de la información y comunicación. También es

válido pensar que la tecnología puede ser clave para resolver uno de los males más devastadores, como es la corrupción en la Contratación Pública a través de herramientas que cierren paso a la discrecionalidad e incrementen transparencia.

ABSTRACT

The economy of the countries has forced to diversify the schemes of contracting goods, services and infrastructure projects, doing more with less and making use of strategies and innovation, substantially improving margins and reducing costs, the growing technological transformation and the work of International standards have transformed conventional Public Contracting and it is required to implement both technologies and innovative processes. In all countries the contracting capacity of the governments is the most important, which is why Public Procurement is attractive for national and international companies, and even many of them depend almost on their sales to the Government, which is why, Public Contracting is not only the conduit to achieve compliance with public policies and social programs, but also, it can be the development mechanism for micro, small and medium enterprises. We can delude ourselves with thinking that an Electronic Public Administration can be real, because globalization is marking a very important trend in the use and growth of information and communication technologies. It is also valid to think that technology can be key to solving one of the most devastating evils, such as corruption in Public Procurement through tools that close the way to discretion and increase transparency.

Keywords: Corruption, Public Contracting, Electronics, Transparency, Innovation

Palabras clave: Corrupción, Contratación Pública, Electrónica, Transparencia, Innovación.

Redes y servicios 5g: tecnología, negocio y regulación.

Por Arturo Azcorra e Ignacio Berberana

RESUMEN

La nueva generación de comunicaciones móviles 5G, que está en proceso de estandarización, supone un cambio radical no solo en los aspectos tecnológicos, sino también en la forma en la que se proveerán los servicios (de forma más personalizada) y en quienes los utilizarán (no solo los consumidores, sino también sectores verticales de la industria). En el artículo se repasan las principales características tecnológicas y casos de uso de las futuras redes 5G, así como aspectos relacionados con su despliegue y regulación. También se revisan las principales iniciativas de I+D+i para el desarrollo de las tecnologías que sustentan 5G, fundamentalmente en Europa, así como los instrumentos que se pueden emplear en el contexto de España para fomentar el desarrollo y adopción del 5G en nuestro país.

Palabras clave: 5G, Tecnologías de la Información y las Comunicaciones, Computación de Proximidad, espectro radioeléctrico, casos de uso, virtualización de red.

ABSTRACT

The new generation of 5G mobile communications, which is in the process of standardization, is a radical change not only in the technological aspects, but also in the way in which the services will be provided (in a more personalized way) and in those who will use them (not only consumers, but also vertical

sectors of the industry). The article reviews the main technological characteristics and use cases of future 5G networks, as well as aspects related to their deployment and regulation. It also reviews the main R & D & I initiatives for the development of the technologies that support 5G, mainly in Europe, as well as the instruments that can be used in the context of Spain to promote the development and adoption of 5G in our country.

Key words: 5G, Information and Communication Technologies, Proximity Computing, radioelectric spectrum, use cases, network virtualization.

EN PROSPECTIVA

Data Privacy in the United Kingdom after Brexit

Por Mark Lubbock

La encuesta #9 bloqueo geográfico digital

Entrevista a Tomás de la Quadra – Salcedo.

En Red nº 9

Año 2017

Número 8

CARTA DEL DIRECTOR

Por Pablo García Mexía

La transformación digital de los servicios financieros una nueva etapa del desarrollo humano

Fátima Cerdán

The Internet of Trust

José Gefaell

ABSTRAC

The contention of this paper is that FinTech Apps combined with the Distributed Ledger Technology (DLT, also called Blockchain) will be the great disruptors of the banking industry and the whole economy, catalysing the development of a new revolution, the Internet of Value, that we propose to call the "Internet of Trust", fuelling the creation of a truly new economy, where reputed and innovative institutions will enjoy a more efficient financing directly from the investors and savers. This paper will focus on one concrete application of these technologies for the banks: an app for the radical self-disintermediation of plain vanilla corporate and institutional lending and bonds, for the benefit of the banks' clients; the radical disintermediation of the simple for the benefit of the issuers and savers, in order to enhance these clients' loyalty in the banks' intermediation of the complex. The aim is to put the clients at the center of the banking industry again, giving them a private communication app that will allow them to "privately" communicate with the institutional issuers and eventually subscribe their private debt issues without a bank as an intermediary. The main sources of this paper have been: (1) the author's developments on the subject; (2) the World Economic Forum research, summarised in two presentations: "The future

of financial infrastructure" (i) and "A Blueprint for Digital Identity" (ii), whose conclusions are partially included here (under per - mission); and (3) Don Tapscott and Alex Tapscott book "Blockchain Revolu - tion: How the Technology Behind Bitcoin Is Changing Money, Business, and the World".

La protección de la propiedad intelectual en el derecho espa- ñol. Obra arquitectónica y libertad de panorama.

Santiago González-Varas. Lorena Rivera Novillo

RESUMEN

Los derechos autor en el entorno del urbanismo han supuesto una fuente constante de dudas y conflictos, que además, en los últimos años, se han vis - to multiplicados por la evolución creciente de las nuevas tecnologías. A tra - vés de este estudio se analizan, de forma general pero a su vez, exhaustiva, los derechos de autor, repasando los principios jurídicos de estos derechos, considerando, entre otros, el derecho al reconocimiento de la autoría, los derechos morales y los derechos de explotación, a través de la exposición de los casos más relevantes en materia de propiedad intelectual relacionada con urbanismo. Sobre esa base, se analiza en más detalle y con más pro - fundidad el llamado derecho de panorama o excepción de panorama en el ámbito de la Unión Europea y el debate actual respecto al mismo, que ha ido cobrando relevancia a consecuencia del desarrollo digital que se está produciendo, el cuál conlleva un nuevo escenario en el deben desarrollarse los derechos de autor.

Palabras clave: derechos de autor, propiedad intelectual, libertad de panorama, urbanismo, derecho comparado europeo.

ABSTRACT

The copyrights in connection with the urbanistic environment has always been source of doubts and conflicts, which has been increased in the last few years due to the evolution of the new technologies. This report analyses copyrights both generally and in depth, reviewing the general judicial principles of those rights. The report considers, among other, the authorship recognition right, the moral rights and the commercialization rights, by means of an analysis of the key cases on intellectual property regarding urbanism. In this regard, the report analyses in depth the so-called freedom of panorama or panorama exception within the European Union, as well as the different opinions arising therefrom. Such debate is becoming a key issue nowadays, due to the digital development that entails a new scenario for the copyrights development.

Key words: copyrights, intellectual property, freedom of panorama, urbanism, european comparative law.

La transformación digital entre las empresas españolas

Alberto Urueña López

RESUMEN

En el presente texto se aborda la situación de la transformación digital entre las empresas españolas. Con este fin se revisan diferentes modelos destinados al análisis de la situación del proceso de transformación derivado de la incorporación de las TIC. Como resultado de esta revisión se propone un análisis basado tanto en la penetración de las TIC en las empresas

español - las. En las siguientes páginas se podrá observar como la incorporación de servicios y tecnologías digitales va en aumento, sin embargo, su penetración dependerá tanto del tipo de tecnología como de las características de las empresas, siendo más difícil la adopción cuando la empresa es de menor tamaño y la tecnología es más reciente.

Palabras clave: Tecnologías de la Información, empresas, indicadores, transformación digital, internet.

ABSTRACT

This paper addresses the situation of digital transformation among Spanish companies. To this end, different models for the analysis of the situation of the transformation process derived from the incorporation of ICT are reviewed. As a result of this review we propose an analysis based on the penetration of ICT in Spanish companies. In the following pages you can see how the incorporation of digital services and technologies is increasing, however, its penetration will depend on both the type of technology and the characteristics of the companies, being more difficult the adoption when the company is smaller and technology is more recent.

Keywords: Information technologies, companies, indicators, digital transformation, internet.

¿Hacia un Impuesto sobre Actos Jurídicos Digitales?

José A. Rozas.

RESUMEN

La digitalización de la economía suele afrontarse por las Administraciones tributarias -desde las iniciativas promovidas por la OCDE - más bien como una oportunidad para eludir o

evadir el pago de impuestos. Sin embargo, la tecnología de las comunicaciones constituye, también, la ocasión para, a par - tir de las oportunidades de tratamiento y acceso a la información que posibi - lita, reformular los sistemas impositivos domésticos -tanto en sus aspectos sustantivos como aplicativos- de forma más eficiente y equitativa. Este reto adquiere especial intensidad cuando desde el Derecho tributario se conside - ra el tratamiento de la llamada economía colaborativa.

Palabras clave: Impuesto digital; Economía colaborativa; Economía digital; Im - puestos de registro.

ABSTRACT

The digitization of the economy is usually faced by tax administrations - from the initiatives promoted by the OECD - and, therefore, in the tax literature generated by them, rather as an opportunity to tax avoidance or tax evasion. However, TIC is also the opportunity to reformulate domestic taxation sys - tems - both its structure and theirs procedures - in a more efficient and fair way, based on the opportunities for treatment and access to the information that is available. This challenge acquires special intensity when we observe the so-called collaborative economy, which uses digital connection systems as a vehicle for arranging transactions of goods and services between individuals. In this work, a germinal reflection is pointed out, based on the analysis of the challenges that a specific manifestation of this sharing economy, Wallapop, a digital platform that uses the possibilities offered by digital technology to put in contact people interested in buying and/or sell goods and services in an flexible, casual, informal and, neighborhood's environments. In a first approach, it is clear the

decadent structure of the transfer taxes on movable properties sales between consumers; at the same time, the digital registration of this civil contracts offers an excellent opportunity for a simple digital duty which could perfectly fit into the framework of the inveterate stamp duties, today on legal documents.

Keywords: Digital Tax; Collaborative Economy; Digital Economy; Stamp Duties.

EN PERSPECTIVA

Desafíos regulatorios de un mercado emergente

Fabio de Pascua Fintech

LA ENCUESTA.

Nº 8. Fintech

La Entrevista

Rodrigo García de la Cruz

En Red N. 8

Legal en red

Número 7

CARTA DEL DIRECTOR

Por Pablo García Mexía

La era digital, una nueva etapa del desarrollo humano

Josep Borell Fontelles

El proceso de reforma de la ICANN: objetivos, régimen jurídico y estructura orgánica

Margarita Robles Carrillo

RESUMEN

La reforma de la ICANN, culminada en 2016, se ha realizado con el doble propósito de proceder a la internacionalización y la privatización de la gobernanza técnica de Internet. El estudio del proceso de transición se inicia considerando los condicionantes históricos, funcionales, internos y exteriores que alimentan dicho proceso. Sobre esa base, el análisis de la articulación jurídica de la ICANN atiende a sus objetivos, obligaciones, valores esenciales

y principios. La estructura orgánica se explica centrándose en sus componentes principales que son los órganos básicos-mpowered Community, Junta Directiva y Comité de nominaciones-, las Organizaciones de Apoyo y los Comités Asesores. Las conclusiones están dedicadas a evaluar el alcance y las consecuencias de los objetivos de la reforma.

Palabras clave: ICANN, proceso, normativa, estructura.

ABSTRAC

The reform of ICANN, in 2016, has been carried out with the dual purpose of internationalizing and privatizing the technical governance of the Internet. The study of the transition process begins by considering the historical, functional, internal and external conditions of the process. The analysis of legal articulation addresses the objectives, commitments, core values and principles of ICANN. The organizational structure is

explained by focusing on its core components -Empowered Community, Board of Directors and Nominating Committee-, Supporting Organizations and Advisory Committees. The conclusions are devoted to assess the scope and consequences of the reform.

Keywords: ICANN, process, norms, structure.

Los derechos de los contribuyentes en un entorno digital

Marina Serrat Romaní

RESUMEN

El presente trabajo se destina a analizar el entorno social y jurídico que rodea las políticas de transparencia, concretamente las de transparencia fiscal, cuya firme apuesta como el mecanismo de mayor impacto para reducir el fraude y la evasión se acordó desde el año 2009. El impacto de estas políticas se plasma, en mayor medida, en los modelos de intercambio de información, cuyas modificaciones en el estándar para pasar de un intercambio previo requerimiento a un intercambio automático de información se han empezado a aplicar recientemente. El objeto del análisis de estas medidas pretende conocer cuál es el impacto que pueden tener sobre los derechos y garantías de los contribuyentes y cuáles son los potenciales riesgos a los que puede conducir, ya que se trata de medidas de lucha contra el fraude adoptadas en y para un entorno digitalizado, que también ha influido en su desarrollo y puesta en marcha.

Palabras clave: Transparencia – Intercambio de datos – Acceso a los datos – Derechos de los contribuyentes – Dataísmo

ABSTRACT

This article is destined to analyze the social and juridical environment surrounding the transparency policies, specifically those related to fiscal transparency whose clear commitment as the most efficient mechanism to face and reduce tax fraud and tax evasion was agreed since 2009. The impact of those policies is mainly embodied in the models of exchange of information.

The recent modifications of the standard of transparency to transfer from an exchange upon request to an automatic exchange of information started recently to be applied. Thus, the object behind the analysis of those measures aims to know which is the impact that those provisions might have on the rights and guarantees of the taxpayers and which are the potential risks they might lead to. Since, it has not to be forgotten that the measures to face the fraud and evasion that are being adopted, they have designed for a digitalized environment and also that influenced their development and setting up.

Key words: Transparency – Exchange of information – Access to data – Rights of the Taxpayers – Dataism.

¿Hemos sido suficientemente ambiciosos con la reforma de la LECrim para dar respuesta eficaz al cibercrimen?

Estudio del nuevo fenómeno que supone la ciberdelincuencia y su investigación

Ana Rosa Flores Martín

RESUMEN

Desde que apareció Internet, la sociedad ha cambiado. Ha aparecido un nuevo fenómeno: la ciberdelincuencia. Cada vez

se cometen más delitos a través de Internet. La solución para hacer frente a esta nueva forma de cometer delitos es difícil: los países no se ponen de acuerdo. Hasta la reforma de la ley, los investigadores no eran capaces de responder ante este fenómeno. Con la LO 13/2015 se han introducido nuevas medidas de investigación que permitirán una mayor eficacia en la persecución de este tipo de delincuencia. Palabras clave: ciberdelincuencia, ciberdelitos, ciberespacio, investigación, Internet.

ABSTRACT

Since the Internet appeared, society has changed. A new phenomenon has appeared: cybercrime. More and more crimes are committed through the Internet everyday. The solution to this new way of committing crimes is difficult: the countries do not agree. Until the reform of the law, researchers were not able to answer to this phenomenon. With the organic law 13/2015 new research measures have been introduced that will allow a greater efficiency in the pursuit of this type of crime.

Keywords: cybercrime, cyberspace, investigate, Internet.

Normalización de la seguridad de las tecnologías de la información

Miguel Bañón y José Antonio Rubio

LA ENCUESTA.

Nº 7. Inteligencia Artificial

La Entrevista

Pilar del Castillo

En Red N. 7
Legal en red

Número 6

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

La Ciberseguridad ha venido para quedarse

Por Carlos Enrique Gómez López de Medina

Privacidad e Internet de las cosas (Internet of things, IoT)

Por Wilma Arellano Toledo

RESUMEN

Numerosos son los impactos y novedades que ha traído consigo la aparición y evolución de las TIC (Tecnologías de la Información y la Comunicación) y, el Internet de las cosas o de los objetos (IoT por sus siglas en inglés, Internet of Things), es una de ellas y ha implicado un enorme avance en el mundo de la tecnología. Y, como todos los fenómenos asociados a las TIC, el IoT plantea serios retos en materia de regulación y legislación sobre su uso y conectividad (que va más allá del ámbito de las tecnologías de la información y llega al terreno de otras industrias y servicios), incluidos todos aquellos aspectos que su existencia implica y que pueden vulnerar

derechos fundamentales como el de la privacidad. En este trabajo abordaremos esos retos, a través del análisis de la Comunicación de la Comisión Europea sobre Internet de las Cosas, el Dictamen del Comité Económico y Social sobre el mismo tema, la Declaración de Mauricio al respecto de la privacidad e IoT, así como otros diversos documentos y estudios doctrinales, para intentar sopesar su alcance. PALABRAS CLAVE: Internet of Things, Internet de las Cosas, privacidad, protección de datos personales.

KEYWORDS: Internet of Things, privacy, personal data protection

¿Cómo afectan las obligaciones de protección de datos personales al bienestar social?

Por Fernando Herrera-González

RESUMEN

En los últimos años se ha facilitado considerablemente la recogida, almacenamiento y proceso de datos. Si se encontrara valor en los datos personales, se incrementaría el bienestar social. Para que un recurso se pueda valorar, se requiere la actividad del emprendedor, dando lugar a un proceso de prueba y error que puede ser dificultado por la regulación. En la Unión Europea, las diversas normas imponen limitaciones a la explotación de los datos personales, que se pueden resumir en los derechos ARCO: acceso, rectificación, cancelación y oposición. En este artículo, se analizan las consecuencias de los derechos ARCO en la actividad emprendedora, y por tanto en el valor que podría obtenerse de los datos personales, y en suma en el bienestar social.

Palabras Clave: Datos personales, regulación, eficiencia, derechos ARCO, emprendimiento.

ABSTRACT

In recent years, collection, storage and processing of data have become easier. If some value were found in personal data, this value would increase social welfare. In order for the value of an asset to be appraised, entrepreneurial activity is required, in a process of trial and error which may be hindered by regulation. In the European Union, the normative puts limits to the exploitation of personal data, which may be synthetized around the so-called ARCO rights: access, rectification, cancellation and objection. In this paper, the consequences of the ARCO rights on entrepreneurial activity are analysed, and thus on the value that may be accrued from persona data, and, in sum, on social welfare.

Key Words: Personal Data, regulation, efficiency, ARCO rights, entrepreneurship.

Los riesgos de los datos personales en un entorno cloud computing: Una aproximación desde el Reglamento Europeo de Protección de Datos

Juanita Pedraza Córdoba

RESUMEN

En este artículo se analizan las características de las técnicas de cloud computing que pueden redundar en la generación de riesgos para la protección de los datos personales. La identificación de tales riesgos, así como el análisis de los mecanismos jurídicos previstos en el nuevo Reglamento Europeo de Protección de Datos Personales (Reglamento (UE)

2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016) para solventarlos, constituye el núcleo central del trabajo, que concluye con un examen del principio de responsabilidad proactiva como piedra angular del nuevo sistema de protección de los datos personales.

Palabras clave: cloud computing, protección de datos personales, Reglamento Europeo para la protección de datos personales, responsabilidad proactiva.

ABSTRACT

In this article, I identify the privacy risks that are associated with cloud computing and I review the legal measure to solve this risks at the light of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 to conclude with some legal considerations about the accountability principle like essential component of the protection of natural persons with regard to the processing of their personal data.

Keywords: cloud computing, personal data protection, General Data Protection Regulation, accountability principle.

La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo

Por Oreste Pollicino y Marco Bassini

La privacidad en la sociedad de la información

Por Miguel Pérez Subías

LA ENCUESTA.

Nº 7. Inteligencia Artificial

LA ENTREVISTA

Con Jorge Pérez, La privacidad en la sociedad de la información

EN RED

Legal en red La privacidad en la sociedad de la información

Año 2016

Número 5

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

El respeto a la privacidad de las comunicaciones, una asignatura pendiente en la España del siglo XX

Por Víctor Domingo.

ESTUDIOS

La ciberseguridad como legitimación para el tratamiento de direcciones IP.

Por Francisco Pérez Bes

RESUMEN

Este artículo analiza las novedades relacionadas con la excepción al consentimiento en el tratamiento de datos de carácter personal, en este caso direcciones IP, por parte de los CERTs dentro de sus labores relacionadas con la prevención,

reacción e investigación de incidentes de ciberseguridad. Todo ello a la luz de las últimas novedades legislativas (en particular, la Disposición Adicional 9ª de la LSSI y el recientemente publicado Reglamento Europeo sobre Protección de Datos) y del Informe emitido por la Agencia Española de Protección de Datos sobre la legitimación de los CERTs para dicho tratamiento.

Palabras clave: datos personales, direcciones IP, excepción al consentimiento, ciberseguridad, CERT/SCIRT.

ABSTRACT

This study focuses on the new regulations that rules the exception of consent for personal data treatment, in particular IP addresses, for SCIRTs during their duties of prevention, reaction and investigation of cybersecurity incidents. All that under the new regulations (in particular, the Additional Provision 9 of the LSSI and the recent European Regulation of Data Protection) and the report published by the Spanish Data Protection Agency regarding the legitimation of the SCIRTs for that treatment.

Keywords: personal data, IP addresses, exception to the consent, cybersecurity, CERT/SCIRT

Propuestas y retos en torno a la prueba electrónica a tenor de las últimas reformas procesales

Por Dr. Federico Bueno de Mata

RESUMEN

En el presente artículo se analiza la figura de la prueba electrónica a tenor de las reformas procesales producidas en el año 2015 en la LOPJ, LECiv y LECRim. Estamos ante un artículo propositivo en el que se pretende dar respuesta a una serie de cuestiones vinculadas a la prueba electrónica tales como su concepto, tipología y regulación. Se estudia igualmente el reconocimiento jurisprudencial de esta figura en los diferentes órdenes jurisdiccionales a través de comentarios a las sentencias más importantes de los últimos meses. De esta manera observaremos como la prueba electrónica es la figura clave para demostrar conflictos como la contratación electrónica, los ciberdelitos, los despidos por usar medios tecnológicos para uso personal en horario de trabajo o incluso conflictos entre portales electrónicos de servicios públicos y los propios administrados. El estudio aborda también una perspectiva práctica al proponer un protocolo para obtener evidencias electrónicas, a través del análisis del contenido que deberá poseer la autorización judicial en caso de vulnerar Derechos Fundamentales. Finalmente, estudiamos de qué maneras debemos proponer e incorporar dichas pruebas a un determinado proceso y se identifican los retos de futuro que la Administración de Justicia española deberá abordar en los próximos años para garantizar una justicia moderna, eficiente y cercana al ciudadano.

Palabras clave: Prueba electrónica, obtención, admisión, proposición, jurisprudencia

ABSTRACT

In this paper we analyze the figure of electronic evidence under the procedural reforms produced in 2015 in the most important civil, criminal and procedural laws organic level. We

are facing a propositional article that is meant to address a number of issues related to electronic evidence such as its concept, typology and regulation. Also, we study the jurisprudential recognition of this figure in the different jurisdictions through comments to the most important sentences in recent months. Thus, we observe how electronic evidence is the key to show conflict as e-procurement, cyber crime, layoffs by using technological means for personal use during working hours or even conflicts between electronic portals of public services and citizens. The study also addresses a practical perspective by proposing a protocol to obtain electronic evidence, through analysis of the content must have the judicial authorization in case of violating fundamental rights. Finally, we study the ways in which we propose and incorporate such evidence to a particular process and the future challenges that the Spanish Justice Administration must address in the coming years to be more modern, efficient and closer to the citizen.

Keywords: Electronic evidence, procurement, admission proposition, jurisprudence

El derecho de control de los datos personales en la plataforma de intermediación de la nueva EAdministración

Por M^a Paz Gil Durán

RESUMEN

El intercambio de datos entre las Administraciones públicas, hoy materializado a través de la denominada “plataforma de intermediación”, se ha tornado imprescindible a causa de la generalizada implantación de la Administración electrónica,

vigorosamente impulsada por las nuevas leyes administrativas de 2015. En este trabajo se analiza el funcionamiento de la plataforma de intermediación de datos desde un punto de vista jurídico y, estimando vulnerado el derecho de la ciudadanía al control de sus propios datos personales, que la jurisprudencia constitucional le reconoce, se proponen unas sencillas modificaciones tecnológicas que proporcionan las mínimas garantías jurídicas imprescindibles para la sumisión de las nuevas tecnologías al ordenamiento jurídico, antes de que el acelerado crecimiento de la plataforma escape de su control.

Palabras clave: Plataforma de intermediación de datos, protección de datos, cesión de datos, privacidad, intercambio de datos entre Administraciones.

ABSTRACT

Data exchange between public administrations, today materialized through the so-called "intermediation platform", has become imperative because of the widespread deployment of eGovernment, strongly driven by new administrative laws in 2015. This paper analyzes the behavior of the data intermediation platform from a legal point of view and, estimating violated the right of citizens to control their own personal data that the constitutional jurisprudence recognizes them, I suggest some simple technological modifications that provide the minimum essential legal guarantees required to submit the new technologies to the legal system, before the rapid growth of the platform become out of control.

Keywords: Data intermediation platform, data protection, data transfer, privacy, data exchange between public administrations.

VENTANA COMPARADA

La misma ley de siempre ante la nueva tecnología ¿es el derecho de autor la ley adecuada para regular la impresión en 3D?

Por Rodrigo Cetina Presuel

RESUMEN

La legislación del derecho de autor ha pasado de proteger solamente ciertos tipos de obras escritas, originalmente únicamente se protegía a los libros, a una lista de obras protegibles que parece crecer sin parar. Ahora también se protegen mapas, tablas, edificios, grabaciones audiovisuales o software. Además, con la aparición de las tecnologías digitales e Internet, se ha pasado de regular únicamente la reproducción de obras a ejercer el control sobre muchos tipos de actividades diferentes más allá del simple copiado. Justo ahora que entramos a la era del Internet de las cosas, el Big Data o macrodatos como se le llama en la Unión Europea, el minado de datos y la impresión en tres dimensiones, de nuevo debemos cuestionar qué papel debe de jugar el derecho de autor en el desarrollo de estas tecnologías. En particular, la impresión en 3D está borrando las líneas entre los archivos de ordenador y los objetos físicos, planteando así nuevos retos para el derecho de autor. Antes de apresurarse a aplicar la regulación existente a las actividades relacionadas con la impresión en tres dimensiones es necesario examinar qué problemas pueden surgir de dicha aplicación. Las interpretaciones restrictivas y los intentos de expansión de lo

que la ley protege podrían no ser el mejor camino debido a las características particulares de esta tecnología. Para evitar un daño a la innovación en una industria emergente, se hace necesario explorar otras opciones, incluso el considerar que no es una buena idea regular a la impresión 3D mediante el derecho de autor y considerar si la protección a través de las patentes no sería una mejor alternativa. Además, hay que tener en cuenta que intentar aplicar el derecho de autor a todo tipo de objeto físico, aún el impreso en tres dimensiones, podría tener consecuencias negativas para el dominio público y por lo tanto para los intereses de todos los usuarios en general.

Palabras clave: Impresión 3D, propiedad intelectual, derechos de autor, patentes, nuevas tecnologías.

EN PROSPECTIVA

Aplicación de la directiva 2014/26 de licencias multiterritoriales de música a la luz de la propuesta de reglamento de portabilidad transfronteriza de contenidos en línea: ¿cuál se aplicará antes en un mercado necesitado de cambios en materias de copyright?

Por Loreto Corredoira y Alfonso

LA ENCUESTA

Seguridad vs privacidad: Backdoors

Con la participación de Ofelia Tejerina Rodríguez, Javier Puyol y Pedro Pablo López Bernal.

LA ENTREVISTA

Con Rosa García Ontoso

EN RED

Normativa, Jurisprudencia y Publicaciones

Por Lorena Rivera Novillo

Año 2016

Número 4

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

De la homologación de las autoridades a la aplicación uniforme del reglamento

Por José Luis Rodríguez Álvarez.

ESTUDIOS

La universalidad en el nuevo reglamento general de protección de datos. El caso del derecho al olvido

Por Esther López Barrero

RESUMEN

El derecho a la supresión o derecho al olvido ha resultado una de las reformas más controvertidas del nuevo Reglamento

General de Protección de Datos de la Unión Europea (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016). En esencia, este derecho supone una actualización y adaptación a Internet del derecho a la cancelación de los datos, recogido ya en la Directiva 95/46/CE. El problema que suscita este derecho es doble. Por un lado, su propio contenido, puesto que no está bien definido en el artículo 17 del Reglamento. Por otro, la aplicación práctica que se le puede dar al mismo. En este sentido, de acuerdo con las normas sobre competencia judicial internacional y sobre determinación de la ley aplicable del nuevo Reglamento, dentro de la Unión Europea se puede reclamar judicialmente el cumplimiento de este derecho, incluso frente a operadores de Internet situados fuera de la UE. No obstante, puede resultar complicado el caso de tener que solicitar la ejecución de una sentencia por la que se reconoce este derecho en un tercer Estado extracomunitario, en especial si la solicitud de reconocimiento y ejecución se dirige a los Estados Unidos. La complicación deriva, no sólo porque la UE está siendo pionera en el reconocimiento legal de este derecho, sino también porque afloran a través de él las diferencias en la protección del bien jurídico “privacidad”, que es en última instancia lo que trata de proteger el derecho al olvido.

Palabras clave: Derecho al olvido, derecho a la supresión, extraterritorialidad, Reglamento General de Protección de Datos, competencia judicial internacional, ley aplicable, responsabilidad extracontractual, asunto Google España.

ABSTRACT

The right to erasure, or the right to be forgotten, has been one of the controversial reforms of the new General Data

Protection Regulation of the European Union (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016). In essence, this right represents an updating of the right to cancel of personal data. The problem raised by the right to be forgotten is twofold. On the one hand, the problem is its own content, since it is not well defined in Article 17 of Regulation. On the other, we find the issues arising from its practical application. In accordance with the rules on international jurisdiction and determining the applicable law of the GDPR, within the European Union can legally claim the fulfillment of this right, even against Internet operators outside the EU. However, it can be complicated if you have to seek enforcement of a judgment that recognized this right in a third non-EU State, especially if the application for recognition and enforcement is requested to the United States. The complication comes not only because the EU is being pioneered in the legal recognition of this right, but also because emerge through it the differences in the protection of the "privacy", which is in the end what tries to protected the right to be forgotten.

Key words: Right to be forgotten, right to erasure, extra-territoriality, General Data Protection Regulation, International Jurisdiction, Applicable Law, Tort Law, Google Spain case law.

Derechos de los interesados en el reglamento general de protección de datos

Por María Arias Pou y Miguel Recio Gayo

RESUMEN

En junio de 2015 la Comisión Europea constató que más de ocho de cada diez personas manifestaron que no tenían un control total sobre sus datos personales. Que el interesado, cuyos datos personales son objeto de tratamiento, tenga el control sobre los mismos es la razón por la que el Reglamento general de protección de datos ha buscado reforzar, mediante la actualización y simplificación de la regulación, los derechos que se reconocen a aquél. Además, el Reglamento incluye también otros derechos nuevos, tales como el de portabilidad de los datos. De esta manera, se quiere mejorar el control del interesado sobre sus datos personales, generando al mismo tiempo la confianza necesaria, que es fundamental, para impulsar el Mercado Digital Único.

Palabras clave: Unión Europea – Comisión Europea – Reglamento general de protección de datos – datos personales – derecho fundamental a la protección de datos – interesado – derechos.

ABSTRACT

In June 2015 the European Commission found that more than eight out of ten people felt they do not have total control over their personal data. That the data subject, whose personal data are processed, has control over them is the reason why the General data protection regulation has sought to reinforce, by updating and simplifying the regulation, the rights recognized to him. In addition, the regulation also includes other new rights, such as the right to data portability. In this way, to improve the control of the data subject about his or her personal data, generating at the same time the needed trust, which is essential, to promote the Digital Single Market.

Keywords: European Union – European Commission – General data protection regulation – personal data – fundamental right to data protection – data subject – rights.

Nuevo marco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del riesgo

Por Paloma Llana González

RESUMEN

El Reglamento General de Protección de Datos (RGPD) requiere que las organizaciones tengan personal experto en la implantación de políticas y procedimientos para garantizar el cumplimiento del Reglamento, sobre todo en los aspectos técnicos y organizativos, ya que las entidades han de demostrar el cumplimiento de las políticas incluso por la vía de la certificación por tercero. El programa de cumplimiento del RGPD incluye, aunque no se limitan, el nombramiento de un delegado de protección de datos (cuando sea preceptivo), el mantenimiento de registros internos; la aplicación de medidas de seguridad de la información; así como la implantación de la privacidad desde el diseño y por defecto y las evaluaciones de impacto. Por lo tanto, las empresas deberán

- Revisar sus actuales programas de cumplimiento. En la medida en que el plan de cumplimiento de una organización no responda plenamente a los requisitos del Reglamento, dicho plan habrá de actualizarse y ampliarse;
- Asegurarse de que tienen un registro de la totalidad de sus actividades de procesamiento de datos.
- Identificar una persona adecuada para cumplir con el papel de delegado de protección de datos y garantizarle recursos e

independencia suficientes para desempeñar adecuadamente sus funciones.

Palabras clave: Delegado de protección de datos, Privacidad desde el diseño, Evaluación de impacto de privacidad, registros internos, medidas de seguridad de la información.

ABSTRACT

The General Data Protection Regulation (GDPR) requires controllers to implement policies and procedures to ensure compliance with the Regulation. In addition, controllers must demonstrate their compliance. Elements of a compliance program include (but are not limited to): appointing a DPO (if required); maintaining internal records; implementing robust information security measures; and privacy by design and DPIAs. Therefore, businesses should

- Review their existing compliance programs. To the extent that a business' existing compliance programme does not fully address the requirements of the Regulation, that programme should be updated and expanded as necessary;
- Ensure that they have clear records of all of their data processing activities. If this information has already been collated (e.g., as the result of a recent registration project) then producing internal records is likely to be straightforward.
- Identify a suitable person to fulfil the role of the DPO (if required) and ensure the DPO has sufficient resources and independence to adequately perform his or her duties.

Keywords: Data Protection Officer, Privacy by Design, Privacy impact assessment, internal records, information security measures

EN PROSPECTIVA

Ya tenemos un reglamento general de protección de datos... ¿y ahora qué?

Por Jorge Villarino Marzo

LA ENCUESTA

Transferencias internacionales de datos

Con la participación de Óscar Casado Oliva, Alonso Hurtado Bueno y Miguel Álvarez de Prada.

LA ENTREVISTA

Con José Luis Piñar Mañanas

EN RED

Normativa, Jurisprudencia y Publicaciones

Por Lorena Rivera Novillo

Año 2015

Número 3

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

Privacidad y seguridad: un dilema permanente

Por Javier Rupérez.

ESTUDIOS

De nuevo sobre los ciberdelitos en el derecho español tras la reforma de 2015

Por Moisés Barrio Andrés

SUMARIO

1. INTRODUCCIÓN.
2. ¿EXISTEN LOS "DELITOS INFORMÁTICOS" O "DELITOS CIBERNÉTICOS"?
3. PROBLEMAS JURÍDICO-PENALES QUE PLANTEA LA CIBERDELINCUENCIA
4. pANORAMA COMPARADO E INTERNACIONAL.
5. LA CIBERDELINCUENCIA EN EL CÓDIGO PENAL ESPAÑOL.
6. LOS DISTINTOS DELITOS EN PARTICULAR.
7. CONCLUSIÓN

RESUMEN

El presente trabajo aborda la problemática de los ciberdelitos en España. Se analiza, en primer lugar, su configuración dogmática. A continuación, se exponen los problemas jurídicos propios que plantea. Seguidamente, se examina brevemente el derecho comparado e internacional en la materia, para pasar a estudiar con detalle el régimen jurídico en España y, particularmente, las modificaciones operadas tras la reforma del Código Penal mediante la Ley Orgánica 1/2015, de 30 de marzo. Finalmente, en sede de conclusiones, se apuntan varias consideraciones críticas y se sugieren diversas líneas de reforma.

Palabras clave: ciberdelincuencia, cibercrimen, delito informático, delito cibernético, hacking, cracking, delitos en internet

ABSTRACT

This paper addresses the problem of "cybercrime" in Spain. It analyzes, first, its dogmatic configuration. Then own legal problems are exposed. Next, examines the comparative and international law in this area, moving to study in detail the legal regime in Spain and particularly the modifications after the reform of the Criminal Code by Organic Law 1 / 2015 of March 30, 2015. Finally, based on findings, it suggests several critical considerations and points out various lines of reform.

Key words: computer crime, cybercrime, hacking, cracking, cyber crime, internet crimes

Análisis de la sentencia de invalidez del acuerdo de puerto seguro (*safe harbour*)

Por María Álvarez Caro

SUMARIO

1. CONSIDERACIONES GENERALES, HECHOS Y CUESTIONES PREJUDICIALES PLANTEADAS EN EL CASO SCHREMS (C-362/14)
2. INTERPRETACIÓN DE LA DECISIÓN 520/2000/CE CONFORME A LA CARTA DE DERECHOS FUNDAMENTALES DE LA UE
3. FACULTADES DE LAS AUTORIDADES NACIONALES DE PROTECCIÓN DE DATOS

4. INVALIDEZ DE LA DECISIÓN 520/2000/CE DE PUERTO SEGURO
5. CONCLUSIONES
6. BIBLIOGRAFÍA

RESUMEN

En octubre de 2015, el Tribunal de Justicia de la UE (TJUE) dictó una sentencia clave en lo relativo a transferencias internacionales de datos personales. Dicho fallo invalida la Decisión 2000/520/CE de la Comisión Europea que declaraba el nivel adecuado en protección de datos del Puerto Seguro (*Safe Harbour*) entre EE.UU y la UE. El TJUE considera que una decisión de la Comisión sobre el nivel adecuado de un tercer país no puede limitar ni anular las facultades de las autoridades nacionales de protección de datos. Igualmente, estima que la Decisión es inválida al contemplar una excepción por razones de seguridad nacional. Esta sentencia genera inseguridad jurídica hasta no tener un nuevo régimen o reglas claras de interpretación del fallo.

Palabras clave: Puerto Seguro, Decisión 2000/520/CE, Directiva 95/46/CE, transferencias internacionales de datos, Carta de Derechos Fundamentales de la UE

ABSTRACT

On October 2015, European Court of Justice (ECJ) issued a key ruling related to international personal data transfers. The mentioned ruling invalidates 520/2000/EC Decision that declared the adequate level of data protection of the Safe Harbour Agreement (*Safe Harbour*) between the US and the EU. The ECJ considers that a European Commission Decision declaring the adequate protection level of a third country

cannot limit or nullify the faculties of national data protection authorities. Also, it estimates that the Decission is not valid as it contemplates an exception for national security reasons. This ruling implies legal uncertainty until a new regime is approved or until there are clear interpretarion rules of this sentence.

Keywords: Safe Harbour, 520/2000/EC Decision, 95/46/EC Directive, international data transfers, EU Charter of Fundamental Rights

El desarrollo de mecanismos internacionales de cooperación para combatir el ciberterrorismo. Estado de la cuestión.

Por Vicente Moret Millás

RESUMEN

La preocupación de los Gobiernos de todo el mundo por asegurar un cierto nivel de ciberseguridad a sus ciudadanos está justificada. Una de las principales amenazas contra nuestras sociedades adopta la forma de ciberterrorismo, concepto sometido a debate acerca de su concreta definición. La respuesta a esta amenaza vendrá en parte desde el derecho internacional y la necesaria cooperación entre los Estados. En este sentido, las herramientas más útiles para combatir al ciberterrorismo serán los acuerdos internacionales así como los mecanismos de cooperación internacional entre las autoridades judiciales y policiales de los distintos Estados. Por ello, se considera que el establecimiento de una normativa internacional que permita combatir de forma coordinada la amenaza del ciberterrorismo será imprescindible si queremos

asegurar un nivel de protección adecuado de nuestras sociedades.

Palabras clave: Ciberterrorismo, Ciberseguridad, Cooperación internacional, Directiva NIS, Infraestructuras críticas.

ABSTRACT

The concern of governments around the world to ensure a certain level of cyber security to its citizens is justified. One of the major threats is the different forms of cyberterrorism, concept subject to debate about its precise definition. The response to this threat will come in part from the international law and the need for cooperation among States. In this sense, the most useful tools to combat cyberterrorism are international agreements and mechanisms of international cooperation between judicial and police authorities from different States. Therefore, it is considered that the establishment of an international standards that allows a coordinated way to fight the threat of cyberterrorism will be essential if we are to ensure an adequate level of protection of our societies.

Keywords: Cyberterrorism, Cybersecurity, NIS Directive, Critical Infrastructures, International Cooperation.

“Interoperabilidad legal” y otros problemas jurídicos derivados del manejo de “datos científicos” como “big data” por servicios web e infraestructuras de la economía del conocimiento: el ejemplo de los datos sobre diversidad biológica.

Por Enrique Alonso García

EN PROSPECTIVA

Apuntes sobre la reforma procesal en materia De investigación tecnológica

Por Elvira Tejada de la Fuente

LA ENCUESTA

Adblocking

*con la participación de Pepe Cerezo, Pablo Fernández Burgueño y
Paula Ortiz.*

LA ENTREVISTA

*Con Doña Mar España Martí. Directora de la Agencia Española dDe
Protección De Datos*

EN RED

Normativa, jurisprudencia y publicaciones.

Número 2

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

La robótica como paradigma tecnológico de importancia clave en el presente y futuro inmediato

Por Víctor Calvo-Sotelo Ibáñez-Martín

ESTUDIOS

Robótica en transformación: retos, riesgos y futuro

Por Antonio Luis Flores

RESUMEN

La robótica está actualmente en plena transformación, motivada por los avances en otras disciplinas paralelas, como son la Internet de las cosas, las telecomunicaciones y el fenómeno Internet. Además, la sociedad se digitaliza cada día más y esto facilita nuevos usos y aplicaciones de los robots, más allá de su tradicional ámbito industrial, para liderar iniciativas como los vehículos sin conductor o los drones. Sin embargo, los mayores avances en robótica siguen siendo en el campo militar, donde la gran inteligencia y capacidad de los nuevos aviones no tripulados o robots soldados comienzan a preocupar a la comunidad científica. En este artículo se pretende dar una visión global sobre todas estas cuestiones para ganar perspectiva y poder predecir cuál puede ser el futuro de la robótica en los próximos años.

Palabras clave: Robot, robótica, androide, humanoide, UCAV, UAV, coche Google.

ABSTRACT

Robotics is currently undergoing transformation, driven by parallel progress in other disciplines, such as the Internet of Things, Telecommunications and Internet phenomenon. In addition, society gets increasingly digitized and this facilitates new uses and applications of robots beyond its traditional industrial field, to lead initiatives as driverless vehicles or drones. However, the greatest advances in robotics correspond to the military field, where the strong intelligence and capacity of new drones or robot soldiers begin to worry the scientific community. This article gives an overview on all these issues to gain perspective and be able to predict what the future of robotics could be in the coming years.

Key words: Robot, robotics, android, humanoid, UCAV, UAV, Google car.

La robótica y el cambio de paradigma de la cuarta revolución industrial

Por Francisco Javier García Díaz

RESUMEN

Este trabajo es un análisis sobre lo que recientemente el “consenso” -tecnólogos, científicos, sociólogos, consultores y empresas industriales- ha venido a denominar Industria 4.0 y lo que ello representa a través del uso de las nuevas tecnologías para que sea considerada una nueva “evolución” dentro del marco de la Revolución Industrial: la Cuarta Revolución Industrial. Industria 4.0 supone un cambio de paradigma de los medios de producción, que las empresas

habrán de ir adaptando mediante la implantación del concepto de “factoría inteligente”, cuyo core business está basado en aplicaciones robóticas y en un ecosistema plenamente digital interconectado mediante Internet.

Palabras clave: Revolución Industrial, Robótica, Internet de las Cosas, Cadena de valor digital, Industria 4.0

ABSTRACT

This paper is an analysis about what the consensus of opinion -technologists, scientists, sociologists, consultants and manufacturing industries- has lately named Industry 4.0 and about what it represents by using new technologies in order to be accepted as a new “evolution” in the Industrial Revolution framework: the Fourth Industrial Revolution. Industry 4.0 involves a change of paradigm in terms of production that the firms will have to adapt across the implementation of the “smart factory” concept of which core business is based on robot applications and a fully digital ecosystem interconnected on the Internet.

Keywords: Industrial Revolution, Robotics, Internet of Things, Digital value chain, Industry 4.0

Cuestiones jurídicas que plantean los robots

Por Alejandro Sánchez del Campo Redonet

RESUMEN

La creciente automatización de tareas y trabajos y el desarrollo exponencial de las tecnologías relacionadas con la inteligencia artificial empiezan a plantear cuestiones legales que el sector

jurídico no puede ignorar. El presente trabajo aborda cómo la línea entre persona y máquina se va haciendo cada vez más difusa y cómo va a afectar el desarrollo de los futuros “robots inteligentes” al régimen de responsabilidad e incluso a las categorías de personalidad legal reconocidas en nuestro Código Civil. También se analiza si tiene sentido crear una *lex robótica* y cómo se debe regular la innovación disruptiva.

Palabras clave: robots, responsabilidad, regulación, personalidad, ética.

ABSTRACT

The increasing automation of tasks and jobs and the exponential development of technologies related to artificial intelligence are starting to pose important legal issues the legal sector cannot ignore. This paper addresses how the line between man and machine is increasingly blurring and how the development of new "intelligent robots" might affect liability rules and even the categories of legal personality recognized in the Spanish Civil Code. It also covers whether it makes sense to create a *lex robotica* and which would be the best way to regulate disruptive innovation.

Keywords: robots, liability, regulation, personality and ethics.

VENTANA COMPARADA

La robótica y las lecciones del derecho cibernético

Por Ryan Calo

RESUMEN

Dos décadas de análisis han producido una rica variedad de conocimiento de cómo la Ley debería aplicarse a las

características peculiares de Internet. Pero, entretanto, la tecnología no se ha quedado parada. Las mismas instituciones públicas y privadas que desarrollaron Internet, desde las fuerzas armadas hasta los motores de búsqueda, han iniciado un cambio significativo hacia el desarrollo de la robótica y la inteligencia artificial.

Este Artículo es el primero en examinar lo que la introducción de una tecnología nueva e igualmente transformadora, significa para el derecho Cibernético y la formulación de una normativa. La Robótica tiene un conjunto de características esenciales distinto de las de Internet y como consecuencia suscitará distintos temas jurídicos. La Robótica combina por primera vez, la promiscuidad de los datos con la capacidad de causar daño físico; los sistemas robóticos logran tareas por vías que no se pueden prever con antelación; y los robots cada vez más desdibujan la línea entre persona e instrumento.

La Robótica demostrará “lo excepcional” en el sentido de propiciar cambios sistemáticos en la legislación, las instituciones y en el mundo académico del derecho. Pero no veremos un panorama claro: muchos de los conocimientos y métodos básicos del derecho cibernético demostrarán que son cruciales en la integración de la robótica y tal vez en lo que nos traiga la tecnología.

EN PROSPECTIVA

Lex robótica y derecho digital

Por Pablo García Mexía

LA ENCUESTA

Robótica y Derechos Humanos

con la participación de Borja Adsuara, Lorenzo Cotino y Ricard Martínez.

LA ENTREVISTA

Con Erica Palmerini.

EN RED

Normativa, jurisprudencia y publicaciones.

Número 1

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

El valor de la transparencia

Por Elisa de la Nuez

ESTUDIOS

Consideraciones sobre la protección de datos y los servicios de Cloud referencia al nuevo reglamento Europeo.

Por Luis Felipe López Alvarez

RESUMEN

Cada vez es más usual el uso de los servicios de computación en nube. Junto a los beneficios económicos que su utilización lleva consigo, es importante también tener presente los riesgos que este nuevo sistema de tratamiento de datos implica, en especial en lo relativo a la protección de los datos personales. En este trabajo, se van a revisar los problemas legales que presenta la computación en nube y las soluciones que el ordenamiento jurídico, español y comunitario, ofrece mediante la actual normativa de protección de datos: la Directiva 1995/46/CE, de 24 de octubre, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo, y las decisiones vinculantes adoptadas por la Comisión Europea y la Agencia Española de Protección de Datos. El estudio de la normativa vigente se completa con un análisis de la próxima normativa de aplicación

general en toda la UE, el Reglamento General de Protección de Datos, mostrando los logros y ventajas que contiene, y avisando de los posibles problemas que su aplicación puede plantear.

Palabras clave: Protección de datos, servicios en nube, transferencias internacionales de datos, habeas data, Reglamento General de Protección de Datos de la UE.

ABSTRACT

It is increasingly common use of cloud computing services. Together with the economic benefits that its use entails, it is important to keep in mind the risks that this new system of data processing means, especially as regards the protection of personal data. In this paper, we will review the legal issues involved in cloud computing and the legal solutions that Spanish and Community law offers through the current data protection regulations: Directive 1995/46 / EC of 24 October, Law 15/1999, of December 13, Protection of Personal Data and its implementing regulation, and the binding decisions adopted by the European Commission and the Spanish Data Protection Agency. The study of current legislation is completed by an analysis of the EU upcoming general rules, the General Data Protection Regulation, showing the achievements and benefits it contains, and warning about potential problems that may pose its implementation.

Key words: Data protection, cloud computing services, international data transfers, habeas data, EU General Data Protection Regulation

El indispensable equilibrio entre el derecho y la privacidad ciudadana y el principio de transparencia pública: algunas claves para superar su colisión y lograr su complementación en democracia.

Por Marta Méndez Juez

RESUMEN

Un Estado de Bienestar debe garantizar y proteger derechos ciudadanos y libertades públicas cada vez más amplios y, en numerosas ocasiones, cada vez más difíciles de ensamblar entre ellos. Un claro ejemplo lo constituye la aparente colisión entre la Privacidad ciudadana y la Transparencia pública, en donde se percibe que la salvaguarda del interés particular en aspectos relacionados con la intimidad, el honor y la propia imagen del ciudadano, parece no poder conciliarse con el interés colectivo de suministrar la información que generan o que poseen las instituciones político-administrativas a la sociedad. La regulación que el legislador español lleva a cabo sobre tales aspectos, pone de manifiesto la necesidad imperante de complementar Privacidad y Transparencia en Democracia, a través de técnicas organizativas como la anonimización, que fomentan la máxima publicidad de la información pública, respetando la protección de datos de carácter personal desde el origen.

Palabras clave: Democracia; Transparencia; Privacidad; Diseño; Información; Excepción; Anonimización.

ABSTRACT

Welfare State must guarantee and must protect civil rights and liberties increasingly large and, many times, it is more difficult to assemble between them. A clear example is the apparent

collision between citizen Privacy and public Transparency, where it is perceived that the safeguarding of particular interest in issues related to intimacy, honor and self-image of the citizen, it not seems to be reconciled with the public interest to provide information that generate and possess the political-administrative institutions of society. The regulation that the Spanish Legislator carried out on such aspects, it highlights the urgent need to complement Privacy and Transparency in Democracy, through organizational techniques such as anonymity, that it promotes maximum disclosure of public information respecting protection personal data from the source.

Keywords: Democracy; Transparency; Privacy; Design; Information; Exception; Anonymization.

Privacy by Desing: la privacidad como ventaja competitiva.

Por Cristina Garcerán Ortega

RESUMEN

En nuestros días se encuentra disponible a nivel globalizado un volumen de información personal de una magnitud cuantitativa sin precedentes. La sociedad y el mercado evolucionan hacia un escenario de marcado carácter tecnológico, generándose nuevos retos para la privacidad. El futuro Reglamento Europeo de Protección de Datos convertirá en exigencia legal el cumplimiento de los dictados de Privacy by Design, concepto que promueve la implantación de la privacidad por defecto desde el momento de diseño de todo proyecto, garantizando el máximo respeto y seguridad en el tratamiento de la información personal. Las siguientes líneas

ahondan en el estudio de Privacy by Design, presentando la privacidad como ventaja competitiva para la empresa.

Palabras clave: Empresa, Innovación, Ventaja competitiva, Privacy by Design, Normativa-compliance.

ABSTRACT

Nowadays, it is available a volume of personal information, in a global level, in a quantitative unprecedented magnitude. Both, society and market are evolving towards a technological scenario. The future European General Data Protection Regulation will turn into legal requirement compliance with Privacy by Design, concept that promotes implantation of privacy as a default condition, embedded into the design of any project, ensuring the highest respect and safety in the processing of personal information. Through the following lines Privacy by Design is studied presenting privacy as a competitive advantage for the companies.

Keywords: Company, Innovation, Competitive advantage, Privacy by Design, Compliance.

VENTANA COMPARADA

El impuesto Catalán sobre la provisión de servicios de comunicaciones electrónicas.

Por José A. Rozas.

RESUMEN

El 10 de diciembre de 2014 se publicó en el núm. 6767 del Diari Oficial de la Generalitat de Catalunya, la Ley 15/2014, de 4 de diciembre, por la que se crea en esta Comunidad Autónoma el impuesto sobre la provisión de contenidos por parte de prestadores de servicios de comunicaciones electrónicas y de

fomento del sector audiovisual y la difusión cultural digital, en adelante IPSCE (la versión en castellano de dicha ley se publicó en el Boletín Oficial del Estado, núm. 309, de 23 de diciembre de 2014). Durante todo el año 2014 se había venido trabajando en el mismo, pero su tramitación parlamentaria fue verdaderamente acelerada, pues la fecha de registro del proyecto de ley en el Parlamento, el 19 de noviembre, es apenas un mes anterior al de su aprobación. El Gobierno de la Nación ha anunciado su intención de presentar recurso de inconstitucionalidad contra el mismo, pese a lo que la Generalitat no renuncia a su implantación, estando pendiente a la fecha de redacción de estas líneas su necesario desarrollo reglamentario, sin el que no es posible su aplicación efectiva.

Se trata de un impuesto propio de la Comunidad autónoma catalana por el que se sujeta a gravamen la provisión de servicios de adsl y cuya recaudación está afectada a la financiación de políticas culturales de la Generalitat de Cataluña en el ámbito del sector audiovisual y digital. El objeto del presente trabajo es presentar a los lectores italianos dicho impuesto, verdaderamente singular, exponiendo en primer lugar su naturaleza y características generales (epígrafe 1) para a partir de la exposición de sus elementos estructurales y régimen aplicativo y sancionador (epígrafe 2) abordar una aproximación a su eventual inconstitucionalidad y vulneración del Derecho comunitario (epígrafe 3) y terminar con unas conclusiones sobre su razón de ser y el problema que aborda (epígrafe 4).

EN PROSPECTIVA

El futuro de las Agencias de Protección de Datos.

Por Rosa García Ontoso

LA ENCUESTA

Mercado digital Europeo.

Con la participación de Stephan Fuetterer, Alejandro Perales y Enrique Ferrer

LA ENTREVISTA

Con Bárbara Navarro

EN RED

Normativa, jurisprudencia y publicaciones.

Número 0

CARTA DEL DIRECTOR

Por Pablo García Mexía

TRIBUNA DE HONOR

El reto de personalizar respetando la privacidad de los usuarios

Por Miguel Pérez Subías

ESTUDIOS

Acerca de la evolución de la figura del encargado del tratamiento

Por Miguel Recio Gayo

RESUMEN

La figura del encargado del tratamiento ha pasado de ser una desconocida a convertirse en una protagonista. Es necesario que la misma siga siendo analizada para delimitar claramente su responsabilidad. Las garantías que ofrezca en el desempeño de sus funciones y, en su caso, una posible certificación, podrían ser clave para su futuro.

Palabras clave: Protección de datos – encargado del tratamiento – responsable del tratamiento –tratamiento de datos personales – cumplimiento – responsabilidad.

ABSTRACT

The figure of the processor has gone from being an unknown to become a main actor. It is necessary that the same keep being analyzed to delineate clearly its liability. Guaranties

offered in the performance of its functions and, where appropriate, possible certification, could be key to its future.

Keywords: Data protection – processor – controller – processing of personal data – compliance – accountability.

La lucha por el principio de igualdad en la red.

Por Mercedes Fuentes

RESUMEN

Hace años que se trata de asentar el mástil del carácter abierto y neutral de la Red con el fin de ofrecer una navegación por Internet respetuosa con la libertad e igualdad de los ciudadanos. Este trabajo se centra en la evolución de la lucha por garantizar la neutralidad en la Red, esto es, el principio de igualdad.

Palabras clave: Neutralidad de la Red; Internet abierta; Principio de igualdad.

ABSTRACT

Settling the mast the open Internet and net neutrality is a necessary purpose in order to guarantee navigation over the Internet which respects the freedom and equality of citizens. This work focuses on the evolution of the fight to ensure neutrality in the network, that is, the principle of equality.

Key words: Net neutrality; open Internet; Principle of equality.

Privacidad y propiedad intelectual: el justo equilibrio entre derechos.

Por Jorge Villarino Marzo

RESUMEN

La protección de los derechos de propiedad intelectual se ha visto particularmente afectada por la implantación del mundo digital. Algunos mecanismos provistos por las Directivas europeas se han visto limitados por el respeto debido al contenido esencial de los derechos fundamentales y, particularmente, del derecho a la protección de datos. La ponderación de los derechos fundamentales en cada caso concreto ha sido una de las soluciones adoptadas por la jurisprudencia de los tribunales europeos y nacionales. Otras cuestiones que forman parte de este debate son el régimen de responsabilidad de los proveedores de servicios de internet y el debate todavía abierto sobre si las direcciones IP son o no datos personales.

Palabras clave: propiedad intelectual, protección de datos, prestadores de servicios de internet, direcciones IP.

ABSTRACT

The protection of intellectual property rights has been particularly affected by the implementation of the digital world. Several mechanisms deployed by European Directives have been limited by the due respect to the core content of fundamental rights, and particularly of the right to data protection. Balancing fundamental rights on a case by case basis has been one of the solutions adopted by the jurisprudence of European and national courts. Other issues of concern in this debate have been the liability regime of internet

service providers and the still open debate of whether IP addresses are personal data or not.

Keywords: intellectual property, data protection, internet service providers, IP addresses.

VENTANA COMPARADA

De nuevo a vueltas con la neutralidad de las búsquedas.

Por Enric Goldman

EN PROSPECTIVA

La nueva economía de mañana o la post revolución de las TIC

Por Jesús Venegas

LA ENCUESTA

Internet y el terrorismo Islamista.

Con la participación de Paloma Llana González y Ángel Gómez de Agreda.

LA ENTREVISTA

Con José Luis Rodríguez Álvarez, Director de la Agencia Española de Protección de datos.

EN RED

Normativa, jurisprudencia y publicaciones.



www.rdu.es



Síguenos en Twitter (@Revista_rdu)