

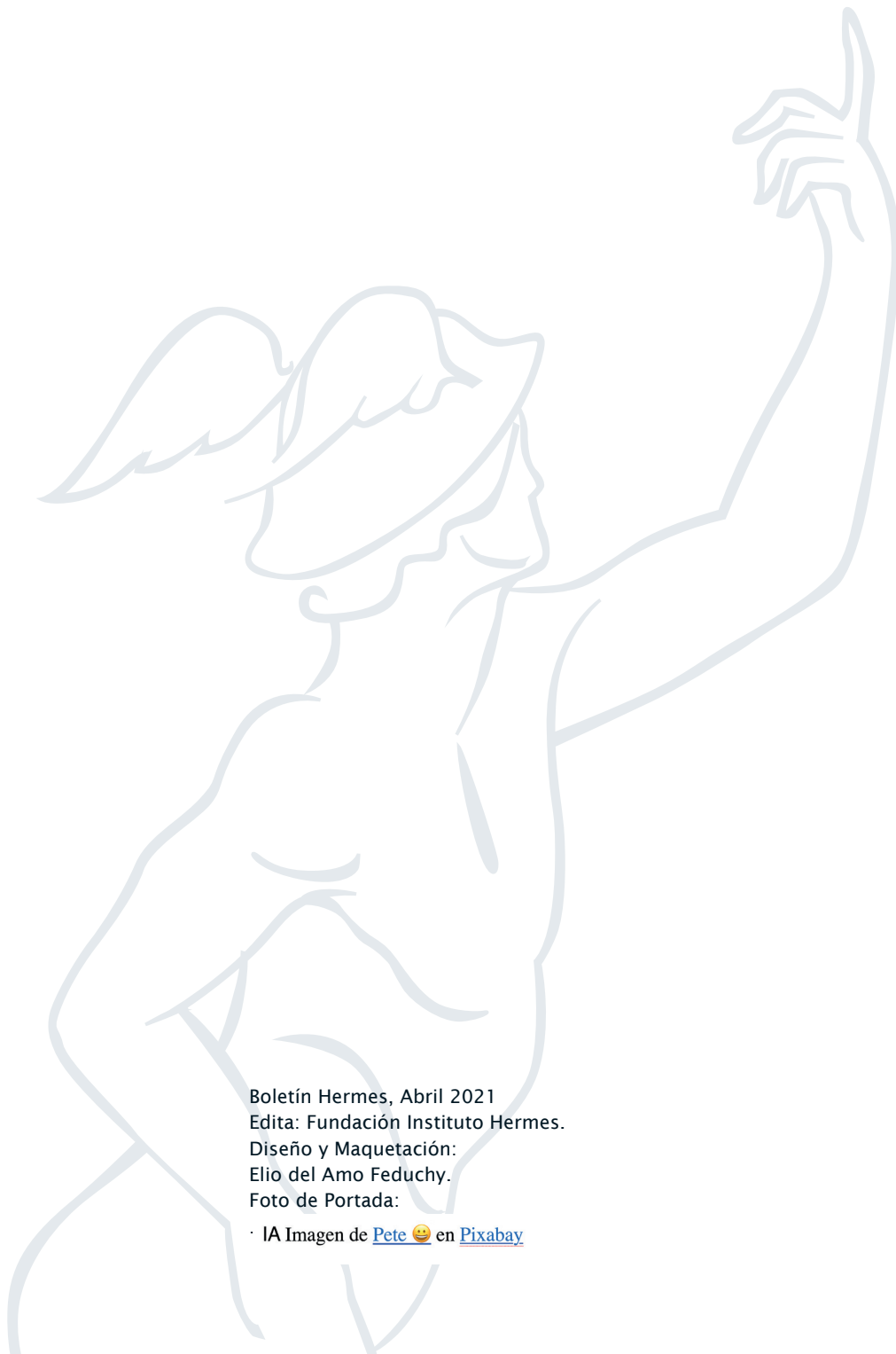


**Instituto
Hermes**

Derechos de ciudadanía digital

BOLETÍN HERMES

Año 2 • nº 7 • abril 2021



Boletín Hermes, Abril 2021
Edita: Fundación Instituto Hermes.
Diseño y Maquetación:
Elio del Amo Feduchy.
Foto de Portada:

· IA Imagen de [Pete](#) 😊 en [Pixabay](#)



Índice

Inteligencia Artificial	2
Los delirios y las alucinaciones de la IA	2
¿Son los comportamientos predecibles?.....	3
Regulación europea de la IA	5
Trabajo y derechos digitales	9
«No regulamos plataformas sino derechos».....	9
Neuroderechos: Chile aprueba el proyecto de ley que regulará los Neuroderechos	12
Datos Abiertos	13
El marco legal de protección de datos de la UE no se interpone en el camino del desarrollo de la economía de datos	15
Identidad Digital	16
Italia: Protección al menor	16
Alemania: Seguridad de datos y DNI digital	17
Francia: Nuevo DNI Digital.....	19
Presidencia Portuguesa de la UE: Reglamento ePrivacy.....	19
Monedas digitales soberanas	20
El Euro Digital	20
China: divisa digital soberana.....	24
«Bitcoin»	26
Breves	27
Plan de digitalización España 2025.....	27
Derechos Digitales y Reto Demográfico	30
Educación.....	30
Recomendamos.....	32
Multimedia.....	32
«Made for Love», primera serie sobre neuroderechos	32

Inteligencia Artificial

Los delirios y las alucinaciones de la IA

En la comunidad científica crece la preocupación y la estupefacción ante comportamientos registrados por Inteligencias Artificiales incomprensibles para el ser humano. En ocasiones anteriores Hermes se ha hecho eco de «fracasos» de servicios online automatizados que se vieron obligados a suspender su actividad tras episodios de delirio de la IA a cargo. David Susillo, uno de los científicos más reputados en el terreno de la Inteligencia Artificial es coautor de un paper que analiza y categoriza los errores cometidos por una IA de traducción automática alimentada con repositorios de documentos de la UE.

En el estudio explica que los sistemas de traducción automática neuronal (NMT) han alcanzado un alto nivel rendimiento y su utilización va en aumento. Sin embargo, persiste el desconocimiento sobre su funcionamiento o sobre por qué puede llegar a corromperse. Lo sorprendente es que pone en evidencia que los sistemas NMT pueden generar traducciones completamente desvinculadas del texto original. A esta traducción patológica la denominan alucinaciones de la IA.

Describimos un método para generar alucinaciones y mostramos que muchas variaciones comunes de la arquitectura NMT son susceptibles a ellas. Estudiamos una variedad de enfoques para reducir la frecuencia de las alucinaciones, incluido el aumento de datos, los sistemas dinámicos y las técnicas de regularización.

Los usuarios de una de las mejores IAs de traducción, que es además de las más usadas en el ámbito empresarial en Europa, **DeepL**, han denunciado la reciente tendencia de la IA alemana a añadir líneas e incluso párrafos de su propia cosecha a las traducciones. Algunos usuarios observaron además una cierta fijación contra China y el uso de expresiones violentas sin venir a cuento.

«¿Habrà desarrollado una forma de entender el subconsciente de los autores?», se preguntaba un usuario habitual. Hay que decir que deepL fue entrenada con una gran masa de textos oficiales y vinculados a la burocracia de la UE.

La alarma ante las IA ha ido creciendo hasta tal punto que el **Foro Económico Mundial** identifica como uno de los riesgos globales el colapso de infraestructuras críticas por «aportes creativos» de las IAs. Estamos mucho más allá de la queja por los posibles sesgos discriminatorios.

En principio los sesgos pueden corregirse en la medida en que generalmente se atribuyen no a los algoritmos sino a desequilibrios en los datos que alimentan a las IAs. Desequilibrios que proyectan desequilibrios estadísticos en la vida real que aunque no necesariamente reflejan desigualdades sociales, cuando lo hacen tienden a reproducirlas.

En la hipótesis general en caso de sesgo, en realidad bastaría resetear los procesos de deep learning con bases de datos re-equilibradas.

Pero con las alucinaciones estamos con los dos pies en otro mundo. El de HAL en 2001. El que ha llevado a los militares franceses a desaconsejar la automatización del control de su armamento nuclear. Un mundo en el que las jugadas creativas de la IA puede ser tan destructivas como impredecibles... y casi imposibles de arreglar.

Las dificultades de los investigadores a la hora de identificar el origen de los problemas y corregirlos en algo tan relativamente sencillo como un traductor automático, nos colocan de frente ante la realidad: la IA genera de forma dinámica en sus procesos de aprendizaje algoritmos que no podemos describir, testar ni comprender.

Solo podemos - y todavía de forma tan solo tentativa - asignar riesgos al delirio. Es decir, nos movemos en un mundo probabilístico en el que muchas veces, juzgar las decisiones de la IA es materialmente imposible y en el que no podemos discernir claramente entre respuestas inesperadas pero correctas y delirios.

Algo que los jugadores de Go descubrieron ya durante lo que los estadounidenses llamaron el momento Sputnik de la IA, el famoso torneo entre AlphaGo y el gran maestro coreano Lee Sedol. Entonces, *una jugada creativa* de Google AlphaGo permitió a Lee Sedol dar la vuelta a la única partida que el humano ganó contra el ingenio de Google.

¿Son los comportamientos predecibles?

Ha sido muy comentado un estudio realizado por científicos sociales para analizar la capacidad predictiva de los sistemas de aprendizaje automático supervisados (SML por sus siglas en inglés). Publicado por 112 coautores en *Proceedings of the National Academy of Sciences*, los resultados sugieren que los sociólogos y científicos de datos deben tener cuidado al usar modelos predictivos, especialmente en su aplicación a programas sociales y al sistema judicial.

Los investigadores propusieron predecir seis resultados de vida tomando como fuente los datos de seguimiento de más de 4.000 familias de EEUU registrados desde el año 2000. Se lanzó un proyecto de colaboración masiva, «Fragile Families Challenge» al que se unieron 160 equipos de diferentes universidades que utilizaron las series de datos para entrenar sus modelos predictivos. Se les permite el acceso a 5 cortes a lo largo del tiempo y se definen las métricas que se deben medir. La sexta ola de datos solo es conocida por los organizadores del reto. Los equipos son juzgados por una métrica común que evalúa la precisión de sus predicciones.

Con independencia del método utilizado por los equipos, los resultados fueron bastante pobres, las predicciones fueron consistentemente erróneas para un subconjunto de familias en cada uno de los métodos. Tomados uno a uno, los estudios difícilmente podrían haber sido utilizados. Y lo que es más, **los sistemas SML en la mayoría de las ocasiones fueron superados por modelos de regresión estándar.**

En las conclusiones del trabajo, se recomienda **evitar el uso indiscriminado de modelos predictivos complejos** y aplicarlos únicamente cuando sea posible una mejora en los resultados en comparación con modelos simples, ya que estos han demostrado un mejor desempeño. A raíz de su publicación, en la comunidad científica han recordado que *la predicción no es un objetivo típico en las ciencias sociales a pesar de los recientes argumentos que defienden que debería serlo. Los científicos sociales se centran en la inferencia: es decir, en comprender cómo se relaciona un resultado con algún insumo.*

Nuestra incapacidad para predecir los resultados de la vida podría significar que las variables de nuestra investigación (impulsadas por nuestras teorías actuales) no captan las dimensiones relevantes de la vida de las personas, o podría significar que los resultados de la vida son demasiado idiosincrásicos y están sujetos a un límite de previsibilidad.

No obstante, consideran que el «Fragile Families Challenge» es un gran avance en las ciencias sociales, constituye un ejemplo de colaboración masiva y evalúa la previsibilidad de comportamientos en una encuesta longitudinal de alta calidad. El hecho de no predecir los resultados individuales y familiares, en este caso, es todo menos decepcionante.

Regulación europea de la IA

La Comisión Europea ha propuesto un marco regulatorio sobre IA con el objetivo de **garantizar la protección de los derechos fundamentales y la seguridad** de los usuarios, así como fortalecer la **confianza** en el desarrollo y la adopción de la IA.

Establece la prohibición de usos considerados especialmente nocivos, como el uso de identificación biométrica indiscriminado en espacios públicos.

Todos los sistemas de IA destinados a utilizarse para la identificación biométrica remota de personas se considerarán de alto riesgo y estarán sujetos a evaluaciones de la conformidad ex ante y por terceros, incluida la documentación y los requisitos de supervisión humana desde su diseño. También se prohíbe la práctica de la «calificación social» en las aplicaciones de inteligencia artificial.

Para facilitar la aplicación del reglamento, proyecta la creación de un «**Consejo Europeo de Inteligencia Artificial**», compuesto por un representante de cada país miembro y representantes de la Comisión y del Supervisor Europeo de Protección de Datos. Hasta la fecha, un total de 19 Estados han adoptado estrategias nacionales en materia de IA: Alemania, Bulgaria, Chequia, Chipre, Dinamarca, Eslovaquia, Estonia, Finlandia, Francia, Hungría, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Portugal, Suecia y, más recientemente, España y Polonia, en diciembre de 2020), además de Noruega.

Atendiendo al Pacto Verde, la Comisión propone acelerar la investigación para lograr sistemas de IA sostenibles que consuman «menos datos y menos energía».

A continuación ofrecemos un resumen del texto publicado el 21 de abril de 2021.

El nuevo marco se aplicará a los **agentes tanto públicos como privados de dentro y fuera de la UE** en la medida en que el sistema de IA se introduzca en el mercado de la Unión o su uso afecte a personas establecidas en ella.



Propone un planteamiento basado en el riesgo, para el que define cuatro niveles:

RIESGO INADMISIBLE

1

Se prohibirá un conjunto muy limitado de **usos especialmente nocivos** de la IA que **violen los derechos fundamentales** (por ejemplo, puntuación social por parte de los Gobiernos, explotación de los puntos débiles de los niños, uso de técnicas subliminales y, salvo contadas excepciones, determinados sistemas de identificación biométrica remota en directo en espacios públicos con fines policiales «vigilancia social indiscriminada»).

ALTO RIESGO

2

Se considera de alto riesgo un **número limitado de sistemas de IA** que tienen un **impacto negativo en la seguridad** de las personas o en sus **derechos fundamentales** (protegidos por la Carta de los Derechos Fundamentales de la UE). Con el fin de garantizar la confianza y seguridad de las personas, se formulan una serie de requisitos que deben cumplir los sistemas de inteligencia artificial en cuanto a la calidad de los conjuntos de datos utilizados; la documentación técnica y el llevar un registro; la transparencia y la divulgación de información a los usuarios; la supervisión humana, y la solidez, la precisión y la ciberseguridad. En caso de infracción, los requisitos permitirán a las autoridades nacionales acceder a la información necesaria para investigar si el uso de la IA cumplió la legislación.

RIESGO LIMITADO

3

En determinados sistemas de IA se imponen obligaciones específicas de **transparencia**, por ejemplo, cuando exista un riesgo claro de manipulación (por ejemplo, mediante el **uso de robots conversacionales**). **Los usuarios deben ser conscientes de que están interactuando con una máquina.**

RIESGO MÍNIMO

4

Riesgo mínimo: Todos los demás sistemas de IA pueden desarrollarse y utilizarse con arreglo a la legislación vigente sin obligaciones jurídicas adicionales. La inmensa mayoría de los sistemas de IA utilizados actualmente en la UE pertenece a esta categoría. De forma voluntaria, los proveedores de estos sistemas pueden optar por aplicar los requisitos de una IA digna de confianza y adherirse a códigos de conducta voluntarios.

La Comisión presta especial atención a la **identificación biométrica remota en tiempo real, y en un principio, plantea su prohibición**. Desde el punto de vista de los derechos fundamentales, su utilización en lugares públicos con fines coercitivos plantea especiales riesgos en especial para «la dignidad humana, el respeto de la vida privada y familiar, la protección de los datos personales y la no discriminación». Señala algunas excepciones, estrictamente definidas, limitadas y reguladas; entre ellas:

- Su empleo por parte de la policía para la búsqueda selectiva de víctimas potenciales específicas de delitos, incluidos menores desaparecidos;
- La respuesta al peligro inminente de un atentado terrorista;
- La detección e identificación de autores de delitos graves.

Esta decisión se justifica en base a las graves consecuencias que tendría un error en la identificación de una persona. La precisión de los sistemas de reconocimiento facial puede variar considerablemente en función de factores muy diversos, tales como la calidad de la cámara, la luz, la distancia, la base de datos, el algoritmo y la etnia, edad o sexo del sujeto. Lo mismo se aplica a los sistemas de reconocimiento vocal y de la forma de andar y otros sistemas biométricos.

Si bien un índice de precisión del 99% puede parecer bueno en general, se trata de un riesgo considerable cuando pueda llevar a sospechar de una persona inocente. Incluso un porcentaje de error del 0,1% es alto si afecta a decenas de miles de personas.

Todos los **sistemas de reconocimiento emocional y categorización biométrica estarán siempre sujetos a requisitos específicos de transparencia**. También se considerarán aplicaciones de alto riesgo si entran en los casos de uso definidos como tales, por ejemplo en los ámbitos del empleo, la educación, la aplicación de la ley, la migración y el control de fronteras.

Por último, el «**Reglamento sobre máquinas**» dispone que la nueva generación de maquinaria deberá garantizar la seguridad de los usuarios y consumidores, sin menoscabo de la innovación. Esto incluye una amplia gama de productos de consumo y profesionales, desde robots hasta cortadoras de césped, impresoras 3D, máquinas de construcción y líneas de producción industrial.

En cuanto a la implementación del nuevo marco legal, el Parlamento Europeo y los Estados miembros tendrán que adoptar las propuestas de la Comisión sobre un planteamiento europeo en materia de inteligencia artificial y de maquinaria en el procedimiento legislativo ordinario. Una vez adoptados, los Reglamentos definitivos serán directamente aplicables en toda la UE.

Trabajo y derechos digitales

«No regulamos plataformas sino derechos»

España se ha situado a la cabeza de la UE en el reconocimiento de los derechos laborales de las personas que trabajan en redes de reparto de plataformas digitales. El Ministerio de Trabajo ha presentado el Acuerdo Social que regula la relación de los «riders» con sus empleadores.

La Ministra de Trabajo, Yolanda Díaz explicó una de las claves introducidas en el Estatuto de los Trabajadores directamente relacionada con los derechos digitales en el ámbito laboral. El artículo 64 establece la obligación de informar sobre la fórmula matemática o algorítmica que afecta a la relación laboral, «no solo de las personas dedicadas al reparto sino en todos los puestos de trabajo vinculados a plataformas».

De esta forma se pretenden neutralizar los «**castigos algorítmicos**, que se penalice por rendimientos, interpretados de forma sesgada, o por desarrollar una huelga» ha detallado Díaz. «**No regulamos plataformas sino derechos**».

Este nuevo marco revela el creciente interés por limitar situaciones de discriminación provocadas por la intervención de sistemas automáticos. El control de los algoritmos que afectan a la distribución de trabajo es un primer paso, y con alta probabilidad el anuncio de lo que está por venir con la transformación digital del trabajo.

Sin entrar en el tipo de relación entre el trabajador y la empresa, el Parlamento Europeo ha pedido a la Comisión el desarrollo de una ley que otorgue el derecho a desconectarse digitalmente del trabajo. Los eurodiputados creen necesario el desarrollo de una legislación a nivel europeo que defina los requisitos mínimos para el trabajo en remoto, horarios, periodos de descanso y condiciones de trabajo.

No podemos abandonar a millones de trabajadores europeos que están agotados por la presión de estar siempre «activos» y jornadas laborales excesivamente largas. Es hora de actualizar los derechos de los trabajadores para que se correspondan con las nuevas realidades de la era digital. Alex Agius Saliba, ponente de la iniciativa legislativa en el Parlamento de la UE (S&D)

La iniciativa legislativa ha contado con el respaldo de 472 votos, frente a 126 en contra y 83 abstenciones. Los eurodiputados consideran el **dere-**

cho a desconectarse como un derecho fundamental que permite a los trabajadores abstenerse de realizar tareas relacionadas con el trabajo, como llamadas telefónicas, correos electrónicos y otras comunicaciones digitales, fuera del horario laboral. Así mismo, animan a los Estados miembros a tomar todas las medidas necesarias para permitir que los trabajadores ejerzan este derecho.

Una investigación de Eurofound, *Fundación Europea para la Mejora de las Condiciones de Vida y de Trabajo*, sobre trabajo digital (TICTM - Trabajo móvil basado en TICs) muestra que las personas que trabajan regularmente desde casa tienen más del doble de probabilidades de superar el máximo de 48 horas de trabajo por semana, en comparación con las que trabajan en las instalaciones de su empleador. Casi el 30% de los que trabajan desde casa informa que trabaja en su tiempo libre todos los días o varias veces a la semana, en comparación con menos del 5% de los trabajadores de oficina. Desde el estallido de la pandemia COVID-19, el trabajo desde casa ha aumentado en casi un 30%.

Un caso de estudio realizado en el sector bancario español destacó el impacto positivo del TICTM en el equilibrio entre la vida laboral y personal. Cuando los empleados trabajan en remoto, suelen hacerlo por la tarde y, en menor medida, por la noche, en lugar de en el horario laboral principal, sobre todo si tienen que atender necesidades familiares. Las modalidades TICTM dan a los empleados mayor autonomía para organizar su horario según sus propias necesidades cuando trabajan fuera de los locales del banco. Para garantizarlo, la política de la empresa pretende evitar que los directivos actúen de forma que puedan socavar la autonomía de los empleados, por ejemplo, fijando cuándo deben estar disponibles o estableciendo reuniones innecesarias.

Esta apreciación coincide con el decálogo Hermes para el trabajo digital elaborado por la fundación en que se recoge, entre otros la organización del trabajo digital por objetivos y no por tiempos, primando la autonomía de los equipos.

Decálogo Hermes para la digitalización



Digitalizar una empresa es

Aumentar la **productividad** mediante la transformación de los **procesos** de trabajo y producción utilizando **herramientas digitales**.

El sujeto es el equipo

Tanto del **aprendizaje** como del trabajo digital. No el individuo.

El trabajo digital se organiza por objetivos

No por tiempos. La productividad no es el resultado de una matriz de tiempos diarios de navegación y de uso de programas/aplicaciones.

El trabajador digital es autónomo

Su remuneración paga su aporte al equipo, dado el **cumplimiento de resultados colectivos**, no su tiempo de trabajo.

El equipo es responsable de su rendimiento

Precisa de sistemas de **autoevaluación** y **autonomía** en el reparto interno de incentivos y en la selección de proveedores.

La coordinación entre

funciones/equipos exige ciertas dosis de **presencialidad** que corresponde organizar a la empresa.

Las necesidades de formación

deben ser **detectadas y reportadas por los equipos**. La empresa debe responder con la adjudicación de un presupuesto.

La relación con los clientes

debe seguir unos estándares fijados por la empresa en cuanto a **formas, herramientas, criterios de seguridad**; y en cuanto a objetivos y resultados.

Proveedores y clientes

de la empresa deben de participar de los sistemas de evaluación.

Digitalizar no es hacer mudanza de espacios

Es **personalizar** las **funciones** en los equipos y **transformar** los **procedimientos en sistemas** de determinación de **objetivos**.

Precisamente en España, banca y sindicatos firmaron el convenio colectivo del sector que establece, entre otras, las condiciones de uso de la Inteligencia Artificial en los entornos de trabajo con el objetivo de evitar que las entidades tomen decisiones sobre el empleado basadas solo en algoritmos. En el artículo 80 del convenio, relativo a los derechos

digitales y la transformación digital, se regula el derecho a la educación digital y el derecho ante la inteligencia artificial. La empresa deberá informar sobre el uso de analítica de datos o sistemas de inteligencia artificial cuando la toma de decisiones en recursos humanos y relaciones laborales se basen exclusivamente en modelos digitales sin intervención humana. Como mínimo, de los datos que nutren los algoritmos, la lógica de funcionamiento y la evaluación de los resultados.

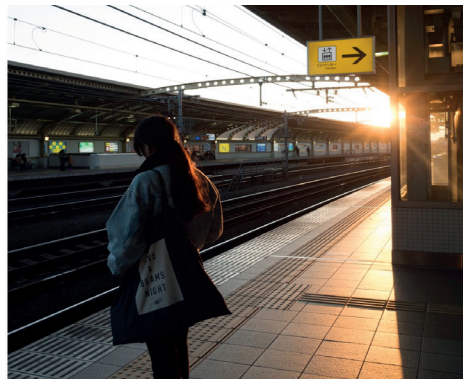
También reconoce el derecho a la desconexión digital, el derecho de intimidad en el uso de dispositivos móviles y el derecho a la intimidad frente al uso de dispositivos de vídeo-vigilancia, grabaciones de sonidos y geolocalización en el ámbito laboral.

Lo cierto es que nunca se ha hablado tanto del trabajo como en los últimos meses, las áreas de recursos humanos muestran su preocupación ante la necesidad de suplir los intangibles que la presencialidad genera para la organización. Se ensayan fórmulas de pertenencia que van desde la organización de cafés virtuales a la instalación de canales musicales para expresar el estado de ánimo.

Entre los empleados, se suceden las anécdotas de reuniones en pijama y las ponderaciones de esta nueva experiencia que difumina las fronteras entre la *vida* y el trabajo. En Japón, la compañía de seguros Dai-ichi Life Insurance cosechó un récord histórico en su edición del concurso de *haikus*, donde el trabajo digital fue el tema estrella.

*Voy a trabajar,
solo un fusuma de distancia,
teletrabajo.*

*No termina
porque no hay últimos trenes,
dink party en Zoom.*



Neuroderechos: Chile aprueba el proyecto de ley que regulará los Neuroderechos

La Comisión del Futuro del Senado aprobó por unanimidad la reforma constitucional para proteger «la integridad mental de las neurotecnologías». En una histórica votación, el 13 de abril la Comisión presidida por el senador Guido Girardi, aprobó el proyecto de reforma constitucional que modifica el artículo 19, número 1°, de la Carta Fundamental «para proteger la integridad y la indemnidad mental con relación al avance de las neurotecnologías».

La iniciativa de reforma constitucional, junto al proyecto de ley sobre protección de los neuroderechos y la integridad mental (también en trámite en el Senado) son inéditas en el mundo. Durante la votación estuvo presente Rafael Yuste, miembro de Hermes, coautor de la normativa y coordinador del proyecto BRAIN e impulsor de «Neurorights Initiative» una red que promueve los neuroderechos a nivel internacional y de la cual el Instituto Hermes forma parte.

Las expectativas sobre la nueva regulación chilena han llegado hasta la industria del cine, Werner Herzog, ha anunciado la realización de un documental sobre Neuroderechos y su tramitación en el Congreso Nacional de Chile.

Este es un proyecto que desafía el futuro y plantea ir por delante de los problemas y no detrás de ellos, cuando ya es casi imposible regularlos. Guido Girardi

Para el senador Juan Antonio Coloma la próxima ley afecta *al más relevante de todos los artículos, que es el derecho a la vida. Le confiere a la integridad física y psíquica un desarrollo y sobre todo un sentido de respeto permanente en función de lo que es persona humana.*

El profesor Yuste afirmó que este es un proyecto ejemplar tanto en el fondo como en la forma; cumple con el objetivo de proteger al cerebro, y, es producto de un amplio consenso.

En el momento en que culmine el proceso, Chile se convertirá en el primer país cuya constitución *protege la actividad cerebral, la información y la integridad mental.* Por el momento, el nuevo artículo estipula que:

El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la actividad física y psíquica. La ley regulará los requisitos y condiciones para su utilización en las personas, debiendo propender especialmente, al resguardo de la actividad cerebral, así como la información proveniente de ella.

Datos Abiertos

Las propuestas presentadas por el Parlamento a la Comisión Europea en materia de datos incluyen la creación de nueve espacios comunes en sectores como la sanidad, la agricultura y la energía y el fomento de un mayor intercambio de datos industriales.

Bajo esta propuesta reside la idea de que la incorporación de sistemas digitalizados a la producción y a los servicios precisa de un ingente volumen de datos que sólo será posible alcanzar mediante la cooperativización a nivel europeo de los datos generados por los ciudadanos en sus interacciones con agentes públicos y privados. La apuesta europea por la soberanía tecnológica ha servido de catalizador para el impulso de esta iniciativa. China y EEUU llevan cuerpos de ventaja en sistemas de inteligencia artificial o desarrollos en la nube, lo mismo ocurre con los motores eléctricos, los sistemas de conducción automatizada o de control de suministros eléctricos.



Para apoyar el establecimiento de tales espacios, la Comisión espera avanzar en la «Ley de Gobernanza de Datos» propuesta el año pasado, que tiene como objetivo proporcionar el marco para fomentar un mayor intercambio de datos dentro de la Unión.

Y en paralelo, la creación de una infraestructura de datos soberana y segura a través **el proyecto GAIA-X**. Sin embargo, la iniciativa se ha dado de bruces con la burocracia europea; El diseño de implementación de Gaia-X establecía que corporaciones europeas asentadas, Deutsche Telecom, Telefónica, SAP, la gestora de datos francesa Atos..., trabajaran con empresas emergentes en la creación de un estándar de proceso y gestión de datos asegurando la protección y el intercambio aplicando software libre.

En la práctica el mero hecho de constituir la empresa inicial involucró a 22 empresas y precisaba de la intervención de la Comisión Europea. Además de contar con la asesoría de consultoras de gestión y despachos de abogados. Tras una larga travesía de trámites administrativos «**Gaia-X Association internationale sans but lucratif**» -Gaia-X AISBL, por sus siglas- se inscribió en el registro comercial de Bélgica el 1 de febrero de 2021.

Las empresas se quejan de la lentitud, **aún no se ha escrito una línea de código** y ni siquiera se han definido las especificaciones que regirán el desarrollo de productos específicos y los tiempos apremian.

A escala país un ejemplo de explotación de datos cooperativizados es el proyecto **Datadis** impulsado por la **Asociación Española de Empresas Eléctricas (ASEME)**. A través de una plataforma web se ofrece a cualquier usuario identificado el acceso a informes predefinidos de energía, por ejemplo, número de contratos por comunidad y tarifas; y solicitudes de información procesada bajo consulta en función de los parámetros particulares de interés geográfico, de suministro o temporal.

Alemania, con su nueva Ley de Datos Abiertos regula la obligación de proporcionar datos abiertos a la administración federal

Amplía la gama de datos federales abiertos a instituciones y corporaciones de derecho público. De este modo, la Ley de uso de datos crea condiciones de uso uniformes y no discriminatorias para los datos del sector público. En el futuro, los datos de proyectos de investigación con participación de la administración federal también estarán disponibles como datos abiertos.

Fuentes del Ministerio de Economía y Energía (BMWi) explicaban que «los datos abiertos son datos abiertos», es decir, datos brutos de la administración a los que se puede acceder libremente a través de Internet y no son personales. En la actualidad son la base de muchos proyectos de datos, por ejemplo, el «Atlas de accidentes de Alemania», que pueden consultar ciudadanos y gestores de tráfico para identificar puntos críticos.

Esta Ley viene a reemplazar a la de reutilización de información, garantiza las mismas condiciones de uso para todos los actores y extiende por primera vez su alcance a las empresas públicas (agua, transporte, energía). Elaborada para facilitar el desarrollo de de inteligencia artificial, la provisión de datos dinámicos permitirá, más adelante, su uso en tiempo real.

Los datos son un recurso esencial para crear nuevos valores y productos competitivos. Con la Ley de Uso de Datos, estamos dando el siguiente paso en datos abiertos y creando una mejor base para modelos comerciales innovadores basados en datos. Sobre todo, queremos apoyar el desarrollo y uso de aplicaciones de Inteligencia Artificial. Para alcanzar un futuro con vehículos autónomos, ciudades en red y sistemas inteligentes de gestión de energía, es esencial que permitamos que los datos que tenemos estén disponibles y los usemos lo mejor posible.



Thomas Jarzombek, representante de BMWi para la economía digital y las empresas emergentes

La Secretaría de Estado del Ministerio del Interior ha mostrado públicamente su respaldo a la iniciativa de datos abiertos. Su titular, Markus Richter defiende que los datos han de estar disponibles gratuitamente para la sociedad, la ciencia y la investigación.

Con los datos abiertos promovemos la innovación, aumentamos la eficiencia y allanamos el camino para los modelos comerciales digitales.

El marco legal de protección de datos de la UE no se interpone en el camino del desarrollo de la economía de datos

El Supervisor Europeo de Protección de Datos (EDPB) y el Comité Europeo de Protección de Datos han emitido un dictamen conjunto sobre la Ley de Gobernanza de Datos (DGA). Consideran imprescindible que en la redacción de la DGA se recoja de forma «clara e inequívoca» que no se verán afectados el nivel de protección de los datos personales, los derechos de las personas y las obligaciones establecidas en la actual legislación sobre protección de datos.

En cuanto a la reutilización de datos personales en poder de organismos del sector público, recomiendan alinear la DGA con las normas existentes sobre protección de datos personales establecidas en el RGPD y con la Directiva de Datos Abiertos. Además, debe aclararse que la reutilización de datos personales en poder de organismos del sector público solo puede permitirse si se basa en la legislación de la UE o de los Estados miembros.

Sobre los proveedores de servicios de intercambio de datos, el dictamen conjunto destaca la necesidad de garantizar la información previa a las personas, teniendo en cuenta los principios de protección de datos desde el diseño de los sistemas y, por defecto, la transparencia y la limitación de la finalidad.

«El marco legal de protección de datos de la UE no se interpone en el camino del desarrollo de la economía de datos. Todo lo contrario, lo permite», asegura el presidente del EDPB.

Por su parte, el ejecutivo de la UE está llevando a cabo una consulta pública sobre la publicidad de contenidos políticos en el marco del Plan de Acción para la Democracia Europea. Una de las líneas de acción de este programa es que las campañas políticas digitales sean justas y abiertas, y que apoyen, no debiliten, los derechos fundamentales de los ciudadanos para formar libremente sus opiniones políticas. En el horizonte está la redacción de una propuesta legislativa sobre información patrocinada, medidas de apoyo y orientación a Estados miembros, partidos

políticos y autoridades competentes. Una de las cuestiones a valorar es la prohibición del «microtargeting» bajo determinadas circunstancias. La evaluación de impacto inicial contiene tres posibles opciones para abordar esta cuestión:

1. **Medidas de «soft law»** basadas en iniciativas existentes y nuevas herramientas como códigos de conducta para partidos políticos, campañas de información, recomendaciones y promoción de acciones voluntarias de transparencia.
2. **Legislación específica** que establece estándares mínimos obligatorios para la transparencia, el acceso y la divulgación de datos para facilitar el cumplimiento, los arreglos extrajudiciales y el etiquetado de anuncios políticos.
3. **Legislación que armoniza condiciones y criterios específicos** en el contexto de la publicidad política que establece reglas comunes sobre financiación, moderación de contenidos y correulación.

Aunque el compendio de respuestas se dará a conocer en las próximas semanas, aportaciones de organizaciones de la sociedad civil como el Center for Democracy & Technology Europe (CDT Europe) y la Stiftung Neue Verantwortung (SNV) coinciden en la necesidad de implementar mecanismos de transparencia para señalar contenido político patrocinado y de definir aquellos actores cuya comunicación siempre se considera política, por ejemplo: partidos políticos, candidatos, grupos parlamentarios, asociaciones de lobby... etc. También apuntan a la creación de un registro público de libre acceso para consultas de contenidos promocionados y anuncios realizados en las plataformas online.

Identidad Digital

En las últimas semanas tres países de nuestro entorno han anunciado avances sustanciales en sus sistemas de identidad con el fin de establecer mecanismos de identificación digital seguros.



Italia: Protección al menor

El gobierno italiano está analizando una propuesta para establecer un marco de seguridad para los menores en Internet. Pretende ampliar el «Sistema Público de Identidad Digital (SPID)» y establecer un mecanismo efectivo de supervisión de la actividad y acceso de los menores a sitios web, servicios online y plataformas de redes sociales.

En su planteamiento de trabajo, el Ministerio de Innovación Tecnológica, ha solicitado la colaboración de las principales plataformas digitales en la elaboración del proyecto.

La iniciativa, en parte, es la respuesta al aumento de accidentes entre los menores durante su «vida» en las redes sociales. En Italia una niña de 10 años murió al intentar un «**desafío de asfixia**» en TikTok. La aplicación del sistema SPID permitirá a padres y personas a cargo supervisar su registro en servicios online.

Aunque muchas de las plataformas imponen restricciones de edad en su acceso, no realizan una comprobación de la información introducida. En la práctica no es más que una medida cosmética que reduce la posibilidad de ser sometidas a demandas legales.

Internet no puede considerarse un no lugar. Claramente, es necesaria la colaboración de las plataformas sociales, que deben adaptar sus sistemas permitiendo el acceso a los menores solo si tienen una identidad digital a partir de la cual puedan rastrear su edad. Paola Pisano, Ministra de Innovación Tecnológica.

Los tutores también recibirán notificaciones relacionadas con la navegación, comunicando solicitudes de acceso a sitios para mayores de edad, o de contenido dañino o peligroso para un menor.

En la práctica, uno de los progenitores iniciaría una solicitud, declarando su relación con el menor y sus datos de nacimiento, entre otros. A continuación recibirá y deberá activar un SPID especial, anónimo, asociado a su identidad.

La propuesta deberá contar con la aprobación de la Autoridad Italiana de Protección de Datos y la Autoridad Garante de la Infancia y la Adolescencia antes de ser implementada.



Alemania: Seguridad de datos y DNI digital

Entre las propuestas legislativas aprobadas por el gobierno federal para la digitalización de la economía, la sociedad y la administración se encuentra la regulación de la identidad y la garantía de la privacidad en el entorno digital.

El gobierno de Alemania ha querido ir un paso por delante en la identificación digital y ha aprobado el desarrollo de un sistema de identificación electrónica sobre dispositivos móviles. A partir del próximo otoño, los ciudadanos podrán llevar su ID oficial en sus teléfonos, lo que les permitirá identificarse sin necesidad de portar un documento.

El proyecto de «ID móvil» ha sido presentado por el Ministerio Federal de Interior como un impulso a la transformación digital de la economía y de la soberanía de los usuarios.

Además, el Ministerio Federal de Economía y Energía (BMWí) ha lanzado el proyecto «Identidades Digitales Seguras». Thomas Jarzombek, representante del BMWí para la economía digital y las empresas emergentes se pronunciaba así,

Las plataformas estadounidenses están introduciendo cada vez más soluciones de identificación en el mercado. Creo que es importante que exista una opción de identificación asegurada por el estado en el teléfono inteligente, especialmente que funcione sin intenciones comerciales ocultas con respecto a los datos del usuario. En el pasado, los proyectos estatales han mostrado muy poca orientación al usuario y eran demasiado complicados. En particular, tenemos que crear una oferta que también sea utilizada por las empresas y que tenga un lugar permanente en la vida cotidiana de las personas. En este caso, el nuevo programa es significativamente mejor que las iniciativas anteriores.

Jarzombek hace referencia a un programa novedoso en el ámbito público, la apertura a terceras partes para el desarrollo de soluciones y servicios de identidad digital segura. El Ministerio reconoce que las identidades digitales son un pilar fundamental para la soberanía digital de Alemania y Europa. Habilitar una solución segura y fácil de usar supondría simplificar las relaciones con la administración, reducir la presencialidad y al mismo tiempo, potenciar los servicios comerciales con plenas garantías para los usuarios.

Está previsto el desarrollo de cuatro proyectos, el primero de ellos, IDunion tiene como finalidad la implementación de aplicaciones en las áreas de administración electrónica, educación, finanzas, industria, Internet de las Cosas, comercio electrónico, movilidad y salud. Para su ejecución se constituirá una cooperativa europea y se dotará con 15,6 millones de euros.

La identidad es una expresión de nuestra autodeterminación. Ponemos un gran esfuerzo en proteger a los ciudadanos de los abusos y al mismo tiempo, posibilitar transacciones comerciales dentro del marco de la legalidad. La Smart eID Act supone un salto cualitativo para los modelos de negocio en Internet y la comunicación digital con la administración.

Markus Richter, Secretario de Estado del Ministerio Federal de Interior y Comisionado del Gobierno Federal para Tecnologías de la Información .

El Ministerio Federal de Economía y Energía (BMWí) también ha presentado un proyecto de ley que regula la protección de datos y la protección

de la privacidad en las telecomunicaciones, con el objetivo de aportar claridad jurídica para la protección de datos y la protección de la privacidad en el mundo digital. La ley, conocida por sus siglas, TTDGS, vendría a garantizar un equilibrio justo entre los intereses de los usuarios de los servicios digitales y los intereses de las empresas, según un comunicado oficial del propio Ministerio.



Francia: Nuevo DNI Digital

En el mes de marzo, Francia estrenó DNI electrónico. En una primera etapa, a modo de piloto, se podrá utilizar en el departamento de Oise, y se espera que a partir de agosto pase a estar operativo en todo el país. Se trata de una tarjeta física que incorpora un chip que permite almacenar datos biométricos -en una primera fase, dos huellas dactilares- los datos personales y la firma del ciudadano. También incluye foto.

Según el Ministerio del Interior: «el DNIE protegerá a la población contra el robo de identidad», y sigue las directrices marcadas por la Comisión en el Reglamento Europeo para la Identificación Electrónica y los Servicios de Confianza. Sin embargo, el nuevo documento francés no permite identificarse ante administraciones públicas de otros países de la Unión, una decisión política para tranquilizar a los franceses sobre el uso de datos.

La Comisión Nacional de Informática y Libertades (CNIL) ha manifestado su disconformidad ya que deseaba hacer recomendaciones sobre el almacenamiento y la protección de los datos personales.



Presidencia Portuguesa de la UE: Reglamento ePrivacy

Uno de los puntos del programa de la presidencia portuguesa de la UE es la revisión del reglamento **ePrivacy**, relativo a la privacidad electrónica.

El reglamento de ePrivacy detalla las condiciones bajo las cuales los proveedores de servicios pueden procesar datos de comunicaciones electrónicas. Dichos datos incluyen los transmitidos en el uso de servicios en línea, incluidos los mensajes enviados en WhatsApp y las vídeo-llamadas en plataformas como Zoom o Skype.

La propuesta de Portugal es que el procesamiento de datos almacenados en el equipo terminal de los usuarios finales se pueda permitir, con consentimiento, solo si la información finalmente se convierte en anónima. Es decir, si el procesamiento se «limita a información que está seudonimizada», y si la información o los datos no son posteriormente utilizados para crear un perfil del usuario.

El Comité Europeo de Protección de Datos emitió a su vez un comunicado en el que sostiene que el Reglamento debería hacer hincapié en el papel de la anonimización como garantía fundamental y que como tal, debe ser favorecida cuando se utilizan datos de comunicaciones electrónicas. Así mismo, defiende el cifrado de extremo a extremo, del remitente al destinatario, como única manera de garantizar la plena protección de los datos en tránsito. En este sentido, afirma que cualquier intento de suprimir el cifrado, incluso con fines de seguridad nacional, privaría por completo de estos mecanismos de protección debido a su posible uso ilícito.

La propuesta inicial de la Comisión para el Reglamento de privacidad electrónica se presentó en enero de 2017, en un intento por «reforzar la confianza y la seguridad en el mercado único digital».

Monedas digitales soberanas



El Euro Digital

En un seminario organizado por Bruegel, Fabio Panetta, miembro del Comité Ejecutivo del Banco Central Europeo, anunció que el BCE está considerando la posibilidad de emitir un euro digital. Esta decisión permitiría a la entidad innovar y ofrecer al público «dinero soberano en formato digital». A diferencia de otros medios de pago, sería un derecho frente al Banco Central en lugar de un derecho frente a un banco privado intermediario.

Para el organismo, un euro digital representa una evolución natural en línea con la transformación tecnológica, «no sólo para apuntalar la eficiencia y la innovación, sino también para preservar el papel del Banco Central a la hora de ofrecer medios de pago seguros».

Para conocer el pulso de la sociedad a este respecto, el BCE ha organizado una consulta pública. El análisis de las respuestas se dará a conocer en esta primavera. Como es lógico, en paralelo se están analizando las implicaciones económicas, financieras y sociales de la emisión de un euro digital.

Panetta compartió el contenido de algunas de las discusiones sobre los principales efectos sobre la estabilidad financiera y el sistema financiero internacional.

Beneficios asociados a la digitalización de servicios financieros

Entre los factores a tener en cuenta, estarían:

- Aumento del número de proveedores de tecnologías y productos innovadores.
- Cambio en las preferencias en los pagos minoristas con una disminución del uso de efectivo (en aceleración por la pandemia)
- Riesgos asociados a los derechos digitales:
 - Los gigantes tecnológicos (GAFA y BAT) están marcando el ritmo también en los servicios financieros. «Buscan eludir las redes de distribución tradicionales, incluidos los sistemas de pago, a través de su control de las redes sociales, de los mercados on line y de las tecnologías móviles».
 - Los modelos basados en datos ponen en peligro la privacidad con riesgo de uso indebido de información personal.
 - La integración de servicios financieros por parte de las tecnológicas puede reducir la competencia, limitando la elección del consumidor.
 - Se podría generar dependencia de empresas tecnológicas ajenas al espacio europeo y depender de «tecnologías gobernadas en otros lugares».
- Posible absorción por parte de las tecnológicas de monedas estables, que podría crear riesgos sistémicos e incluso poner en peligro la soberanía monetaria.

Una respuesta a las tendencias identificadas podría ser que los bancos centrales se vuelvan digitales para «preservar el dinero como bien público».

Estaría diseñado para ser seguro, sin costo, de fácil acceso y simple de usar, apoyando así la inclusión financiera. Tendría la protección de la privacidad como una prioridad clave, ayudando así a mantener la confianza en los pagos.

El BCE ya ha analizado aspectos técnicos y de seguridad, si bien esta labor continuará en los próximos meses. El objetivo sería hacer interoperable un euro digital con las soluciones de pago privadas, para que se pueda acceder a él a través de ellas.

Posibles efectos injustificados en el sistema financiero

Se han planteado varias cuestiones relativas al impacto potencial de la introducción de un euro digital en el sistema financiero. Algunas de ellas

fueron recogidas durante el periodo de consulta pública, y, estando aún pendientes de su publicación final, el BCE ha adelantado que una de ellas, paradójicamente, estaría relacionada con un éxito del euro digital por encima de lo esperado.

El regulador bancario ha expresado su temor ante la posibilidad de que sus principales fortalezas -seguridad y liquidez- puedan operar en contra de la estabilidad monetaria si su diseño no fuera el adecuado. Considerados sus efectos uno a uno, entrarían a evaluar:

1. Efectos sobre la intermediación financiera y la asignación de capital en tiempos normales

Más allá de las adaptaciones de diseño, el pensamiento económico sobre el posible impacto de un euro digital en la intermediación financiera no está claro.

El BCE no tiene previsto interactuar directamente con los usuarios potenciales del euro digital. Su función estaría más orientada a proporcionar «dinero seguro», mientras que los intermediarios financieros continuarían ofreciendo servicios a los usuarios.

Una consideración adicional es que un euro digital podría «mejorar la asignación de capital al facilitar el acceso a los pagos y reducir los costes de transacción».

2. Efectos potenciales en tiempos de crisis

La emisión de un euro digital en tiempos de crisis conlleva riesgos más pronunciados para la intermediación financiera.

Se podría desencadenar una corriente de «digital runs» de los bancos comerciales al Banco Central. Llevaría a los ahorradores a reducir sus depósitos bancarios y también a aumentar la volatilidad en tiempos normales. No obstante, un euro digital podría proporcionar herramientas adicionales para contrarrestar estos riesgos para la estabilidad financiera.

Con todo, no se puede descartar el riesgo de que un euro digital genere efectos adversos en tiempos de crisis.

3. Impacto en el sistema monetario internacional

El euro digital también podría tener un impacto en el sistema financiero a nivel transfronterizo, dependiendo de si se permite el acceso a no residentes y se autoriza la interoperabilidad con sistemas de pago distintos al euro.

«Un euro digital accesible a los no residentes podría hacer que la moneda única sea más atractiva como medio de pago seguro para las transacciones minoristas transfronterizas» facilitando operaciones de pagos, transferencias de remesas... etc.

Al mismo tiempo, un euro digital muy líquido puede hacer que los inversores extranjeros lo utilicen de manera desproporcionada, alterando los reequilibrios ante perturbaciones financieras. Investigaciones recientes sugieren que en presencia de una «CBDC o Central Bank Digital Currency», los «shocks podrían generar mayores fluctuaciones del tipo de cambio y tener un efecto más fuerte en las condiciones financieras externas».

Por otro lado, la ausencia de un euro digital podría hacer que Europa sea más vulnerable a los desarrollos internacionales: la adopción generalizada de monedas digitales por parte de los bancos centrales extranjeros podría hacer que la economía y el sistema financiero europeos sean más sensibles a las perturbaciones del exterior.

4. Diseño y políticas

El BCE ha puesto en marcha un grupo operativo para estudiar el lanzamiento del euro digital. La decisión final al respecto será tomada una vez analizados todos los aspectos comentados anteriormente.

Por otro lado, el diseño que se adopte deberá garantizar la privacidad en los pagos digitales, la inclusión financiera y el acceso universal.

Un euro digital debería ser un medio de pago eficaz, tanto a nivel nacional como internacional. Pero, fundamentalmente, para preservar la estabilidad, debe diseñarse de manera que evite que se utilice como una forma de inversión.

Para lograrlo, una opción podría ser limitar la cantidad de euros digitales que pueden poseer los usuarios individuales. Por ejemplo, permitiendo el uso combinado de euro digital y dinero privado.

Otra sería fijar un límite para la tenencia de euros digitales a partir del cual se aplica una «penalización». Hasta ese umbral, los importes mantenidos en euros digitales nunca estarían sujetos a tipos de interés negativos y, por tanto, nunca recibirían un trato menos favorable que el efectivo.

Son aún muchas las incógnitas a resolver, pero el camino está abierto. Desde el BCE sostienen el compromiso de incorporar opiniones y aportes de ciudadanos, bancos, organizaciones y partes interesadas para garantizar que el euro digital se diseña de manera óptima para que «sirva a los europeos».



China: divisa digital soberana

El Banco Popular de China, comenzó a mediados de 2020 las pruebas de su moneda digital en dos áreas específicas del país, allanando el terreno para convertirse en el primero en establecer un sistema nacional de pago electrónico.

Durante la última cumbre virtual del G7 los Ministros de Finanzas se mostraron cautelosos ante el liderazgo de China en la emisión de moneda digital soberana, ya que, a largo plazo podría suponer una amenaza para las posiciones internacionales de sus propias monedas.

China aparentemente ha estado sentando las bases para crear una zona económica con sus participantes en el proyecto **Belt and Road**, de refuerzo de las redes de infraestructura en Asia, Oriente Medio, Europa y África, donde el yuan digital se usaría como moneda común de liquidación.

Takahide Kiuchi, economista ejecutivo del Nomura Research Institute en Tokio, declaraba durante la cumbre que el yuan podría volverse tan influyente como el dólar en todo el mundo si el intento de China de internacionalizar su moneda se consolida con éxito:

Si la internacionalización del yuan avanza de manera constante, el panorama competitivo del dólar y el yuan cambiaría drásticamente.

Fuentes diplomáticas de delegaciones del sudeste asiático fueron aún más categóricos ante la maniobra de China. Con un alto grado de escepticismo aseguraban que mientras el gobierno chino «liderado por comunistas» sea el administrador del yuan, la moneda no servirá como medio de pago global.

Debe renunciar a su sistema de tasa flotante administrado por el Banco Central que controla el Partido Comunista. Es un dilema para China.

China propone un conjunto de reglas globales a los bancos centrales para regular las monedas digitales

Sin atender a las suspicacias de sus vecinos de zona, China ha seguido avanzando en el despliegue del yuan digital. Semanas antes de la cumbre virtual, el **Banco Central Chino** comunicó a bancos centrales y autoridades monetarias un conjunto de reglas globales para regular las monedas digitales, establecer sistemas comunes de vigilancia y seguridad, y habilitar la interoperabilidad entre CBDC (Central Bank Digital Currency).

La adopción de normas comunes permitiría a los supervisores monitorizar los flujos de transacciones y verificar el cumplimiento de las legislaciones. Y sobre todo, contribuiría al mantenimiento de la soberanía de los bancos centrales frente a la emisión de monedas por operadores privados.

El director del Instituto de Monedas Digitales, Mu Changchun, comunicó esta propuesta en un evento organizado por el Banco de Pagos Internacionales (BPI) celebrado a finales del mes de marzo. En declaraciones de Mu, el «suministro justo de monedas digitales» de los bancos centrales debería ser una regla mundial.

Una moneda digital emitida por un banco central no debería afectar a la capacidad de otro banco central para cumplir con su mandato de estabilidad monetaria y financiera.

Los bancos centrales de Emiratos Árabes Unidos, Tailandia y Hong Kong han anunciado su cooperación para comenzar a realizar pruebas con el Banco Central Chino.

La **administración Biden** ha mostrado su apoyo a la investigación sobre la viabilidad de un **dólar digital**. El presidente de la Reserva Federal de EEUU, Jeremy Powell, ha declarado que consideran el dólar digital un proyecto de alta prioridad, si bien aún no está prevista una fecha de emisión. La Secretaria del Tesoro de los Estados Unidos, Janet Yellen, defiende que un dólar virtual podría beneficiar a los millones de estadounidenses que no tienen una cuenta bancaria.

El Banco de Japón comienza la primera fase del experimento sobre la moneda digital del banco central

Por su parte, Japón hacía público el 5 de abril el inicio de un proyecto para contrastar las funciones básicas de una moneda digital controlada por el Banco Central.

El regulador probará durante un año la emisión, distribución y canje de una moneda digital, entre otras, en tres etapas hasta marzo de 2022. En la primera fase se analizarán aspectos técnicos relacionados con la seguridad y el anonimato.

Con independencia de los resultados, las autoridades del banco central han aclarado que no está entre sus prioridades avanzar en la implementación de una moneda digital, aunque ven imprescindible «prepararse para responder» a posibles cambios.

En un editorial histórico a finales de año, el «Mainichi Shibun» ya había adelantado la posición del nuevo gobierno japonés en materia de digitalización. Ante la inexistencia de reglas internacionales sobre la transformación digital alertaba sobre un incremento de los temores ciudadanos ante los avances tecnológicos. Y no es precisamente Japón un país refractario a la tecnología. Sin embargo,

Los GAFAs y otros gigantes tecnológicos, incluido Alibaba, se han vuelto lo suficientemente poderosos como para predecir el comportamiento de los usuarios en función de los colosales volúmenes de datos personales que acumulan e incluso guiar su comportamiento.

Recordaba además que muchos países en un primer momento se habían opuesto al lanzamiento de la moneda digital de Facebook por considerarlo una amenaza para la soberanía monetaria. Y advertía de la imposibilidad de alcanzar una sociedad digital sólida si las superpotencias y los gigantes tecnológicos siguen por el camino de la supremacía y la priorización de sus propios intereses.

Finalizaba instando a EE.UU, China y Japón a desarrollar reglas y principios comunes, ya que, «la digitalización no es más que una herramienta para mejorar la sociedad».



«Bitcoin»

Visto el auge de bitcoin, el gobierno británico ha dado la orden de explorar la implantación de una libra digital. El proyecto, conocido como «Bitcoin», fue anunciado por el Ministro de Finanzas, Rishi Sunak.

El Banco de Inglaterra y el Tesoro trabajarán juntos para evaluar los beneficios de una moneda digital del Banco Central. Según Sunak, se trata de conseguir que el Reino Unido sea «más abierto, más ecológico y más avanzado tecnológicamente».

Si podemos capturar el extraordinario potencial de la tecnología, consolidaremos la posición del Reino Unido como el principal centro financiero del mundo.

En una posición similar a la del BCE, el Banco de Inglaterra propone que la moneda digital pueda ser utilizada por «familias y empresas» como complemento al dinero en efectivo y los depósitos bancarios, sin reemplazarlos. De cara a una futura implementación, los expertos sugieren que consumidores y empresas podrían tener directamente cuentas con el Banco Central.

Breves

Plan de digitalización España 2025

Entre 2020 y 2022 se movilizarán más de 70 mil millones de euros de inversión pública y privada. De ellos, 20 mil serán de inversión pública, 15 mil a cargo de los fondos Next Generation EU.

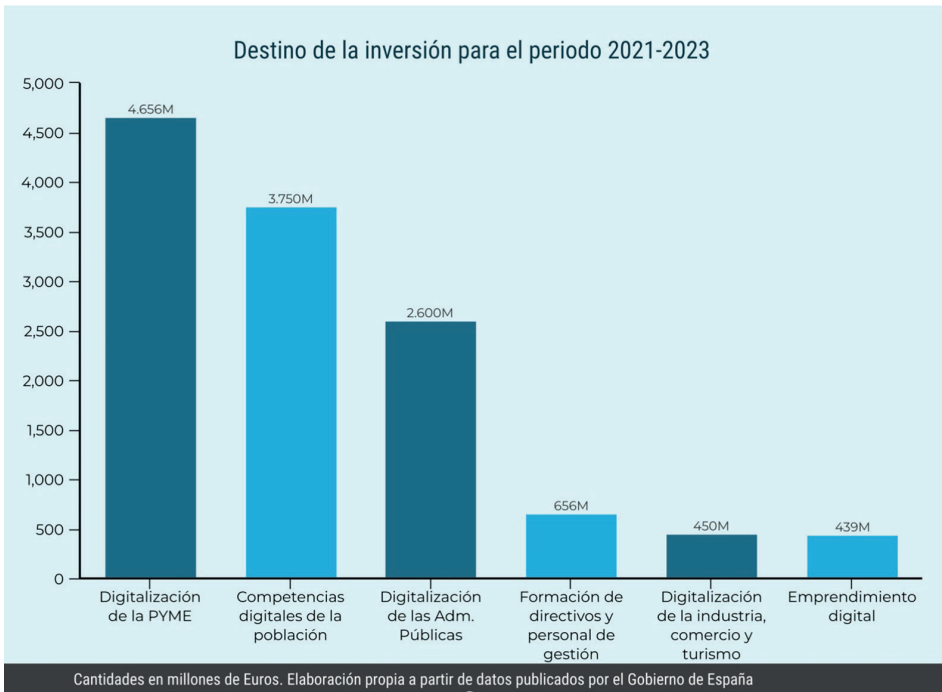
El programa España Digital incluye cerca de 50 medidas agrupadas en 10 ejes estratégicos que establecen objetivos a alcanzar en 2025:

1. **Conectividad digital:** Conseguir que el 100% de la población tenga cobertura de 100 Mbps, promoviendo el fin de la brecha digital entre zonas rurales y urbanas.
2. **Despliegue 5G:** Para preparar el 100 % del espectro radioeléctrico al 5G.
3. **Competencias digitales:** Con énfasis en trabajadores y conjunto de la ciudadanía. Teniendo en cuenta las necesidades del mercado laboral y la educación. Objetivo: que el 80% de las personas tengan competencias digitales básicas y que la mitad de ellas sean mujeres
4. **Ciberseguridad.** Se busca disponer de 20.000 especialistas en ciberseguridad, Inteligencia Artificial y datos en 2025 gracias, entre otros aspectos, al polo de actividad empresarial que supone el entorno del Instituto Nacional de Ciberseguridad (INCIBE).
5. **Digitalización de las Administraciones Públicas,** particularmente en ámbitos clave como el Empleo, la Justicia, o las Políticas Sociales. 50% de los servicios públicos disponibles a través de app móvil. Simplificación y personalización de la relación de ciudadanos y empresas con las Administraciones.
6. **Digitalización de las empresas,** con especial atención a las micropymes y a las start-ups. Como meta, que al menos el 25% del volumen de negocio de las pymes provenga del comercio electrónico.
7. **Digitalización del modelo productivo** mediante proyectos tractores de transformación digital en sectores estratégicos: Agroalimentario, Movilidad, Salud, Turismo, Comercio o Energía, entre otros. Estos proyectos tienen como meta una reducción del 10% de las emisiones de CO2 por efecto de la digitalización de la economía en 2025.
8. **Producción audiovisual:** Con una meta de incremento del 30% del volumen respecto a la producción actual.

9. Transición a la **economía del dato**, garantizando la seguridad y privacidad, aprovechando las oportunidades que ofrece la Inteligencia Artificial (meta 2025: 25% de empresas que usan IA y Big Data). Como medidas, incluye la creación de una **Oficina del Dato**, que será responsable de garantizar la buena gobernanza en el uso de los datos públicos; y potenciar un espacio ibérico, junto a Portugal, que impulse el desarrollo de **tecnologías avanzadas de computación de datos**.
10. **Garantizar los derechos en el nuevo entorno digital**, y en particular, los derechos laborales, de los consumidores, de los ciudadanos y de las empresas. En este ámbito se fija como objetivo la elaboración de una Carta de Derechos Digitales.

El gobierno creará el Consejo Consultivo para la Transformación Digital, para facilitar el diálogo y participación multisectorial de los agentes relevantes para la transición digital del país.

DESPLIEGUE



Atendiendo a estos 10 ejes, el presidente Sánchez anunció en los últimos días de enero una inversión total de **11.000 millones de euros hasta 2023** para mejorar las competencias digitales de la población, digitalizar las pequeñas y medianas empresas (pymes) e incidir en la transformación digital de la Administración, según ha explicado en una rueda de prensa virtual celebrada en La Moncloa.

Esto supone una sensible reducción en relación al diseño del programa, teniendo en cuenta que abarcaría a tres de los 10 ejes definidos, pero adelanta la consecución de los objetivos en dos años.

En este marco, el Instituto Hermes se ha centrado en transmitir una idea: **hay que medir el impacto en los derechos digitales de los proyectos de transición digital financiados con dinero público**. Para ello, hemos diseñado una metodología que utiliza 52 variables para clasificar y cuantificar el resultado de las diferentes dimensiones de un proyecto.

Además colaboramos con el ONTSI (Observatorio Nacional de Tecnología y Sociedad) dependiente del Ministerio de Asuntos Económicos y Transición Digital en elaborar un procedimiento «**Do No Significant Harm**».

La Comisión Europea aplica el principio de no causar daños significativos, «Do No Significant Harm» en la evaluación de proyectos para establecer un marco que facilite las inversiones sostenibles. Estableciendo los objetivos medioambientales sobre los que debe evaluarse la posible generación de daños significativos.

Siguiendo este modelo, nuestro objetivo es establecer un principio de «digital rights preserving». Así, de la misma forma que se mide el impacto de un proyecto en los 6 objetivos medioambientales, proponemos la creación de una taxonomía, que, siguiendo los derechos formulados en la *Carta de Derechos Digitales* permita asegurar que los proyectos vinculados a la digitalización no dañarán los derechos digitales de los ciudadanos.

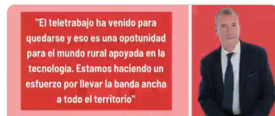
En el futuro inmediato, el «digital rights preserving» y los estudios de impacto sobre derechos de ciudadanía digital serán tan importantes en proyectos tecnológicos como lo son los de impacto medioambiental sobre los proyectos de infraestructuras.

Derechos Digitales y Reto Demográfico



“Sería ingenuo pensar que el mundo rural volverá a llenarse de gente gracias al teletrabajo. Pero sí puede significar un incremento de población en algunas zonas” #RetoDemográfico #ElRetoDeTodos

Entrevista a @Pacoboya en @aragonradio



En el curso de una entrevista radiofónica, Paco Boyas, Secretario de Estado para el Reto Demográfico se refería al impacto de la pandemia en la movilidad de las personas. Una cuestión que desde el Ministerio, afirma, les gustaría estudiar más a fondo.

A día de hoy si bien es cierto que el teletrabajo ha hecho plantearse a muchas familias su establecimiento en entornos rurales, esto no siempre es posible por la falta de conectividad en todos los puntos del territorio.

Sin embargo, Boyas afirmaba que el teletrabajo ha venido para quedarse y que eso es una oportunidad para el mundo rural apoyada en la tecnología. «Estamos haciendo un esfuerzo por llevar banda ancha a todo el territorio».

Pero, también trazó un techo, remarcando que puede suponer un incremento de población en algunas zonas, pero esto no significa que el «mundo rural vuelva a llenarse» gracias al teletrabajo.

A este respecto, el Gobierno ha autorizado la tramitación urgente de la **Ley General de Telecomunicaciones**. En el nuevo texto se incluye que las velocidades de acceso deben garantizar la prestación, de modo funcional, de servicios digitales esenciales. Entre ellos, mensajería instantánea, servicios de videoconferencias, correo electrónico, noticias y servicios financieros online.

Asimismo, para garantizar la **asequibilidad** y al mismo tiempo la capacidad de elección del usuario, se establece la posibilidad de que **el servicio universal pueda ser prestado por todos los operadores**. Hasta la fecha, el operador que garantizaba este servicio era Telefónica. Con la nueva Ley aplicará el mecanismo de licitación, mientras que hasta ahora sólo se acudía a este mecanismo si había varios interesados que así lo habían manifestado tras un proceso de consulta.

También introduce modificaciones para el refuerzo de los derechos de los usuarios protegiendo de un modo «más eficaz» los datos de carácter personal. Las compañías deberán dar más información a sus clientes sobre la información que almacenan a partir de sus registros de navegación -cookies- y amplía las garantías del consumidor con mejoras en las condiciones de portabilidad, entre otros.

Educación

El intento de mantener el ritmo de las clases en formato online durante la pandemia ha creado una gigantesca base de datos distribuida con experiencias de usuarios. Es preciso señalar que en la inmensa mayoría de

los casos, es imposible hablar de digitalización de la educación cuando en la práctica cotidiana ha consistido en una sucesión de videoconferencias en Zoom, escaneo de tareas e interminables hilos de Gmail.

Resultado: angustia de los profesores, desesperación de los padres, y, mucho más importante, aburrimiento y tedio en los niños, que, privados de la presencialidad ven su día a día reducido a una lista de «entregables». Con todo, el aburrimiento ha demostrado ser un disparador del ingenio, y confirmando el lema «ningún sistema informático es infalible», hemos visto cómo niños de primaria lograron escabullirse de las clases online hackeando las aplicaciones.

A modo de ejemplo, una niña de 8 años estuvo durante más de tres semanas sin «asistir al colegio» por un supuesto fallo de Zoom. El servicio denegaba su acceso, ni sus padres, ni el informático de la escuela conseguían entender el origen del problema. Sus tutores consintieron que fuera educada, bajo supervisión, en casa... sin embargo, la dicha de la niña llegó a su fin cuando, en la casa de una compañera fue pillada in fraganti tecleando sus datos de usuario y contraseña de forma compulsiva en la pantalla de login. Había descubierto que cada vez que introducía sus datos erróneamente, se bloqueaba su acceso durante 20 minutos y que cada intento fallido sumaba días de permiso en Zoom.

Esta anécdota nos revela, por un lado, el drama de la improvisación, pero también evidencia el riesgo de aceptar como digitalización algo que está muy lejos de serlo.

No menos impactante ha sido la **brecha de seguridad** detectada en la aplicación educativa de mayor uso en Alemania. Al estar financiada con fondos de la Unión Europea, un gran número de centros educativos optaron por «Anton» durante la pandemia. Fue demasiado tarde cuando se supo que los datos de los niños no estaban protegidos por contraseñas ni ninguna otra medida de seguridad.

Los desarrolladores han confirmado la solución del problema, pero los nombres y apellidos de los niños, los datos del colegio y clase a los que pertenecen, así como los registros de uso de la aplicación y resultados educativos han estado a libre disposición en la red. La investigación sobre el acceso a la información aún sigue en curso, y las autoridades no han precisado si terceros han podido hacer uso de ella. En el market de Android, las descargas de Anton habían sobrepasado el millón cuando se anunció el agujero de seguridad.

Recomendamos

1. SCMP: China prepara la reforma de su legislación sobre Internet.
<https://www.scmp.com/tech/policy/article/3119095/nailing-jell-o-wall-how-china-wants-keep-controlling-internet>
2. SCMP: La ruta de la seda digital.
<https://www.scmp.com/news/china/diplomacy/article/3126280/can-chinas-digital-silk-road-ensure-dominant-role-information>
3. NYT + Nature: Criptografía cuántica.
<https://www.nytimes.com/2021/03/17/science/abel-prize-mathematics.html>
Nature: <https://www.nature.com/articles/d41586-021-00694-9>
4. Euractiv: Cuando la **anonimidad** de las redes se convierte en promesa de impunidad, las mafias toman el terreno.
<https://www.euractiv.com/section/justice-home-affairs/news/european-police-pounce-after-cracking-encrypted-phone-network/>
5. Handelsblatt: Código ético para programadores de software y empleados de empresas tecnológicas.
<https://www.handelsblatt.com/politik/international/interview-mit-vera-jourova-eu-kommissarin-will-macht-der-tech-konzerne-begrenzen-meine-geduld-ist-am-ende/26820710.html>
6. The Guardian: **Criptoarte** o como hacer que el arte digital sea susceptible de especulación, infalsificable (al menos hasta que se desarrolle la computación cuántica) y por tanto «valioso».
<https://www.theguardian.com/culture/2021/mar/05/what-is-cryptoart-how-much-does-it-cost-and-can-you-hang-it-on-your-wall>
7. Campaña AEPD: La Agencia Española de Protección de Datos lanza «Lo paras o lo pasas» para denunciar la difusión ilegítima en Internet de contenidos sensibles, sexuales o violentos y fomentar el uso del Canal Prioritario de Denuncias.
<https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/lo-paras-o-lo-pasas-nueva-iniciativa-aepd>



Multimedia

«Made for Love», primera serie sobre neuroderechos

A través de un mosaico de personajes, la serie muestra diferentes aproximaciones, significados e implicaciones de los neuroderechos a nivel físico, comercial, social, espiritual... alertando sobre las consecuencias de los excesos de las corporaciones tecnológicas.

Relacionado: El Dr. Rafael Yuste en TVE: El cazador de cerebros: Humanos híbridos



Fundación Instituto Hermes
C/. Orense 81, 7ª planta - 28020 Madrid
fundacion@institutohermes.org
<https://institutohermes.org>