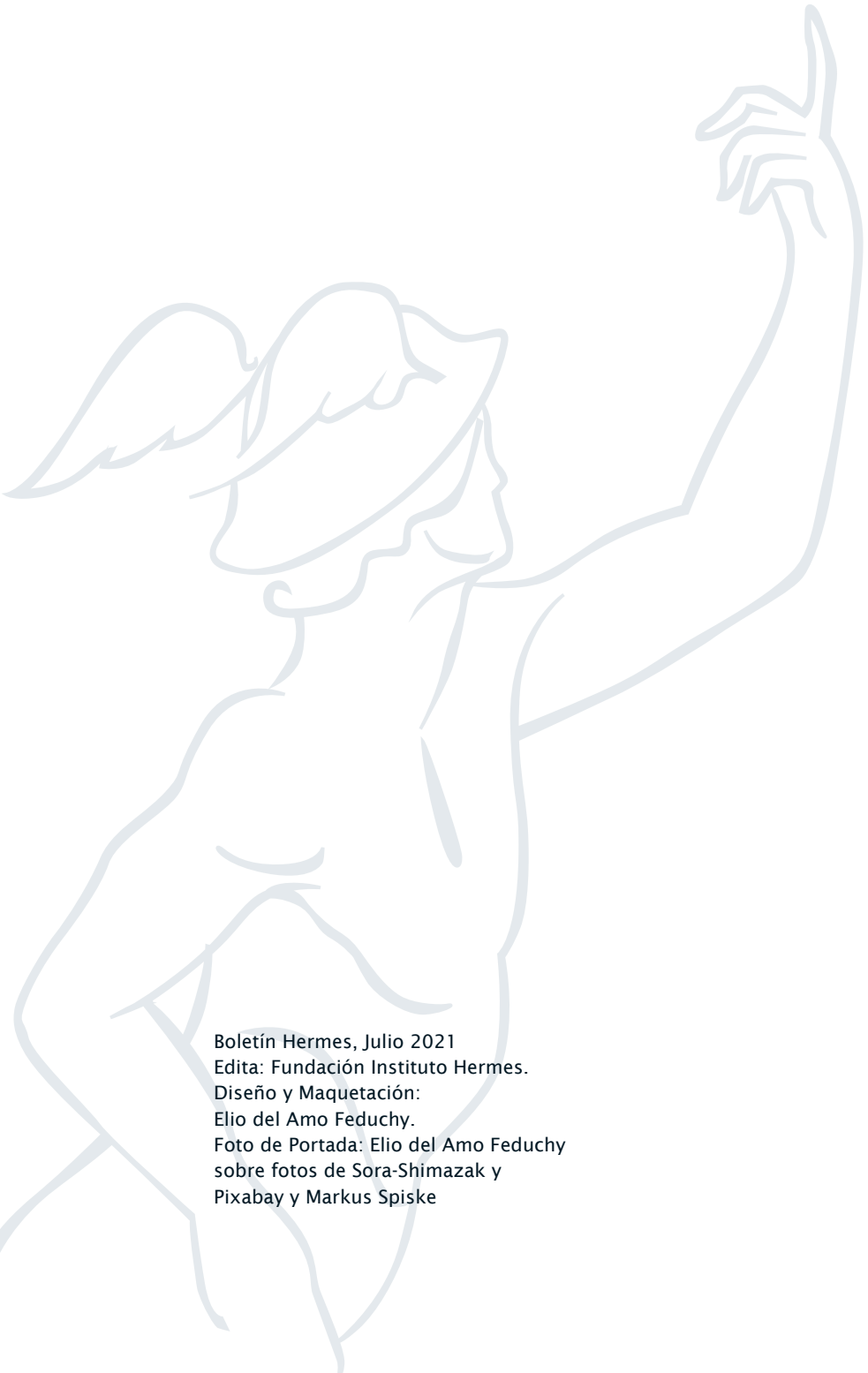

Instituto
Hermes
Derechos de ciudadanía digital
BOLETÍN HERMES
Año 2 • nº 8 • julio 2021



Boletín Hermes, Julio 2021
Edita: Fundación Instituto Hermes.
Diseño y Maquetación:
Elio del Amo Feduchy.
Foto de Portada: Elio del Amo Feduchy
sobre fotos de Sora-Shimazak y
Pixabay y Markus Spiske

Índice

1. La ciberseguridad en el centro de la actualidad política

Visita oficial del presidente Obama a Alemania en 2013

Junio comenzó con el descubrimiento del espionaje organizado por el gobierno del presidente Obama a líderes europeos. Salía a la luz que entre 2012 y 2014 el servicio de inteligencia militar y extranjero danés (Forsvarets Efterretningstjeneste, FE) permitió a la NSA utilizar la estación de escucha secreta Sandagergardan cerca de Copenhague. Las escuchas telefónicas estaban dirigidas contra los principales políticos de Alemania, Suecia, Noruega, los Países Bajos y Francia. En Alemania además de Merkel y el actual presidente federal Frank-Walter Steinmeier, violaron las comunicaciones del entonces candidato a canciller del SPD, Peer Steinbrück. La NSA tenía acceso a mensajes de texto, llamadas telefónicas y actividades en Internet, incluidas las búsquedas, los chats y los servicios de mensajería. Parecía el mayor de los escándalos posibles y se daba en un momento crítico en la recuperación del diálogo entre EEUU y la UE. Pero pronto iba a quedar en segundo plano.

Pocos días después, un ataque de ransomware de «DarkSide», el grupo de crackers rusos que ya había atacado en mayo el oleoducto de «Colonial Pipeline», paraliza la distribución de 1/5 de la carne que se come en

EEUU. La sensación de fragilidad e indefensión en la sociedad estadounidense se hace proporcional al impacto.

En pleno cuestionamiento de su estrategia para «contener» a Rusia, Biden pide a Putin que tome cartas en el asunto y reprima a la «industria» de los secuestros digitales. Pero para **Rusia supone más de 50.000 millones de dólares y una forma de guerra asimétrica especialmente rentable en términos daño-represalia**. Moscú no da señales de responder a la petición de Washington y dos semanas después los servicios de inteligencia estadounidenses y británicos publican un informe detallado sobre las campañas de ciberataques rusas, sus estructuras y sus objetivos.

En Europa las cosas no van mejor. Solo en España, el ataque al SEPE, que paralizó el cobro y tramitación de los ERTE, seguros de desempleo y ayudas sociales afectando a casi dos millones de trabajadores, fue seguido de un ataque a la estructura informática del Ministerio de Trabajo cuyas consecuencias siguen sin superarse completamente en el momento de redactar este boletín.

Viendo la escalada, el Parlamento Europeo pide a la Comisión y el Consejo una nueva política de ciberseguirdad. La respuesta del Comisario de Exteriores, Josep Borrell, fue relativamente rápida: dos días después declaró en nombre de la Comisión que Europa construirá un «brazo operativo» para defenderse del fuego cruzado de aliados y rivales en la ciberguerra ya en marcha.

Bruselas llevaba tiempo señalando las actividades subversivas no solo de Rusia sino de China. Y no se equivocaba. El hackeo del servicio de email de Microsoft, utilizado -irresponsablemente, pues era conocida su vulnerabilidad estructural- por todo tipo de organizaciones empresariales, militares y gubernamentales, resultó ser el producto de hackers chinos según denunció la Comisión.

Pero el ataque colmó el vaso de la paciencia estadounidense. El día 19 de julio, por primera vez **EEUU acusó directamente al gobierno de Pekín e intentó formar una coalición internacional para tomar partido contra las actividades ciberterroristas del gobierno chino**.

El secretario de Estado, Antony J. Blinken, aseguró que el Ministerio de Seguridad del Estado de China «ha fomentado un ecosistema de piratas informáticos, criminales que llevan a cabo actividades patrocinadas por el estado y delitos cibernéticos para su propio beneficio financiero».

Sin embargo, aunque la coalición que suscribió sus palabras ganó una gran fuerza política al incorporar a la UE y, por primera vez, a todos los miembros de la OTAN, fue incapaz de traducir la indignación en sanciones.

Y si todo esto pareciera poco, emergió ***Pegasus***.

En la prensa europea y americana habían pasado desapercibidas las revelaciones del diario israelí Haaretz denunciando que Israel había prestado a Arabia Saudí software de cibervigilancia de última generación. Desarrollado por «Quadream», una empresa del consorcio ciber-militar que sostienen las IDF, **el programa permite «hackear cualquier iPhone con un solo click».**

Ahora sabemos que no era el único ciber-armamento que la industria militar-tecnológica «sabra» estaba licenciando a países con un dudoso track-record en derechos humanos. Los servicios secretos de Marruecos, Hungría, México, Togo... habían recibido Pegasus de la mano de una empresa militar privada vinculada a los servicios y el ejército israelí y lo habían usado para seguir a 50.000 personas. En la lista 24 jefes de estado o de gobierno, como Macron, miles de periodistas y centenares de activistas pro derechos humanos. Las conexiones de algunos de estos estados con actividades clandestinas y la penetración del narco en el estado mexicano -evidente al hacerse pública la lista de periodistas intervenidos- no hicieron más que agravar el escándalo.

De modo previsible, donde primero suscitó una reacción pública contundente fue en Israel. Pegasus fue parte de los «regalos» que Netanyahu intercambió por apoyos en estos últimos años. Así que las columnas y editoriales se sucedieron durante días. Entre las exigencias más frecuentes en la prensa israelí se planteó una cuestión regulatoria básica: **¿Debe prohibirse la exportación de ciber-armamento?** ¿Cabe esperar otro uso distinto del que hemos visto por países como Marruecos o México? Y por otro lado: ¿Puede esperarse algo mejor de las grandes potencias?

Una semana después, Amnistía Internacional hace suya la propuesta, pero la adapta y plantea una moratoria mundial en el uso de herramientas de cibervigilancia.

Más interesante fue la reflexión abierta por **Pavel Durov**, el **creador de Telegram**, explicando el origen de todos estos desastres para la privacidad y los derechos y apuntando directamente a **Apple y Google como corresponsables de su explotación militar y criminal**.

Según las revelaciones de Snowden de 2013, tanto Apple como Google forman parte del programa de vigilancia global que implica que estas empresas tienen que, entre otras cosas, implementar puertas traseras en sus sistemas operativos móviles. Estas puertas traseras, normalmente disfrazadas de fallos de seguridad, permiten a las agencias estadounidenses acceder a la información de cualquier smartphone del mundo.

El problema de estas puertas traseras es que nunca son exclusivas de una sola parte. Cualquiera puede explotarlas. Así que si una agencia de seguridad estadounidense puede hackear un teléfono iOS o Android, cualquier otra organización que descubra las puertas traseras puede hacer lo mismo. Como es lógico, esto es exactamente lo que ha estado ocurriendo: una empresa israelí llamada NSO Group ha estado vendiendo el acceso a las herramientas de espionaje que permitían a terceros hackear decenas de miles de teléfonos [...].

La existencia de puertas traseras en infraestructuras y programas informáticos cruciales supone un enorme desafío para la humanidad. Por eso he hecho un llamamiento a los gobiernos del mundo para que empiecen a actuar contra el duopolio Apple-Google en el mercado de los teléfonos inteligentes y les obliguen a abrir sus ecosistemas cerrados y permitir una mayor competencia.

Hasta ahora, a pesar de que la actual monopolización del mercado aumenta los costes e impide la privacidad y la libertad de expresión de miles de millones de personas, los responsables gubernamentales han actuado con mucha lentitud. Espero que la noticia de que ellos mismos han sido objeto de estas herramientas de vigilancia haga que los políticos cambien de opinión.

Durov vive exiliado en un país del Golfo desde que la presión del gobierno Putin por controlar su sistema de chat convirtió su seguridad física en un problema. Se enfrenta ahora a una ley creada específicamente

para cerrar el servicio de Telegram en su país natal, Rusia, y en Bielorrusia. En ambos países -así como en Irán y toda Asia Central- Telegram ha llegado a ser la espina dorsal de la oposición y la sociedad civil. Durov se ha convertido por tanto en el «enemigo público número uno» de varios estados autoritarios. Una medida de la importancia que los gobiernos aliados de Teherán y Moscú dan a Telegram la tuvimos este junio cuando aviones de guerra bielorrusos desviaron un vuelo comercial con destino a Lituania solo para detener al creador de un canal Telegram opositor. Abrir una crisis diplomática internacional no importó entonces a Lukashenko. Y solo era un canal entre muchos.

Telegram colabora rutinariamente con los jueces europeos, estadounidenses y británicos para frenar contenidos jihadistas y contrarios a los derechos de la infancia. Con sus más de 500 millones de usuarios es hoy insustituible como herramienta para la comunicación segura. Whatsapp está completamente desacreditado y se ha convertido en el objetivo de la mayor parte de ONGs de derechos digitales en Alemania y Francia. Y «Signal», un sistema pensado desde el libertarismo anglosajón que se jactaba de estar blindado incluso a los jueces de países democráticos, ha sido recientemente penetrado por los cuerpos de seguridad europeos -entre ellos los españoles- en una operación conjunta contra el tráfico de drogas que ha ocupado las portadas de este verano. Lo que quiere decir que es penetrable también por estados totalitarios con muchos más recursos y muchos menos controles legales.

2. El asesinato civil y el acoso digital son una industria... la misma que la desinformación

El aumento de la demanda de servicios de hostigamiento está dando lugar a una floreciente industria en Europa. Algunos expertos apuntan que buena parte de las empresas dedicadas a publicidad online, marketing digital y gestión de campañas comerciales han renovado su oferta para incluir servicios delictivos. Impacto, alcance y eficacia cruzan al lado oscuro para abrazar a un nuevo sector: **desinformación, asesinato civil y «black marketing» por encargo.**

El funcionamiento de esta reciente industria se ha podido conocer a raíz de una investigación realizada por la plataforma alemana **Netzpolitik**, dedicada a los derechos básicos y las libertades en el mundo digital.

Buscando el origen de los rumores sobre los riesgos para la salud de la vacuna Pfizer/Biontech, descubrieron la vinculación de un entramado de empresas europeas que durante meses habían estado dedicadas a distribuir información manipulada que alertaba sobre el aumento de muertes tras recibir una dosis de la vacuna.

Siguiendo los manuales de instrucción diseñados por los servicios de inteligencia británicos y estadounidenses, disponibles en cursos universitarios y de formación profesional, los materiales utilizaban cifras oficiales extraídas por centros estadísticos para respaldar el mensaje de la campaña: «la administración de la vacuna de Pfizer/Biotech provoca muertes».

La empresa se ocupa además de convertir la información proporcionada por el cliente en «publicidad nativa», selecciona a los prescriptores e incorpora su plataforma de medios a la campaña. Hasta 2.000 euros pueden llegar a pagar a un youtuber con un puñado de seguidores por mostrar contenidos tóxicos.

Según analistas de seguridad esta estrategia hace parte de una industria que lejos de ser secreta está creciendo a gran escala. Su núcleo lo forman empresas que ya venían haciendo «black marketing» y que pasan por «especialistas en marketing digital». Compañías que aunque no se dedican en exclusiva a estas actividades tienen departamentos cuya función principal es organizar campañas de desprestigio y asesinato civil.

A ellas se suman ahora compañías de reciente creación -no pocas de ellas espoleadas desde Moscú- que desarrollan actividades en la sombra

relacionadas con operaciones de influencia geopolítica, adentrándose en un terreno en el que hasta ahora operaban principalmente las agencias de inteligencia.

Su amplio abanico de servicios incluye la difamación y persecución de personas y organizaciones con el fin de propiciar su muerte civil, la diseminación de relatos para dañar a un competidor, la propagación de teorías de la conspiración o la intervención tóxica en procesos democráticos.

Un estudio realizado por la Universidad Oxford estima que el número de empresas que se dedica a estas actividades se ha duplicado en el último año, vinculando el crecimiento del mercado al caso Cambridge Analytica. Un episodio, formulan, que habría despertado el interés oportunista de ciertos agentes al descubrir las cantidades de dinero que se mueven entre el social media y el marketing político.

Como comentaba Graham Brookie, director del Atlantic Council's Digital Forensic Research Lab,

> *Hay, por desgracia, una gran demanda en el mercado ... y un montón de sites en todo el ecosistema (digital) que están más que dispuestos a satisfacer esa demanda.*

En un artículo, el New York Times, incorporaba a la ecuación las posibilidades que abren las tecnologías digitales al hacer accesible a prácticamente cualquier persona generar lotes de cuentas falsas con fotos de perfil difíciles de rastrear, junto con el uso de métricas instantáneas que permiten perfeccionar la eficacia de los mensajes. Lo mismo ocurre con el acceso a los datos personales de los usuarios, que se compran fácilmente al por mayor.

Sin embargo, poco a poco las sociedades desarrolladas van percibiendo este problema y haciéndose más beligerantes. Según el último estudio de la Liga contra la Difamación, principal organización civil contra el odio en EEUU, el **87,5% de los estadounidenses están de acuerdo o muy de acuerdo en que el gobierno debería endurecer las leyes y aumentar los recursos de la policía para luchar contra el odio y el acoso online**.

Este es el marco en el que hay que entender la batalla entre Facebook y el gobierno de EEUU que recogieron los medios durante los primeros días de julio.

Todo comenzó cuando el «Surgeon General» de EEUU, Vivek Murthy, equivalente a un ministro de Sanidad, envió una advertencia formal a las plataformas sobre su inacción ante la desinformación contra las vacunas: «Estas plataformas tienen que reconocer que han jugado un papel importante en el aumento de la velocidad y la escala con la que se difunde la información errónea», dijo Murthy en el programa de CNN «State of the Union».

La verdad es que todos los estudios, expertos y centros científicos están señalando que la principal causa de crecimiento del Covid en EEUU no es la mayor contagiosidad de la variante delta sino la resistencia a la vacunación. Pero las campañas de desinformación en la red están consolidando una masa crítica que puede hacer imposible la inmunidad de grupo en un futuro próximo.

Facebook y twitter emitieron quejas contra las declaraciones sin comprometerse a ninguna acción. Facebook incluso publicó una declaración conminando al gobierno a dejar de «señalar con el dedo».

Pero a los dos días, el Presidente Biden, preguntado por los periodistas fue aun más claro. Según el relato del New York Times:

> *Biden declaró en un lenguaje inusualmente fuerte que las plataformas estaban «matando gente». «Mire», agregó, «la única pandemia que tenemos es entre los no vacunados, y eso está matando gente».*

La respuesta de Facebook fue... un anónimo. Un directivo que no quiso dar su nombre acusó en un directo de CNN al gobierno Biden de «estar buscando chivos expiatorios».

Por otro lado, la desinformación sobre las vacunas no solo ocurre en EEUU. Las cifras son ya muy preocupantes en Francia -donde los antivacunas han llegado a sacar a las calles a más de 165.000 personas en manifestación este julio- y ni hablemos en Rusia donde ni siquiera la coerción gubernamental está consiguiendo llevar a los ciudadanos a los vacunódromos.

De forma significativa, el canal internacional francés «France24» destacaba que España ha sido el primer país europeo en trazar una estrategia nacional contra la desinformación. Repasaba las campañas locales de fake news de los antivacunas en Facebook y Whatsapp (un subconjunto de las francesas) e insinuaba la necesidad de extender el modelo a otros países UE.

Pero no es solo en Europa y EEUU donde las plataformas generan cada vez más hastío por enrarecer el clima social. En China las comunidades online de fans reúnen a millones de personas, en su mayoría jóvenes, en los equivalentes locales de Whatsapp, twitter y Facebook. El nivel de violencia y acoso en estos grupos ha llevado al estado a intervenir. Como relataba el diario hongkonés South China Morning Post, propiedad del fundador de Alibaba.com, Jack Ma:

> *La Administración del Ciberespacio de China (CAC) aseguró que tomará medidas enérgicas contra las actividades que induzcan a los menores a «convertirse, amenazas mediante, en un vector de intoxicación online» a favor de sus ídolos, lo que implica buscar y publicar información privada con intenciones maliciosas sobre un individuo particular en Internet.*
>
> *También detendrá las actividades que alienten a los fans a hacer alarde de poderío, manipular los comentarios de las redes sociales, inventar noticias falsas en línea para secuestrar la opinión pública y usar bots para aumentar los datos de tráfico relacionados con sus ídolos.*
>
> *El regulador dijo que cerrará cuentas y disolverá los grupos de redes sociales que se consideren una «mala influencia», y castigará a las plataformas de Internet que han «permitido» tal caos y no han corregido sus actividades tras repetidas órdenes para hacerlo.*

3. Monedas Digitales

Las inundaciones en China han sido una de las noticias más dramáticas del verano y han sido cubiertas por prácticamente todos los medios internacionales. Pero lo que pocos han trazado es su relación con bitcoin y las llamadas criptodivisas.

En los últimos meses China ha endurecido el ataque a la minería de bitcoin. Parte de las preocupaciones oficiales se centraban en su impacto energético y medioambiental. **Solamente sostener el blockchain de bitcoin implica un consumo eléctrico superior al de un país industrializado como Italia**.

Este descomunal gasto energético permitió en primera instancia a las autoridades encargadas de imponer las nuevas normas, localizar las instalaciones mineras monitorizando el consumo eléctrico. Se trata de una metodología similar a la que la policía realiza para descubrir plantaciones ilegales de marihuana. Pero esta vez el número de factorías de

La provincia china de Sichuan es, sin duda, la mayor concentración de mineros de bitcoins del planeta, ya que las operaciones mineras de Sichuan aprovechaban las centrales hidroeléctricas para obtener electricidad, lo que les proporciona una tarifa media de 0,01 dólares por kWh durante la estación húmeda.

bitcoin encontradas era significativamente menor del esperado, lo que alertó a las fuerzas de seguridad.

Utilizando las viejas redes de información e investigación sobre el terreno, solo en la primera semana de julio la policía intervino 26 mineras clandestinas de blockchain en la provincia de Sichuan... donde luego ocurrieron las inundaciones.

¿Por qué no habían podido detectarlas mediante los mapas de consumo? Porque **los mineros, buscando esconder su consumo habían comprado decenas de presas hidroeléctricas de hasta 50MW, las menos monitorizadas por el regulador. De ese modo conseguían producir electricidad en sus instalaciones sin pasar por la red eléctrica**, donde podían ser descubiertos por el incremento de consumo.

En realidad, lo que las autoridades debían monitorizar era el inusual flujo de agua liberado por las presas medianas y pequeñas. Así que la represión siguió buscando allá donde había quejas de los campesinos y pescadores.

Durante las dos semanas anteriores a las lluvias, el éxito policial precipitó un aluvión de ventas a través de markets online de toda esta

masa de hidroeléctricas además del desmontaje de decenas de grandes centros de datos cuyos materiales inundaron rápidamente el mercado norteamericano.

El exceso de desvíos de agua, diques, embalses e instalaciones hidroeléctricas, y no solo el mal diseño de los nuevos cursos de agua, ha sido reconocido por los expertos chinos como el principal agravante del desbordamiento que ha costado cerca de un centenar de vidas y miles de desplazados. En ese marco, el estado de decenas de centrales hidroeléctricas en Sichuan, abandonadas por sus propietarios mineros de blockchain, ha sido un agravante de primer orden.

Blockchain y las criptos han conseguido, una vez más, hacer su aporte al caos.

Otro tipo de caos, no natural sino económico e incluso social, es el que ha llevado a un viejo amigo de las criptos, el gobierno británico, a prohibir cualquier tipo de actividad a «Binance», el mayor cambista de monedas digitales.

En la misma línea, la Gobernadora de la FED, Hellen Yellen lanzó un llamamiento a regular las «stablecoins» antes de que sea demasiado tarde.

¿Qué son las «stablecoins»? Criptos basadas en blockchain que se colateralizan o utilizan algoritmos para reducir la volatilidad y estabilizar precios. Entre las colateralizadas las más conocidas son Tether -que lleva todo el camino de convertirse en la próxima estafa tecnofinanciera- y TrueCoin, respaldadas ambas con dólares supuestamente en poder de la empresa que las gestiona. Y decimos «supuestamente» porque cada vez son mayores las dudas en el mercado. De hecho, la falta de confianza en la viabilidad de Tether parece ser el detonante de la respuesta de la FED. Otras stablecoins colateralizadas usan cestas de otras criptomonedas (DAI), oro (G-coin) o incluso inversiones inmobiliarias.

En España mientras tanto, se ha aprobado la **«Ley de medidas contra el fraude fiscal»** que establece una serie de obligaciones de suministro de información a la Agencia Tributaria para tenedores y gestores de monedas virtuales.

Según informaba Moncloa, los propietarios de criptos tendrán que presentar en su IRPF un registro de todas las transacciones que hayan sido realizadas y de sus saldos. De no hacerlo, tendrán multas de 5.000€ por cada dato no declarado, además de las correspondientes correcciones y

pagos en la declaración del impuesto. La nueva norma, podría afectar a unos cuatro millones de propietarios de criptodivisas en España.

Por su parte, las empresas que gestionan estos activos en criptos y prestan servicios relacionados con la operativa, deberán informar a las autoridades tributarias sobre quienes son los dueños de las monedas digitales y sus saldos. Por último, los cambistas deberán comunicar los domicilios, identificaciones fiscales, movimientos, precio y fecha de todas las operaciones que realicen por cuenta de sus clientes.

Estas reglas son aplicables tanto a los activos que se encuentran dentro o fuera de España y aquellas que se sitúen en el exterior se incluirán en el modelo 720 dentro de la declaración sobre bienes y derechos situados en el extranjero.

Es la primera acción decidida de un gobierno español contra la opacidad e impunidad de las transacciones realizadas en criptomonedas. Distintos países europeos trabajan ya en la misma línea y es previsible que, vista la actitud de la Reserva Federal, EEUU acabe optando por una regulación similar.

La gran noticia europea, sin embargo la dio el BCE al «dar un paso más y poner en marcha el proyecto del euro digital». No se han hecho públicos nuevos detalles ni tan siquiera la fecha de emisión. Sin embargo se confirman los lineamientos que publicamos en el anterior boletín y que ya se habían presentado oficialmente como resultado de los estudios y trabajo teórico del Banco.

Teletrabajo y Trabajo Digital

Podemos decir ya con certeza que los confinamientos cambiaron para siempre el panorama laboral acelerando drásticamente la digitalización del trabajo.

Frente a la idea que transmitieron algunos como el nuevo líder de WeWork, Sandeep Mathrani, de que el teletrabajo daría cobijo «a los menos comprometidos», son cada vez más los grandes gestores y estudiosos de la vida corporativa que afirman lo contrario. Entre ellas destacaremos dos.

Este mes apareció una interesante carta en el Financial Times. Estaba firmada por Max Thowless-Reeves y en ella afirmaba, «la mediocridad se esconde en las oficinas», asegurando que era más fácil identificar qué

persona agregaba más valor cuando todos trabajaban de forma remota. Thowless-Reeves es un exbanquero privado de UBS que ahora tiene una pequeña empresa de gestión de patrimonio en Stafford, al norte de Birmingham, con 15 empleados. Además es profesor en la Aston Business School. Habla por experiencia. Aunque no cerró su oficina, puso a todos sus trabajadores a utilizar suites de trabajo en grupo, digitalizando sus procedimientos antes de mandar a todos a trabajar en remoto. El resultado según él mismo ha sido un aumento general de la productividad... que ha dejado en evidencia a los remolones.

En realidad, como avanzábamos hace ahora un año en la presentación del «Decálogo Hermes» ese es el quid de toda la discusión sobre el teletrabajo. Como decía Alexia Gambon, directora de investigación de Gartner, en una columna en The Observer, **«el problema no es el trabajo remoto, sino aferrarse a las prácticas basadas en la oficina»**, es decir teletrabajar sin haber digitalizado previamente los procedimientos de la empresa.

En España parece ser un punto de vista cada vez más extendido, porque según un estudio publicado este mes por Boston Consulting Group, el 65% de las empresas españolas quiere optar por un modelo «híbrido» de presencialidad y trabajo remoto. Además, el 54% de las empresas consultadas por la firma declara aspirar a que el número de jornadas que los trabajadores de oficina realicen fuera de la sede sea de 2,5 o más cada semana. Es decir, la mayor parte de las empresas tendrán más horas de teletrabajo que de trabajo presencial.

Por parte de los trabajadores el entusiasmo parece parejo. La Asociación Nacional de Distribuidores de Cerámica y Materiales de Construcción (Andimac) aseguraba el mes pasado que un 15,7% de los españoles tenía planeadas reformas en su hogar destinadas a crear espacios aptos para el trabajo remoto.

A este porcentaje hay que sumar los que han emprendido la aventura de buscar **espacios rurales** -un fenómeno en el que España va a la zaga de Portugal pero que ya despunta- o de costa, dando nueva vida a los apartamentos turísticos de playa. Se trata de una tendencia cuya consolidación sin embargo no dependerá de empresas ni trabajadores en exclusiva, sino sobre todo de la creación de condiciones de conectividad, infraestructuras y servicios, especialmente sanitarios, culturales y educativos. Es decir, de la regulación e inversión pública.

Un aparte merecen los nómadas digitales. Este verano están siendo noticia porque cada vez son más los países europeos que están creando visados especiales para favorecer su llegada.

Son 13 ya los estados que dan visados de teletrabajo dentro la UE. A partir de 2022, estos visados para nómadas digitales permitirán teletrabajar dentro de todo el espacio Schengen por periodos de 90 días en cada país. Darán derecho a realizar las mismas actividades económicas que un residente (abrir una cuenta bancaria, por ejemplo) sin necesidad de regularizar el permiso de trabajo, que por muy automático que sea dentro de la UE, puede consumir ese tiempo.

En España, el anteproyecto de la **«Ley de Startups»**, aprobada por el Consejo de Ministros el 13 de julio, contempla una serie de incentivos para atraer a trabajadores digitales. Además de ventajas fiscales, crea un nuevo visado para extranjeros que teletrabajan de forma estable desde España y para nómadas digitales que les permitirá residir en el país por un periodo de un año ampliable a tres.

En esta competencia creciente por los nómadas digitales, Airbnb lanza paquetes globales pensados para ellos, aerolíneas como Air France crean sistemas de tarificación especiales y las ciudades y centros vacacionales empiezan a competir por colocarse como destinos apetecibles en rankings específicos para este target.

En la última lista que ha saltado a los medios anglosajones, Madrid no aparece hasta el puesto 21 con una valoración de 79,17 puntos sobre 100 y Barcelona hasta el 29 con 77 puntos. Lisboa en cambio suma 81,16 puntos y ocupa la posición número 15. El ranking ha sido realizado por Nestpick, una plataforma de alquileres internacional.

La carrera por los datos y la Inteligencia Artificial

El futuro proyecto de la **«Ley de gobernanza de datos»** (DGA) ha salido ya del Comité de Industria, Investigación y Energía del Parlamento Europeo. El objetivo de la ley es crear nuevas reglas sobre neutralidad de los mercados de datos y facilitar la reutilización de datos generados por el sector público (sanidad, medioambiente, agricultura) que no estaban contemplados en la Directiva de Datos Abiertos.

Dicho en pocas palabras: el objetivo de la DGA es f**acilitar el acopio de datos por empresas emergentes para impulsar el desarrollo de la IA en la UE creando «un Schengen de los datos»**.

Entre los elementos más interesantes de la posición del Parlamento destacamos:

- Los organismos del sector público deberían **evitar la celebración de acuerdos que creen derechos exclusivos para la reutilización de ciertos datos**. En todo caso, afirman los eurodiputados, los acuerdos exclusivos deberían tener un período máximo de 12 meses antes de liberarse al dominio público y quedar en manos de la ciudadanía y las PYMEs.

- Los **datos sensibles del sector público pueden transferirse a terceros países solo cuando se benefician de un nivel de protección similar al de la UE**. La Comisión declarará si un tercer país proporciona dicha protección mediante un acto delegado que permita al Parlamento opinar sobre la decisión.

- La **donación de datos de los ciudadanos con fines altruistas** («como la investigación científica, la atención médica, la lucha contra el cambio climático o la mejora de la movilidad») no solo exigirá consentimiento informado sino **que deberá articularse a través de organizaciones reconocidas por la Unión** que inscribirán los datos en un registro específico.

Las referencias a la «mejora de la movilidad» equiparándola a objetivos sociales como la investigación médica o la lucha contra el cambio climático, no son inocentes. Europa está intentando recuperar terreno a toda velocidad en la carrera por la conducción autónoma.

Alemania acaba de aprobar una ley que permite el uso diario de vehículos autónomos y proporciona una coherencia legal de la que carecen los Estados Unidos... lo que no ha pasado inadvertido a la industria y los medios norteamericanos. Temen que la recopilación masiva de datos de conducción real en Alemania primero y luego en toda Europa den ventaja a las grandes firmas europeas. Porque además, lo que parece seguro, según declaraban a la edición francesa de Slate ingenieros y usuarios de Tesla, es que la IA desarrollada en EEUU para la conducción autónoma «te convierte en un peligro» si se utiliza en Europa, con una estructura viaria y comportamientos al volante muy diferentes.

El sentido de urgencia que se extiende en la industria no está relacionado solamente con la competencia entre firmas de distintos orígenes. **Cada vez surgen más dudas y problemas con la IA en general y con la IA dedicada a la conducción autónoma en particular**.

En EEUU los choques en los que se ven envueltos vehículos con el piloto automático de Tesla están siendo revisados. Las víctimas ya se están organizando a nivel nacional y culpan a un fallo de la tecnología del número creciente de accidentes.

Y no es el único campo en el que emergen problemas. Este mes se hizo público que los gestores de fondos automatizados que usan IAs en España acumulan 12 millones de pérdidas en 4 años.

No es solo una cuestión de volumen de información. Un artículo publicado en la revista científica Chemestry World este mes daba la clave. Los algoritmos describen o se asemejan a la realidad, pero no son la realidad. Las simulaciones informáticas tienen, aunque se olvide, una condición: que la realidad sea igual, sin nada más ni nada menos, que el resultado de nuestro modelo. Da igual que esté elaborado por un equipo humano o por una IA, nunca funcionará al 100%... ni siquiera en cristalografía.

La reflexión de los científicos es muy relevante y tiene repercusiones directas sobre los derechos ciudadanos.

Por ejemplo, Polonia se opuso al artículo 17 de la Directiva de Copyright que permite a las plataformas vigilar y eliminar contenidos de forma automatizada aduciendo un potencial peligro para la libertad de expresión. Los polacos mostraron ejemplos en los que algunos contenidos eran borrados por IAs de plataformas por contener citas o tras establecer paralelismos en absoluto claros. El «Abogado General» del Tribunal superior de la UE (equivalente a un Fiscal General) adujo sin embargo el pasado 15 de julio que el artículo no infringe el derecho a la libertad de expresión... bajo ciertas condiciones que incluyen el derecho de cita.

Es decir, la legalidad misma de una directiva que ha de incorporarse a la legislación de cada país miembro depende de cómo valoremos la posibilidad de error de un sistema opaco. Los químicos del artículo citado arriba, conscientes de las limitaciones algorítmicas, se inclinarían seguramente por dar la razón a los juristas polacos, pero la industria y los gobiernos, presionados por la competencia con China y EEUU, parecen decididos a tomar más riesgos.

6. Breves

España

La actualidad del mes en España siguió marcada por la **«Carta de Derechos Digitales»**. En la inauguración de una mesa redonda sobre el proyecto, Mª Teresa Fernández de la Vega, Presidenta del Consejo de Estado aseguró que «sería importante que la Carta de Derechos Digitales se convirtiera en Ley Orgánica, porque se refiere a derechos fundamentales». Pocos días después, «la Carta» se presentaba públicamente en un acto oficial en el Palacio de la Moncloa.

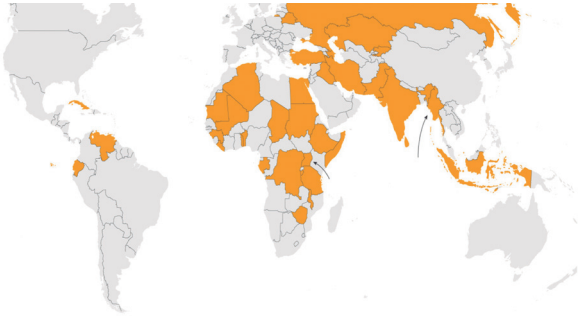
El Gobierno, a través de la SEDIA, presentó también la **Ley de Startups**, los resultados de la aportación española al proyecto europeo «GaiaX» -destacando el papel jugado por las PYMEs- y el Fondo público-privado «Next Tech» al que destinará 2.000 millones de euros para impulsar el crecimiento de empresas tecnológicas y la inversión de proyectos tecnológicos de alto impacto. Además, el Ministerio del Interior presentó el nuevo **«DNI-e 4»**, que sigue el nuevo estándar europeo.

Pero no todo fueron buenas noticias. Según denuncian funcionarios y letrados, los fallos de las videoconferencias están retrasando el funcionamiento de la Justicia y los tribunales. Y la fragilidad de la estructura informática del Estado quedó de manifiesto además con el hackeo del Ministerio de Trabajo y el fallo de seguridad de la aplicación Covid en la Comunidad de Madrid.

En la sociedad civil destacamos que **un equipo español lidera el desarrollo del primer chip europeo en hardware libre**, una cuestión **clave** en plena crisis de **abastecimiento de semiconductores en toda la industria europea**; y que Google, Indra y la Universidad de Granada han creado un centro de Inteligencia Artificial en la capital oriental andaluza.

Mundo

Axios señala que desde 2019 35 países, 3 de ellos en Iberoamérica, han sufrido apagones de Internet o bloqueos de social media por parte de sus gobiernos. El único inesperado es Ecuador. En **Alemania**, la candidata de los Verdes quiere un cambio constitucional para **asegurar que Internet sea un servicio económico de interés general y que la banda ancha sea un derecho efectivo en todo el territorio.**



En Alemania, distintos medios han publicado artículos asegurando que l**os próximos unicornios digitales serán «verdes»**: unirán lo digital con la Transición ecológica. No es solo una profecía, el desarrollo de las vacunas de BioNTech y Curevac ha creado una verdadera oleada inversora en el país en busca de los líderes de la postpandemia. Eso sí, como en toda burbuja digital ya hay timos... ligados a blockchain.

El «derecho a reparar» productos electrónicos, una parte que está cobrando peso dentro del EU Green Deal y su discurso sobre la economía circular, ha saltado el Atlántico de la mano del Presidente Biden y se ha establecido ya como parte del debate social y mediático.

Las quejas contra Whatsapp por ONGs e instituciones de defensa de los derechos de los ciudadanos y consumidores se han prodigado en Francia y en Alemania.

El New York Times carga contra Facebook por introducirse en el mercado de los boletines de suscripción a noticias. «Es una mala noticia para la democracia», asegura el medio neoyorkino. Desde luego el track-récord de la plataforma y su vinculación a las fake news y la desestabilización no ayudan a darle un voto de confianza.

En EEUU una coalición de 37 fiscales generales demandó a Google por monopolio. La noticia llega después de que Biden nombrara a Lina Khan, una famosa abogada especializada en la lucha antimonopolio. Según la prensa internacional, la conjunción de estos dos movimientos marca el inicio de una política dura hacia Google Amazon y Facebook en Washington.

Recomendamos

1. New York Times. El próximo objetivo de Facebook: dar forma a la religión en EEUU

   «La compañía está intensificando las asociaciones formales con grupos religiosos en los Estados Unidos y dando forma al futuro de la experiencia religiosa». [...]

   https://www.nytimes.com/2021/07/25/us/facebook-church.html

2. Marianne. Alain Bentolila: «Solo la resistencia intelectual de nuestros hijos podrá interponerse en el camino de la barbarie».

   https://www.marianne.net/agora/tribunes-libres/seule-la-resistance-intellectuelle-de-nos-enfants-pourra-faire-barrage-a-la-barbarie

Multimedia

Entrevista a Juliette Dunesque sobre «L'humain au risque de l'intelligence artificielle» en Marianne TV.

https://tv.marianne.net/rencontres/demain-tous-dependants-de-l-intelligence-artifi?autoplay=true

«El día de 2016 en que Facebook desgració Internet», en The New York Times

https://www.nytimes.com/2021/06/09/opinion/facebook-news-feed-zuckerberg.html

Lectura

«L'humain au risque de l'intelligence artificielle»,
Pierre Rabhi y Juliette Dunesque

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