PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

El paquete de información al ciudadano y la guía para personas vulnerables

Esta obra está sujeta a una licencia de Creative Commons Atribución-NoComercial-SinObraDerivada 4.0 Internacional.

Este proyecto ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención nº 788039. Este documento refleja únicamente la opinión del autor y la Agencia no es responsable del uso que pueda hacerse de la información que contiene.

Información sobre el proyecto

Título del proyecto	Enfoques participativos para un nuevo marco ético y jurídico de las TIC
Acrónimo del proyecto	PANELFIT
Número del convenio de subvención	788039
Coordinador del proyecto	UPV/EHU

Información del documento

Número de entrega	D5.5
Título del documento	Paquete de información para el ciudadano
Versión del documento	3.0
Fecha del documento	22 de abril de 2022
Paquete de trabajo	WP5
Tarea	Tarea 5.7
Documento principal	OBCT / ECSA
Licencia de derechos de autor	Licencia internacional Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0.
Nivel de difusión	PU = Acceso público sin restricciones - Proyecto de la UE
Fecha de vencimiento del contrato	2021-08-31 (Mes 34)

Socios del proyecto que participan en el documento

No.	Nombre de la organización	Acrónimo
1	Universidad del País Vasco / Euskal Herriko Unibertsitatea	UPV/EHU
7	Asociación Europea de Ciencia Ciudadana	ECSA
8	Red Europea de Comités de Ética de la Investigación	EUREC
9	Instituto de Ciencias del Mar (Consejo Superior de Investigaciones Científicas)	ICM-CSIC
10	OBC Transeuropa	OBCT

Historia del documento

Estatus	Versión	Fecha	Autor(es)	Revisado por
Borrador	V1.0	21.7.2021	Tim Woods (ECSA)	
Editar	V1.1	22.7.2021		Iñigo de Miguel Beriain (UPV/EHU)
Editar	V1.2	18.8.2021		Federico Caruso (OBCT)
Final	V2.0	19.8.2021		
Final	V3.1	31.8.2021		Roberta Monachello (UE)
Final	V4.0	08.04.2022		Carolina Doran (ECSA), Federico Caruso (OBCT), Johann Cas (ÖAW) y Alessandro Ortalda (VUB)

Índice de contenidos

TIC, datos y personas vulnerables: guía para los ciudadanos 4
Acerca de esta guía 5
Glosario de términos clave 6
¿Cuáles son las cuestiones éticas y jurídicas en torno a las TIC? 8
¿Quién debe considerarse una persona vulnerable? 10
¿Cómo afectan las cuestiones éticas y jurídicas en torno a las TIC a las personas vulnerables? 14
¿Qué puedes hacer? 26
Agradecimientos 33
Expedientes temáticos 36
1. Comercialización de datos: operadoras telefónicas y datos personales 36
2. La estrategia europea de ciberseguridad 44
3. Desequilibrios de poder y libertad de consentimiento: La Europa de la fortaleza digital 58

TIC, datos y personas vulnerables: guía para los ciudadanos

Descargo de responsabilidad

Este proyecto ha sido financiado por el programa de investigación e innovación Horizonte 2020 de la Unión Europea mediante el acuerdo de subvención nº 788039. Este documento refleja únicamente la opinión del autor y la Agencia no es responsable del uso que pueda hacerse de la información que contiene.

Cita

Consorcio PANELFIT (2021) *TIC, datos y personas vulnerables: una guía para los ciudadanos*. UPV-EHU, Bilbao.

Acerca de esta guía

Las TIC, datos personales, derechos digitales, el RGPD, la privacidad de los datos, la seguridad en línea; estos términos, y otros que los sustentan, son cada vez más comunes en nuestras vidas. Pese a que muchos de nosotros estamos familiarizados con estos conceptos, existen aún personas que no son plenamente conscientes del creciente papel de las TIC y los datos en nuestras vidas, y de los riesgos potenciales que su uso acarrea.

A lo largo de esta guía utilizamos el término ciudadano para referirnos a todas aquellas personas que son residentes europeos independientemente de su nacionalidad, o estén sujetas al Derecho de la Unión Europea, aunque sea de forma temporal.

Los riesgos que generan las TIC y el uso de datos personales son más pronunciados para aquellos considerados vulnerables. Las personas pueden ser vulnerables en base a distintas características, que a menudo se solapan entre sí, situándolos en una situación de desventaja frente a la mayoría de los ciudadanos (el cuadro 3 presenta algunas de las muchas formas y causas de la vulnerabilidad). Por ello, las personas vulnerables necesitan un mayor apoyo para desenvolverse en el mundo digital y asegurarse de que pueden ejercer sus derechos. Esta guía explica dónde puede encontrarse ese apoyo, y también responde a las siguientes preguntas:

- Cuáles son las principales cuestiones éticas y jurídicas en torno a las TIC para los ciudadanos vulnerables?
- Quién debe considerarse persona vulnerable en Europa?
- Cómo afectan los problemas en torno a las TIC a las personas vulnerables en particular?

Esta guía es un recurso para miembros de grupos vulnerables, personas que trabajan con grupos vulnerables y ciudadanos en general. También es útil para los "controladores de datos"[5] que recogen datos sobre ciudadanos vulnerables. Aunque se centra en los ciudadanos de Europa, puede ser de interés para personas de otras partes del mundo.

La guía forma parte del paquete de información a los ciudadanos elaborado por el proyecto PANELFIT, y está disponible en inglés, francés, alemán, italiano y español. Le invitamos a traducir esta guía a otros idiomas. Por favor, envíenos un enlace a las versiones en línea en otros idiomas, para que podamos añadirlas al sitio web del proyecto.

Glosario de términos clave

El cuadro 1 explica algunos de los términos clave utilizados en esta guía. No se trata de la "última palabra" sobre estos términos, sino de una definición útil para quienes no conocen la terminología sobre las TIC, los datos y los grupos vulnerables.

Cuadro 1. Términos clave para entender las TIC, los datos y los grupos vulnerables

Ciberseguridad	Se refiere al grado de protección al que están sujetos los datos e información privada en línea; por ejemplo, su protección frente al pirateo, robo o su comunicación pública sin consentimiento.
Comercialización de datos	El tratamiento de datos de individuos o grupos para obtener un beneficio; por ejemplo, a través de la publicidad en línea dirigida o para su venta a otros.
Responsable del tratamiento	Un responsable del tratamiento de datos es cualquier persona que obtiene datos, incluidos datos personales, para utilizarlos con un fin específico. Puede ser una empresa, una organización, un gobierno o autoridad local, un organismo público (por ejemplo, una escuela u hospital) o un instituto de investigación, entre otros.
Gestión de datos	La gestión de datos abarca todo el ciclo de vida del tratamiento de datos: recogida, uso, almacenamiento, intercambio y eliminación. También se refiere al hecho de que quien recoge sus datos (el responsable del tratamiento) debe controlar para qué se utilizan los datos y quién puede utilizarlos.
Protección de datos	Sus datos personales no deben ser tratados a menos que usted lo autorice. La legislación de la UE obliga a los responsables del tratamiento de datos a tomar medidas para garantizar que se almacenen de forma segura y privada. Sus datos no deben ser compartidos, ni puestos a disposición del público a menos que usted lo haya autorizado.
Interesado	La persona cuyos datos personales son recogidos y utilizados por el responsable del tratamiento.

Uso y reutilización de datos	Al solicitar sus datos, los responsables del tratamiento deben explicarle los fines para los que se utilizarán (por ejemplo, un censo o un proyecto de investigación). Si ellos, o un tercero, quieren utilizar sus datos para otro fin -lo que se conoce como reutilización de datos- deben pedirle de nuevo su consentimiento para hacerlo. No pueden dar por sentado que usted está de acuerdo con la reutilización de sus datos.
Brecha digital	Describe la brecha entre las personas que pueden beneficiarse de la tecnología (por ejemplo, las TIC, Internet) y las que no pueden hacerlo. Este fenómeno es cada vez más importante, ya que cada vez más aspectos de nuestra vida se mueven parcial o totalmente en línea (por ejemplo, la educación, la atención sanitaria, la banca, las compras). Los que tienen un acceso limitado o nulo a los servicios digitales corren el riesgo de quedarse "atrás".
Alfabetización digital	A veces denominada "alfabetización en TIC", se refiere a la capacidad de una persona para encontrar, evaluar y comunicar información en plataformas y dispositivos digitales.
Derechos digitales	Se refiere a las leyes y procedimientos (por ejemplo, el GDPR) que están en vigor para proteger nuestros derechos en el mundo digital. Estos derechos incluyen, entre otros, el derecho a la privacidad y el derecho a retirar el consentimiento para el tratamiento de sus datos personales.
Discriminación	La discriminación significa hacer distinciones injustificadas entre las personas, basándose en percepciones sobre ese grupo, o la categoría (o categorías) a la que pertenecen; por ejemplo, su raza, género, edad, religión u orientación sexual, entre otras.
GDPR	El Reglamento General de Protección de Datos es la norma fundamental en materia de privacidad, que regula cuándo está permitido el uso de datos personales y establece derechos y obligaciones para proteger la confidencialidad de los datos personales.
TICs	Las tecnologías de la información y la comunicación incluyen todas las formas de tecnología utilizadas para la comunicación, como Internet, los teléfonos móviles y los smartphones, los ordenadores, las redes sociales, las herramientas de videoconferencia y muchas otras.
Consentimiento informado	Con respecto a los datos y las TIC, se refiere a la obligación de informar y pedir la autorización del interesado para utilizar sus datos personales de una manera específica, que debe de solicitarse hacerse antes de recoger o utilizar sus datos.

Datos personales	Los datos personales son todo lo que se refiere a usted como individuo: su nombre, edad o dirección, por ejemplo. En el mundo digital, también puede incluir sus intereses, hábitos y preferencias; por ejemplo, las páginas que le gustan en las redes sociales, los sitios web que visita para comprar artículos, los vídeos de YouTube que ha visto, y muchos otros.
Privacidad	En relación con las TIC y los datos, la privacidad se refiere a la confidencialidad de su información (protección de datos) y a la amplitud con la que desea que se comparta (por ejemplo, públicamente o sólo por el responsable del tratamiento).
Estigmatización	La estigmatización, o el estigma social, significa desaprobar o discriminar a una persona o grupo de personas basándose en percepciones sobre la persona o el grupo al que pertenece.
Personas vulnerables	Las personas vulnerables son aquellas que, por diversas razones, se encuentran en mayor riesgo de sufrir daños en comparación con la mayoría de las personas de la sociedad. Más adelante en esta guía encontrará ejemplos de grupos vulnerables (Tabla 3). Las personas de determinados grupos sociales se denominan a veces "desfavorecidas" o "socialmente excluidas".

¿Cuáles son las cuestiones éticas y jurídicas en torno a las TIC?

Las TIC han aportado muchos beneficios a nuestras vidas. Han hecho posible comunicarnos rápidamente y a bajo coste con personas de todo el mundo; nos han dado acceso instantáneo a más información de la que nunca supimos que necesitábamos; han aportado enormes avances en la atención sanitaria; nos han ayudado a combatir la pobreza y a llevar la educación a cada vez más personas en todo el mundo.

Sin embargo, estos avances también han ocasionados nuevos desafíos. Muchas TIC necesitan datos para funcionar y, por ello, las empresas, organizaciones, investigadores y gobiernos solicitan -o simplemente toman- nuestros datos. Los datos son un recurso poderoso; quienes los controlan son cada vez más capaces de conocer aspectos de nuestra vida, tanto profesional como privada, y de beneficiarse de esta información, ya sea financiera, políticamente o de otras maneras.

Para muchas personas, los debates en torno a estas cuestiones éticas y jurídicas son difíciles de entender, y descartan adentrarse en ellos por considerarlos aburridos o irrelevantes para su vida cotidiana. Ciertamente, los debates éticos en torno a las TIC evolucionan muy rápidamente y puede

ser difícil para la gente mantenerse al día. En consecuencia, a menudo nos apresuramos a renunciar a nuestros derechos a cambio de los numerosos beneficios que aportan las TIC.

Pero a medida que estas tecnologías se van extendiendo en todos los aspectos de nuestra vida, la creciente demanda de nuestros datos personales hace que estas cuestiones sean cada vez más importantes. ¿Quién se apodera de nuestros datos? ¿Con quién los comparten? ¿Qué hacen con ellos y qué puedo hacer para controlarlos?

Las TIC son un campo en rápido desarrollo y, como tal, las cuestiones éticas y jurídicas que las rodean también cambian constantemente. El cuadro 2 destaca algunas de las principales cuestiones éticas y jurídicas actuales para los ciudadanos en torno a las TIC.

Cuadro 2. Cuestiones éticas y jurídicas relacionadas con las TIC

Muchos ciudadanos tienen un conocimiento limitado de los temas relacionados con las TIC, o están interesados en ellos.	Las cuestiones relacionadas con las TIC suelen ser difíciles de entender para los no expertos. Esto es cierto tanto para las cuestiones legales (por ejemplo, los detalles de los términos y condiciones en línea) como para las cuestiones éticas, como la vigilancia y el futuro papel de la Inteligencia Artificial. Para muchos, esto se combina con una falta de interés en lo que pueden ser temas complejos o documentos llenos de terminología legal como el Reglamento General de Protección de Datos (RGPD). En otros casos, los ciudadanos pueden querer saber más, pero no saben dónde encontrar ayuda para entender estas cuestiones. Esto tiene efectos secundarios, por ejemplo, que la gente haga clic en "Estoy de acuerdo" sin haber leído, o sin haber entendido, los términos y condiciones o la política de privacidad de un sitio web. Además, es posible que la gente no conozca las leyes que protegen sus derechos en el mundo digital, lo que dificulta su ejercicio.
Hay una serie de barreras que limitan la comprensión de los ciudadanos	Para muchas personas existen importantes barreras que les impiden acceder a más información sobre las TIC y los derechos digitales. El idioma es uno de ellos: gran parte de esta información está en inglés y en otras lenguas europeas importantes, pero no todo el mundo en Europa domina estos idiomas. Además, gran parte de esta información sólo está disponible en línea. Para las comunidades sin conexión -las que tienen un acceso limitado o nulo a Internet- sigue estando fuera de su alcance. Esta falta de acceso a la información a través de las TIC es un ejemplo de la "brecha digital".

Se percibe un desequilibrio de poder entre los ciudadanos y las empresas tecnológicas	Los "gigantes tecnológicos" -grandes empresas tecnológicas mundiales, como Facebook y Google- pueden parecer muy poderosos. Para algunas personas, esto también puede ser cierto para las empresas tecnológicas más pequeñas. Por ello, puede ser difícil decir "no" o "no estoy de acuerdo" cuando estas empresas nos piden nuestros datos. La gente piensa que puede dejar de utilizar sus servicios, o le preocupa que estas empresas simplemente tengan acceso a sus datos de todos modos. Esta sensación de impotencia aumenta, por supuesto, cuando la gente no puede o no lee la información sobre sus derechos digitales.
La diversidad de los ciudadanos hace que las personas tengan diferentes preocupaciones en torno a las TIC	Los distintos grupos de la sociedad utilizan las TIC de forma muy diferente y, por tanto, tienen distintas preocupaciones, problemas y retos en su uso. Proporcionar la información que cada grupo o individuo necesita, y en el formato y lenguaje que desean, es un reto. Por ello, mucha de la información sobre las TIC y los derechos digitales es genérica, lo que hace más difícil que la gente encuentre lo que necesita.
El panorama de las TIC cambia constantemente	Las TIC y los derechos digitales son complejos. A esta complejidad se suma el hecho de que la tecnología está en constante desarrollo y nuestros datos se utilizan siempre de formas nuevas y cada vez más complicadas. Esto conlleva sus propios retos, entre los que destaca el hecho de que siempre hay nuevas leyes, procedimientos y otra serie de innovaciones que debemos intentar comprender. Esta complejidad aumenta debido a las diferentes interpretaciones de estos derechos y a las protecciones establecidas para garantizarlos (por ejemplo, el GDPR) en los distintos países.

Fuente: Adaptado del informe del taller de la Acción COST/PANELFIT celebrado en marzo de 2020; complementado con los demás recursos enumerados al final de esta guía.

¿Quién debe considerarse una persona vulnerable?

Los retos éticos y jurídicos que plantean las TIC afectan a todas las personas, ubicadas o no en Europa. Sin embargo, para los grupos vulnerables de la sociedad, estos riesgos suelen ser aún más agudos y, en muchos casos, su capacidad para adaptarse a ellos es menor. Además, existe la posibilidad de que algunas personas vulnerables se pierdan las oportunidades y beneficios que pueden aportar las TIC si no son conscientes de ellos, o si su miedo a estos riesgos supera su deseo de obtener los beneficios.

Pero, ¿qué personas son consideradas personas vulnerables? Responder a esta pregunta reviste de complejidad debido a una serie de factores. El recuadro 1 ofrece un resumen de esta complejidad, y a continuación se explican con más detalle los factores que contribuyen a ella.

Cuadro 1. Cómo identificar factores de vulnerabilidad

Los puntos aquí expuestos no abarcan todos los elementos de la vulnerabilidad, pero ponen de relieve que se trata de un concepto complicado y polifacético. El mensaje general es que la vulnerabilidad es un concepto fluido y dinámico, y que la mayoría de las personas no encajan en categorías binarias de vulnerabilidad.

En su lugar, sugerimos ver la vulnerabilidad como un espectro: los individuos o grupos pueden tener niveles altos o bajos de vulnerabilidad, que pueden ser fijos (estáticos) o cambiantes (dinámicos). Es probable que la vulnerabilidad cambie a lo largo de la vida de una persona: con la edad, por cambios en las circunstancias personales y debido a factores que escapan a su control.

También cabe señalar que *todas las personas* son potencialmente vulnerables, y que su nivel de resiliencia -su capacidad para hacer frente a la vulnerabilidad- viene determinado por su acceso a los recursos (por ejemplo, los servicios públicos disponibles en un país) y por factores culturales (por ejemplo, sus redes de apoyo).

Sobre todo, es importante recordar que todos los grupos e individuos mencionados en esta guía son, ante todo, *personas,* y cualquier otra definición -como sujeto de datos, persona vulnerable, incluso como ciudadano- es secundaria.

Las causas de la vulnerabilidad son muy variadas

Las personas pueden ser vulnerables de muchas maneras diferentes. Por ejemplo, la vulnerabilidad puede estar causada por problemas financieros (por ejemplo, desempleo, deudas inmanejables) o por barreras relacionadas con la salud y la capacidad, como la enfermedad, la vejez o la discapacidad. Otras causas de vulnerabilidad pueden estar basadas en la ubicación, como vivir en zonas rurales remotas con pocos servicios (por ejemplo, hospitales, escuelas). Las causas de la vulnerabilidad pueden ser sociales, como los prejuicios contra los refugiados, los extranjeros o los nómadas. También pueden deberse a la discriminación basada (entre otras) en la raza, la etnia, la nacionalidad, la clase, la casta, la religión, las creencias, el sexo, el género, la lengua, la orientación sexual, la identidad de género y las características sexuales.

Las personas o grupos pueden experimentar más de una forma de vulnerabilidad

La forma que adopta la vulnerabilidad de una persona puede ser complicada. A nivel individual, una persona puede verse afectada por una mala salud y una baja capacidad económica. Estas vulnerabilidades tienen impactos diferentes, pero a menudo están interconectadas; de hecho, una causa de vulnerabilidad puede a menudo exacerbar otras, creando un "círculo vicioso". Siguiendo con el ejemplo citado, la falta de dinero puede provocar mala salud (por ejemplo, debido a una dieta

limitada o a unas condiciones de vida insalubres) y la mala salud resultante puede dificultar la búsqueda de empleo, lo que a su vez aumenta o mantiene la vulnerabilidad financiera de la persona.

La vulnerabilidad puede variar dentro de un grupo de la sociedad

Los individuos de un grupo vulnerable pueden experimentar de forma diferente una misma situación pese a las características compartidas que les unen. Por ejemplo, algunos refugiados en Europa pueden ser más vulnerables que otros debido a una serie de factores como: el país del que proceden (por ejemplo, por qué se fueron y si esto les causó un trauma o problemas psicológicos); el país en el que viven actualmente (por ejemplo, sus instalaciones para los refugiados, las actitudes públicas hacia los refugiados); y su educación, formación y competencias (por ejemplo, conocimientos de idiomas, cualificaciones profesionales). Todo ello influye en su capacidad para asentarse, encontrar trabajo y acceder a los servicios disponibles. Por lo tanto, si bien es cierto que "los refugiados son vulnerables", la gravedad de esa vulnerabilidad y la experiencia de las personas al respecto varían enormemente dentro de ese amplio grupo. De hecho, describir un determinado tipo de vulnerabilidad con un término amplio puede pasar por alto los problemas específicos de los individuos, lo que hace más difícil abordarlos.

La vulnerabilidad puede ser dinámica

Mientras que algunas vulnerabilidades no cambian significativamente durante la vida de una persona (por ejemplo, las discapacidades incurables), otras pueden empeorar o mejorar con el tiempo. Por ejemplo, muchas personas experimentan cambios en sus circunstancias personales, como en su situación económica o en su salud. También pueden cambiar los factores externos que afectan a su vulnerabilidad. Por ejemplo, la cultura o el clima político de un país varia, de tal forma que la sociedad o un Gobierno adopte un posicionamiento político menos favorable respecto a la protección de un grupo vulnerable. En otros casos, la causa de una vulnerabilidad puede desaparecer con el tiempo. Piénsese en el caso de la mejora de un problema de salud, o el hecho de que los desempleados encuentren trabajo, lo que elimina o reduce su vulnerabilidad económica.

Algunos de estos cambios son predecibles, como el aumento de la vulnerabilidad con la edad. Sin embargo, en algunos casos, la causa de la vulnerabilidad puede ser rápida e inesperada: las personas pueden verse afectadas por fenómenos que escapan a su control, como los fenómenos climáticos extremos. Estos sucesos repentinos pueden crear una situación de vulnerabilidad ante la que las personas no se encontraban preparadas.

La vulnerabilidad puede ser asumida

Al considerar la vulnerabilidad dentro de la sociedad, a menudo existe la tentación de asumir que ciertos grupos presentan unas características homogéneas, olvidando que estas pueden no aplicarse a todos los miembros de ese grupo. Por ejemplo, los refugiados pueden tener un alto nivel de estudios, y conocer con profundidad el idioma nativo del país donde son acogidos. Sin embargo, es probable que compartan otros rasgos de vulnerabilidad con otros refugiados, como un acceso más limitado a los

recursos y a las oportunidades de empleo (en comparación con los no refugiados), o el abuso, el abandono, la explotación, los prejuicios y el antagonismo de otros miembros de la sociedad.

Algunos grupos que suelen considerarse vulnerables necesitan una definición cuidadosa y, a veces, incluso deben encuadrarse en subcategorías. Por ejemplo, los niños y los jóvenes (entre 16 y 25 años) suelen ser identificados como vulnerables, pero la naturaleza de la vulnerabilidad variará mucho dependiendo de si son:

- estudiantes en ciclos inferiores, que no son legalmente capaces de tomar todas las decisiones por sí mismos.
- estudiantes de educación superior, lo que puede provocar estrés u otros problemas de salud mental.
- empleados, realizando trabajos que menudo están mal pagados o inseguros para personas integradas en este colectivo de edad.
- personas fuera de las anteriores categorías, lo que puede dar lugar a otra serie de vulnerabilidades (por ejemplo, financieras, condiciones de vida, problemas de salud mental).

La vulnerabilidad también puede ser subjetiva e invisible. Una persona puede sentirse vulnerable, o clasificarse a sí misma como tal, mientras que otra persona en una situación similar (o tal vez incluso peor) no. Al mismo tiempo, cualquier ciudadano puede considerarse vulnerable, por razones que no son inmediatamente evidentes para los demás.

La vulnerabilidad puede afectar a la persona, pero también a su cultura

En algunos casos, no son (sólo) los individuos de un grupo los que son vulnerables. Algunos grupos pueden ver amenazado su patrimonio cultural o su acceso a él. Esto puede deberse a amenazas externas, como el cambio climático: en las regiones polares, todo el modo de vida de los pueblos indígenas está amenazado. Los recursos culturales de los pueblos también pueden ser vulnerables, como su lengua, sus estructuras y redes familiares y sociales, y su patrimonio natural y su entorno.

Grupos vulnerables en Europa

Teniendo en cuenta esta complejidad, a menudo sigue siendo necesario identificar a los grupos e individuos vulnerables. Así pues, ¿quién puede o debe ser considerado "vulnerable" en Europa? No existe una definición única de vulnerabilidad, pero una definición útil para preparar el terreno es la utilizada por la UE[6] para los migrantes:

> ″ Menores, menores no acompañados, personas con discapacidades, personas de edad avanzada, mujeres embarazadas, familias monoparentales con hijos menores, víctimas de la trata de seres humanos, personas con enfermedades graves, personas con trastornos psíquicos y personas que hayan padecido torturas, violaciones u otras formas graves de violencia psicológica, física o sexual, como las víctimas de la mutilación genital femenina″

A partir de esta definición, el cuadro 3 identifica varios grupos vulnerables en Europa,[7] , así como personas que experimentan ciertos tipos de vulnerabilidad.[8] Esto no debe considerarse como una lista completa de grupos vulnerables en Europa, pues dada la naturaleza cambiante de las causas de vulnerabilidad esto sería imposible de lograr. Sin embargo, ofrece un punto de partida útil para reflexionar sobre quién debe encuadrarse dentro de esta categoría.

El cuadro 3 también ofrece un ejemplo de cómo puede afectarles su vulnerabilidad en cuanto a las TIC (véase el siguiente apartado para profundizar en este tema). Los ejemplos que se dan son para ilustrar posibles tipos de vulnerabilidad relacionada con las TIC para cada grupo; es probable que existan muchos otros tipos, dependiendo del grado de vulnerabilidad y de las circunstancias.

No hemos tratado de clasificar estos grupos bajo epígrafes o temas más amplios. Hacerlo sería contradictorio con una de nuestras principales recomendaciones: que la vulnerabilidad se considere dinámica y compleja, no una "etiqueta" que se aplica a determinados grupos o individuos. Etiquetar a grandes grupos de la sociedad como vulnerables puede, de hecho, aumentar la discriminación y la estigmatización que sufren.

¿Cómo afectan las cuestiones éticas y jurídicas en torno a las TIC a las personas vulnerables?

Las cuestiones éticas y jurídicas en torno a las TIC -como las relacionadas con la privacidad de los datos, la comercialización de los mismos y el creciente uso de nuevas tecnologías como el reconocimiento facial- afectan a todos los miembros de la sociedad. Pero, como ya se ha dicho, las personas y grupos vulnerables de la sociedad corren a menudo un mayor riesgo de sufrir daños que otros, y lo hacen de diferentes maneras; el recuadro 2 presenta algunas de ellas.

Recuadro 2. ¿Cómo afectan las TIC a las personas vulnerables en particular?

- Estas personas y grupos no sólo son vulnerables en sí mismos; también son más vulnerables a que sus datos se utilicen de forma que los ponga en peligro (por ejemplo, una mayor vigilancia). Aunque este es un riesgo para todos los ciudadanos, las personas vulnerables suelen enfrentarse a un riesgo mayor. Por ejemplo, pueden ser incapaces de dar su consentimiento o no dominar la lengua o lenguas nacionales del país en el que viven.
- Los desequilibrios de poder entre los interesados y los responsables del tratamiento pueden verse exacerbados con los interesados vulnerables. Por ejemplo, en los casos en los que los datos personales se prestan a un uso indebido por parte de los responsables del tratamiento, las personas vulnerables pueden verse menos capacitadas para controlarlo o impedirlo, porque tienen menos poder, conocimiento o conciencia del problema.
- Existe el riesgo de una (mayor) estigmatización, ya que se agrupa a las personas con fines de investigación y análisis.

Estos riesgos no sólo están relacionados con la naturaleza de la vulnerabilidad de una persona, sino también con el tipo de datos sobre ella que se recogen y utilizan. Ciertos tipos de datos -como la información sobre la religión, el historial médico o la orientación sexual de una persona- pueden entrañar un mayor riesgo, dependiendo del lugar y el contexto en que se utilicen.

Además, como se ha mencionado, la vulnerabilidad puede cambiar con el tiempo, lo que plantea problemas en cuanto a los datos personales. Las personas o grupos que no son vulnerables cuando comparten sus datos pueden llegar a serlo más adelante. En consecuencia, las condiciones en las que dieron su consentimiento para que se utilizaran sus datos pueden dejar de ser válidas. Los equipos de investigación con pocos recursos pueden carecer del tiempo, el dinero y, en algunos casos, la información que necesitan para aplicar medidas que garanticen el cumplimiento de los derechos de los datos y la privacidad de sus sujetos.

Como antes, el mensaje es el siguiente: ¡la vulnerabilidad es compleja! El cuadro 3 destaca algunas de las formas en que los grupos vulnerables de la sociedad pueden verse especialmente afectados en relación con las cuestiones éticas y jurídicas en torno a las TIC y los datos. No significa que los supuestos indiciados se den a todos estos grupos; son simplemente ejemplos para destacar las formas en que puede darse la vulnerabilidad, y la vulnerabilidad relacionada con las TIC y los datos.

Cuadro 3. Ejemplos de grupos vulnerables en Europa, y la naturaleza de sus vulnerabilidades

Grupo vulnerable	Posible vulnerabilidad	Posible vulnerabilidad con respecto a las TIC y los datos

Mujeres	Las mujeres embarazadas o en periodo de lactancia pueden ser, o sentirse, más vulnerables que otras mujeres; por ejemplo, debido a cambios en su salud. Las mujeres en edad fértil corren un mayor riesgo de ser discriminadas en los procesos de contratación.	Las mujeres que se han sometido a una cirugía de reasignación de sexo pueden tener almacenados datos sobre ellas que ya no reflejan su condición.
Padres o tutores solteros / padres o tutores de niños vulnerables o dependientes	Las tareas de cuidado adicionales pueden dejarles con menos tiempo y recursos para cuidar de sí mismos, lo que aumenta su vulnerabilidad.	Es posible que tengan menos tiempo para leer y comprender los temas relacionados con las TIC.
Personas sin hogar	Las personas en esta situación suelen experimentar mayores riesgos para la salud, y un mayor riesgo de violencia, desempleo y pobreza.	Es probable que tengan menos acceso a la información sobre estos temas que otros miembros de la sociedad. Además, es posible que se recojan datos sobre ellos sin su consentimiento informado (por ejemplo, cuando recurren a servicios para personas sin hogar prestados por organizaciones benéficas).
Personas con adicción(es), como drogadicción y/o alcoholismo	Las personas que viven con adicciones se enfrentan a muchas formas de vulnerabilidad, como los riesgos para la salud, un mayor riesgo de violencia, el desempleo y la pobreza.	Pueden tener una capacidad reducida para comprender la información sobre sus derechos en materia de TIC y de datos.
Personas que sufren o corren el riesgo de sufrir violencia doméstica y abusos psicológicos y/o sexuales	Es probable que las personas que se enfrentan a la violencia y los abusos experimenten una serie de vulnerabilidades, como problemas de salud física y mental.	En algunas situaciones, el acceso de las víctimas a la información puede estar restringido como parte del abuso que sufren; por ejemplo, pueden vivir con una pareja que les restringe lo que pueden hacer o a dónde pueden ir.

Personas que han sido sometidas a tortura, violación u otras formas graves de violencia psicológica, física o sexual, como las víctimas de la mutilación genital femenina	Entre otras muchas formas de vulnerabilidad, las personas que las han padecido son propensas a sufrir traumas a largo plazo u otros daños psicológicos, además de las repercusiones en su salud física.	La reticencia a compartir su información personal -por ejemplo, si son inmigrantes o carecen de estatus legal en un país- puede hacer que las víctimas estén menos dispuestas a buscar ayuda médica o a informar a la policía de su situación.
Víctimas de la trata de seres humanos	Las leyes de un país pueden impedir que accedan a los métodos de apoyo disponibles; por ejemplo, por el miedo a ser deportadas cuando los soliciten.	Estas personas pueden no tener acceso a servicios o información en línea, según las condiciones en las que se encuentren (por ejemplo, confinamiento ilegal, esclavitud moderna). Al mismo tiempo, al no estar "en el sistema", pueden ser pasados por alto por los proveedores de servicios que podrían ayudarles.
Minorías religiosas	Puede ser difícil borrar los prejuicios sociales sobre estos grupos.	Algunas personas pueden considerar que su religión es un asunto privado, pero algunos procesos inevitables de recogida de datos siguen exigiendo que las personas declaren su religión (por ejemplo, la normativa fiscal en Alemania).
Personas LGBTQIA+[9] y minorías sexuales	Las personas de este grupo siguen sufriendo una discriminación generalizada en toda Europa.	La nueva tecnología que viola la privacidad (por ejemplo, la elaboración de perfiles faciales) puede ser más probable que se dirija a estos grupos.
Poblaciones transgénero	Las personas de este grupo siguen sufriendo una discriminación generalizada en toda Europa. Por ejemplo, Hungría aprobó recientemente una ley que pone fin al reconocimiento legal de la condición de trans.[10]	Las casillas para marcar hombre/mujer, que suelen aparecer en muchos formularios de recogida de datos, las discriminan, mientras que el lenguaje "tradicional" utilizado en muchas situaciones en línea (por ejemplo, él/ella, su) hace lo mismo.
Prisioneros	Los presos se ven aislados de sus redes de apoyo, y a menudo se enfrentan a amenazas adicionales, como un mayor riesgo de violencia	Estar en prisión puede reducir su acceso a la información sobre sus datos y derechos digitales.

	en la cárcel.	
Personas que salen de la cárcel	Los presos recién liberados pueden carecer de redes de apoyo y tener dificultades para conseguir un empleo o una vivienda.	Su estado vulnerable puede reducir el acceso a la información sobre sus datos y derechos digitales. Dependiendo del tiempo que hayan estado en prisión, pueden desconocer las novedades en materia de protección de datos y privacidad.
Personas con escasa o nula formación	Su vulnerabilidad se ve agravada por el desconocimiento o la imposibilidad de comprender los sistemas de apoyo para reducir su vulnerabilidad. Suelen tener ingresos más bajos, lo que aumenta su vulnerabilidad financiera.	La información sobre las TIC y los derechos de los datos tiende a ser compleja y difícil de entender; el bajo nivel educativo aumentará esta barrera.
Personas que están fuera de la formación y/o educación	Esta situación puede agravar muchos tipos de vulnerabilidad, como la financiera, la sanitaria (especialmente la mental) y las redes de apoyo.	La información sobre las TIC y los derechos digitales suele pasar por entornos formales, como las escuelas o los colegios. Estar fuera de ellos reduce el acceso de las personas a dicha información.
Personas desinformadas, incluidas las que no son capaces de entender la información proporcionada	La información es poder; aquellos que no pueden acceder o entender la información diseñada para ayudarles son, en consecuencia, más vulnerables que los que pueden hacerlo.	Esto se aplica tanto a la información digital como a las formas de información no digitales.
Personas con dificultades de aprendizaje, como dislexia, disortografía, disgrafía y discalculia	Las dificultades de aprendizaje pueden hacer que las personas sean vulnerables de múltiples maneras. Por ejemplo, las personas que no pueden entender la información diseñada para ayudarles son, en consecuencia, más vulnerables que las que sí pueden hacerlo.	Estas y otras dificultades de aprendizaje dificultan la búsqueda y/o comprensión de información relacionada con el derechos de protección de datos, la confidencialidad de los datos, las TIC, etc.

Grupos indígenas	Estos grupos amenazados o que experimentan una disminución de su número pueden requerir la protección de su patrimonio cultural, por ejemplo, a través de su conservación en museos.	Los datos de procedencia -sobre el origen, la propiedad y la custodia de los objetos- no siempre son captados por las TIC; en otros casos, los conocimientos de los indígenas pueden almacenarse sin su conocimiento o aprobación.
Los sami[11]	Como grupo minoritario que vive en una de las regiones más duras de Europa, los sami sufren muchas formas de vulnerabilidad. Un informe del Relator Especial de las Naciones Unidas sobre los derechos de los pueblos indígenas concluyó que Suecia, Noruega y Finlandia no cumplen sus objetivos declarados de garantizar los derechos humanos del pueblo sami.[12]	Los sami siempre han sido objeto de diferentes tipos de investigación. Esto incluye investigaciones basadas en registros y biobancos. En ocasiones, estos proyectos han obviado las consideraciones éticas, por ejemplo, al no comunicar plenamente que un proyecto se dirige al pueblo sami.
Minorías étnicas	Las minorías étnicas de un país suelen ser objeto de discriminación y pueden presentar una mayor prevalencia de varios tipos de vulnerabilidad (por ejemplo, bajos ingresos, baja educación, problemas de salud, barreras lingüísticas).	Pueden tener menos acceso a la información sobre sus derechos a los datos (por ejemplo, si no está disponible en su lengua materna).
Refugiados	Los refugiados suelen ser discriminados y pueden presentar una mayor prevalencia de varios tipos de vulnerabilidad (por ejemplo, bajos ingresos, baja educación, problemas de salud, barreras lingüísticas).	Pueden ser reacios a proporcionar datos personales por temor a su uso indebido. Esto puede excluirlos de los beneficios potenciales que pueden ofrecer las TIC.
Solicitantes de asilo	Los solicitantes de asilo pueden sufrir problemas de salud mental o traumas, por ejemplo si han huido de una zona de guerra o una catástrofe.	Pueden ser reacios a proporcionar datos personales por temor a un uso indebido. Esto puede excluirlos de los beneficios potenciales que pueden ofrecer las TIC.

Migrantes	La naturaleza de las vulnerabilidades de los migrantes varía mucho. Los migrantes más pobres pueden experimentar muchas de las vulnerabilidades a las que se enfrentan los refugiados y los solicitantes de asilo, mientras que los migrantes de altos ingresos pueden experimentar vulnerabilidades muy diferentes (por ejemplo, estrés, resentimiento entre la población local).	Las barreras lingüísticas pueden aumentar el riesgo de que sus datos personales se utilicen indebidamente. Además, la normativa en materia de datos y TIC de su nuevo país puede diferir de aquella a la que están acostumbrados.
Miembros de comunidades itinerantes	Las comunidades itinerantes se enfrentan a menudo a la discriminación y pueden encontrarse fuera de los sistemas de apoyo formales (por ejemplo, escuelas, atención sanitaria).	Pueden ser reacios a proporcionar datos personales por temor a un uso indebido. Esto puede excluirlos de los beneficios potenciales que pueden ofrecer las TIC.
Miembros de la comunidad gitana	Los gitanos han sido históricamente perseguidos en toda Europa, lo que hace que muchos de ellos sean más vulnerables que otras poblaciones, en términos de bajos ingresos, empleo, amenazas a su bienestar y muchas otras formas de vulnerabilidad.	Pueden ser reacios a proporcionar datos personales por temor a un uso indebido. Esto puede excluirlos de los beneficios potenciales que pueden ofrecer las TIC.
Personas enfermas o lesionadas, incluidos los pacientes hospitalizados y de larga duración	Los problemas de salud hacen que las personas sean inmediatamente vulnerables y pueden agravar otros tipos de vulnerabilidad (por ejemplo, la pérdida de ingresos).	Es posible que no puedan dar su consentimiento para el uso de sus datos, por ejemplo, si están sedados, confusos o inconscientes. O pueden dar su consentimiento con demasiada facilidad, por ejemplo, si quieren que la investigación médica les mejore (vulnerabilidad temporal).
Personas con enfermedades crónicas y/o de larga duración, o con múltiples enfermedades crónicas	La vulnerabilidad viene determinada por la naturaleza y la gravedad de la enfermedad. Por ejemplo, muchas de estas afecciones reducen la capacidad de las personas para trabajar y obtener ingresos.	Estas personas suelen quedar excluidas de la información en línea, en función de la aplicación y disponibilidad de herramientas TIC inclusivas. Por ejemplo, las personas con epilepsia pueden ser vulnerables a la exclusión de ciertos recursos online no inclusivos debido a los destellos/luz de las pantallas

		(epilepsia fotosensible).[13]
Personas que viven en residencias	A las personas que viven en residencias (también conocidas como viviendas asistidas) se les quitan muchas decisiones cotidianas. Esta falta de control sobre sus vidas puede aumentar su vulnerabilidad en muchos aspectos (por ejemplo, su dieta, su atención médica, sus finanzas).	Para muchas personas en residencias, los datos sobre ellas pueden estar controlados por otros, como los familiares del personal de su residencia. Esto reduce su capacidad de controlar, o incluso de influir, en el uso de sus datos personales.
Personas con discapacidades y trastornos, ya sean físicos o mentales (o ambos), y tanto temporales como permanentes	Las vulnerabilidades vienen determinadas por la naturaleza y la gravedad de las discapacidades y los trastornos. Por ejemplo, las personas con movilidad limitada pueden depender de otros, lo que aumenta su vulnerabilidad a la explotación o al abandono.	Algunas discapacidades pueden hacer que las personas necesiten ayuda para acceder a los datos o compartirlos, o para entender las declaraciones de privacidad o dar su consentimiento. Esto reduce su control sobre la privacidad de sus datos.
Personas con capacidad de comunicación limitada, como impedimentos del habla	Una capacidad de comunicación limitada impide que las personas soliciten o contribuyan a la información en una serie de escenarios. Esto puede significar que sus necesidades, opiniones o expectativas no se tengan plenamente en cuenta (por ejemplo, en los debates públicos).	Algunas limitaciones en la capacidad de comunicación pueden hacer que las personas necesiten ayuda para acceder a los datos o compartirlos, o para entender las declaraciones de privacidad / dar su consentimiento. Esto reduce su control sobre la privacidad de sus datos.

Personas con discapacidad visual o ciegas	Aunque existen muchas disposiciones para los discapacitados visuales y los ciegos, éstas pueden no estar disponibles o no ser asequibles para todas las personas, lo que aumenta su vulnerabilidad.	Es probable que utilicen un software que les lea la pantalla/plataforma, lo que reduce la privacidad de esa información. Además, pueden ver restringido su acceso a la información, por ejemplo, si los sitios web a los que necesitan acceder no permiten que el software lo lea todo (por ejemplo, las opciones de las casillas de verificación).
Personas excluidas por el idioma, o que se enfrentan a barreras lingüísticas	Las personas que no hablan la lengua de su país de residencia (por ejemplo, algunos inmigrantes y refugiados, o minorías como los criollos en Portugal) tienen un acceso reducido a la información sobre las medidas de apoyo, lo que aumenta su vulnerabilidad.	Los no nativos de un país, o los hablantes de lenguas minoritarias, suelen carecer de información en su propia lengua sobre sus derechos digitales.
Personas que no dominan el inglés	Dado que el inglés es la lengua predominante en toda Europa, es posible que cierta información sólo esté disponible, o de forma más destacada, en esta lengua. Las personas que no hablan o entienden el inglés pueden encontrarse en desventaja con respecto a las que sí lo hablan.	Gran parte de la información sobre los derechos de los datos y la privacidad está en inglés, lo que pone a estos grupos en desventaja. También es probable que tengan menos acceso a compartir sus opiniones sobre el desarrollo y el progreso de las TIC si las encuestas y los debates se realizan en inglés.
Hijos / dependientes / menores	Los jóvenes son intrínsecamente vulnerables, ya que carecen de muchos de los atributos que reducen la vulnerabilidad (por ejemplo, tamaño, fuerza, educación completa, independencia, ingresos).	Los jóvenes no pueden consentir legalmente el uso de sus datos. Es posible que no sepan cómo quejarse del uso indebido de sus datos, o que no sepan que pueden hacerlo.
Adultos emergentes (18-25 años)	En muchos países, este grupo de edad tiene dificultades para acceder a las ventajas que tenían las generaciones mayores, como empleos seguros y bien remunerados o viviendas asequibles.	La falta de empleo y/o de vivienda puede dificultar el acceso a la información sobre los derechos digitales y las TIC (por ejemplo, debido a la falta de acceso a Internet en casa).

Adultos tempranos (20-40)	En muchos países europeos (por ejemplo, Portugal y los Países Bajos), las personas de este grupo de edad tienen una mayor tendencia a trabajar por cuenta propia o como autónomos. Por ello, especialmente en momentos de crisis (como la pandemia de Covid-19), son vulnerables a los cambios drásticos en sus ingresos. También pueden tener familias jóvenes y, por tanto, un mayor nivel de vulnerabilidad (por ejemplo, financiera).	Por el contrario, pueden tener potencialmente mayores niveles de conocimientos técnicos y educación que otros grupos de edad. Esto significa que es menos probable que sean vulnerables a los problemas legales y éticos en torno a la privacidad de los datos, las TIC y sus derechos digitales.
Personas mayores, frágiles o incapacitadas	La vejez es una etapa de la vida intrínsecamente vulnerable, ya que las personas pueden volverse más débiles y depender más de los demás.	Aunque la vejez no siempre va unida al analfabetismo digital, es posible que las personas mayores sean menos conscientes de las cuestiones legales y éticas relacionadas con las TIC, los datos y la privacidad, en comparación con la "generación digital" que ha crecido con esta tecnología.
Personas en situación de desempleo o subempleo, tanto a corto como a largo plazo	El desempleo agrava otras formas de vulnerabilidad, especialmente la financiera y la de la vivienda. También puede provocar problemas de salud y de salud mental.	Los desempleados pueden perderse la formación y la información sobre las TIC que ofrecen los centros de trabajo. Puede que no tengan acceso a Internet en casa (por motivos económicos), lo que significa que desconocen la información sobre las TIC, que cada vez se comparte más en Internet.
Personas de bajo nivel económico	Al igual que el desempleo, la baja situación económica agrava otras formas de vulnerabilidad, especialmente la financiera y la de la vivienda. También puede provocar problemas de salud y de salud mental.	Las personas de este grupo pueden no tener acceso a Internet en casa (por motivos económicos), lo que significa que no conocen la información sobre las TIC, que cada vez se comparte más en Internet.

Clientes y beneficiarios de la asistencia social	Las personas que reciben asistencia social pueden experimentar muchas otras formas de vulnerabilidad (por ejemplo, mala salud, bajos ingresos, vivienda insegura).	Las personas de este grupo pueden carecer de acceso a la formación e información sobre las TIC que se ofrece en los lugares de trabajo, y/o pueden no tener acceso en línea en casa (por razones económicas), lo que significa que no conocen la información sobre las TIC, que se comparte cada vez más en línea.
Personas analfabetas	Gran parte de la información que rige nuestras vidas y pretende ayudarnos se proporciona principalmente en forma escrita. El analfabetismo es una barrera importante para acceder a ella, lo que deja a estas personas en situación de vulnerabilidad. El analfabetismo también puede ser un factor que influya en la situación económica de las personas.	Mucha de la información sobre cuestiones legales y éticas en torno a las TIC se comparte por escrito, especialmente en línea. El analfabetismo significa que la gente será menos consciente de esta información y menos capaz de entenderla.
Personas analfabetas digitales o con escasos conocimientos tecnológicos	Gran parte de la información que rige nuestras vidas y que pretende ayudarnos se proporciona cada vez más en línea; por ejemplo, las citas médicas que sólo se pueden reservar en línea, o la información que sólo se comparte a través de las redes sociales.	Estas personas corren el riesgo de quedarse atrás a medida que la información y los servicios se mueven cada vez más en línea.
Comunidades offline	No se trata de la misma vulnerabilidad que el analfabetismo digital: es una cuestión de la falta de acceso o infraestructura, más que de habilidades/capacidad. Sin embargo, las comunidades sin conexión se enfrentarán a muchas de las mismas vulnerabilidades que los analfabetos digitales.	Estas personas corren el riesgo de quedarse atrás a medida que la información y los servicios se mueven cada vez más en línea.

Las personas con acceso limitado a las infraestructuras públicas	Por ejemplo, los habitantes de las zonas rurales de algunos países carecen de un buen acceso a infraestructuras como hospitales, bibliotecas, banda ancha potente, guarderías y otros sistemas de apoyo. Esto los hace relativamente vulnerables, especialmente durante crisis como la pandemia de Covid-19.	La falta de infraestructuras puede extenderse a un acceso limitado a Internet (por ejemplo, una banda ancha débil o cara) y a otros servicios de TIC. Esto puede reducir el acceso de las personas a la información sobre sus derechos relacionados con las TIC, los datos y la privacidad.
Comunidades que quedan al margen de los procesos de investigación	La ciencia y la investigación sustentan muchos elementos de la sociedad, como la asistencia sanitaria, la gobernanza y la educación. Al estar fuera de estos procesos, ya sea como investigadores o como sujetos de datos, estas comunidades se encuentran con que sus vidas están influenciadas por procesos de investigación en los que no tienen participación ni voz. En consecuencia, las políticas basadas en la investigación pueden no abordar sus necesidades particulares o reducir sus vulnerabilidades específicas.	Esto también es cierto en el caso de la investigación basada en las TIC: las comunidades que no tienen interés o voz en el proceso, o que no tienen acceso a los resultados, pueden encontrarse con que las repercusiones de dicha investigación (por ejemplo, las políticas, las decisiones de financiación) no abordan sus necesidades o no las apoyan. Por ejemplo, las encuestas o cuestionarios en línea son un método de investigación cada vez más común, pero excluyen casi totalmente a las comunidades fuera de línea.
Personas afectadas por fenómenos ajenos a su voluntad	Los acontecimientos o fenómenos extremos pueden causar una vulnerabilidad inesperada. Si bien pueden adoptar la forma de catástrofes naturales (p. ej., volcanes, pandemias mundiales) y fenómenos climáticos extremos (p. ej., sequías, inundaciones), también pueden adoptar la forma de acontecimientos vitales (p. ej., enfermedades inesperadas, accidentes, pérdida de empleo, una muerte en la familia). El carácter inesperado de estos sucesos hace que sea difícil prepararse para ellos, lo que hace que las personas sean menos resistentes.	Tras una crisis, las personas pueden estar cansadas, estresadas o confusas y, por tanto, compartir sus datos personales con más facilidad (es decir, con menos atención) o hacerlo para acceder a determinados servicios (por ejemplo, apoyo tras una catástrofe o atención sanitaria de urgencia). Un ejemplo reciente es la pandemia de Covid-19, en la que las libertades personales y las cuestiones de privacidad se dejaron a menudo de lado para combatir la propagación del virus.

Cualquier ciudadano que, por cualquier motivo, se considere vulnerable	La naturaleza y la gravedad de esta vulnerabilidad, relacionada o no con las TIC, depende de la percepción del sujeto. Sin embargo, es importante reconocer que la vulnerabilidad no es una cuestión simple y medible, sino que puede ser subjetiva, oculta y personal.

Fuente: Adaptado del informe del taller COST Action/PANELFIT celebrado en marzo de 2020; complementado con los demás recursos que se enumeran al final de esta guía.

¿Qué puedes hacer?

Está claro que las personas vulnerables deberían recibir más atención en relación con los debates éticos y jurídicos en torno a las TIC, y debería haber mayores esfuerzos para incluirlas en el desarrollo y la implantación de las TIC y otras nuevas tecnologías que les afectarán (por ejemplo, la inteligencia artificial). Lo ideal sería que hubiera salvaguardias específicas para proteger a las personas vulnerables en cuanto a la privacidad de sus datos y al uso que se hace de ellos.

Sin embargo, como se ha señalado, es difícil -quizá incluso imposible- crear una lista definitiva de todos los grupos vulnerables de la sociedad. Ni siquiera es deseable, debido a la naturaleza dinámica de la vulnerabilidad y al riesgo de simplificar en exceso la complejidad de las situaciones de las personas, o de aumentar el riesgo de estigmatización. Por ello, las salvaguardias específicas para los derechos digitales de las personas vulnerables pueden tardar en entrar en vigor, si es que lo hacen.

Mientras tanto, hay acciones que todos los ciudadanos pueden llevar a cabo para garantizar el cumplimiento de los derechos digitales de las personas vulnerables. La figura 1 esboza una serie de acciones.

También hay medidas específicas que los responsables del tratamiento pueden adoptar para proteger a los interesados vulnerables. La figura 2 ilustra algunas de ellas.

FIGURA 1	**FIGURA 2**
Interesados	**Responsables del tratamiento**
¿Quién? *Todos los ciudadanos, incluidos los ciudadanos vulnerables y los que tienen responsabilidad sobre los ciudadanos vulnerables*	**¿Quién?** *Investigadores, empleados, empresas, autoridades, organizadores de proyectos, etc.*

Cuando alguien solicite tus datos, comprueba lo siguiente: ¿Quiénes son? ¿Para qué los van a utilizar? ¿Cuánto tiempo los conservarán? ¿Con quién los van a compartir?	Al principio del proceso, pregúntese: ¿Quiénes son los sujetos de datos vulnerables en mi proyecto, proceso o tarea? ¿Cómo son de vulnerables?
Si te proporcionan información general (por ejemplo, condiciones, formularios de consentimiento), compruébalo: ¿Los entiendes? Si no es así, pida una versión más fácil de entender (por ejemplo, en su primera lengua).	Considere los riesgos a los que se enfrentarán los miembros de cada grupo vulnerable cuando utilice sus datos, y piense en cómo pueden reducirse o superarse.
Si todavía no está seguro o no está satisfecho con el uso de sus datos, infórmese. Puede hacerlo a través de una oficina de atención al ciudadano o de la autoridad nacional de protección de datos.	Cuando pida datos personales a ciudadanos vulnerables, compruebe: ¿Han entendido para qué se van a utilizar sus datos? ¿Cómo puedo facilitarles la comprensión? ¿Realmente han dado su consentimiento para su uso libremente?
En la mayoría de los casos, usted tiene derecho a retirar su consentimiento para que se utilicen sus datos. Antes de compartir sus datos, compruebe: ¿Cómo puedo retirar el consentimiento más adelante? ¿Con quién tengo que ponerme en contacto?	No busque soluciones concretas, ni trate el tratamiento de la vulnerabilidad como una "casilla a marcar" en su proyecto. Por el contrario, considérelo como un proceso continuo que debe ser revisado regularmente.
Si se han violado sus derechos de datos inmediatamente, póngase en contacto con la oficina de protección de datos correspondiente. Si no te sientes cómodo haciéndolo, en la tabla 4 hay una lista de organizaciones que podrían ayudarte	Considere la protección de datos de los grupos vulnerables en cada fase del proyecto: ¿Supone esta actividad un riesgo para los grupos vulnerables? ¿Qué medidas puede implementar para mitigar ese riesgo?

Recursos útiles

Hay varias organizaciones, sitios web y proyectos dedicados a ayudar a las personas a entender sus derechos en nuestro mundo cada vez más digital, y que apoyan a los grupos vulnerables de diferentes maneras. En el cuadro 4 hemos incluido una lista de ONG con las que puedes ponerte en contacto y buscar información/ayuda en caso de falta de privacidad de datos. Si quieres saber más sobre estos temas, te recomendamos las siguientes.

Tabla 4. Ejemplos de organizaciones que ofrecen apoyo a grupos vulnerables en Europa.

Grupo vulnerable	ONG	Información de contacto de la ONG (por si acaso)
Mujeres	Lobby Europeo de Mujeres: https://womenlobby.org/?lang=en	ewl@womenlobby.org
Padres o tutores solteros / padres o tutores de niños vulnerables o dependientes	COFACE Familias Europa: https://coface-eu.org/about-us/	secretariat@coface-eu.org
Personas sin hogar	FEANTSA: https://www.feantsa.org/en/about-us/what-is-feantsa	information@feantsa.org
	Homeless in Europe International: https://www.homelessineurope.eu/	homelessineuropehope@gmail.com
Personas con adicción(es), como drogadicción y/o alcoholismo	Dianova International: https://www.dianova.org/	switzerland@dianova.org
Personas que sufren o corren el riesgo de sufrir violencia doméstica y abusos psicológicos y/o sexuales	Mujeres contra la violencia en Europa: https://wave-network.org/	office@wave-network.org
	Rape Crisis Network Europe --> También tienen una larga lista de organizaciones (algunas son ONG): https://www.rcne.com/contact/countries/	Cada organización tiene su propio correo electrónico
Personas que han sido sometidas a tortura, violación u otras formas graves de violencia psicológica, física o sexual, como las víctimas de la mutilación genital femenina	Consejo Internacional para la Rehabilitación de las Víctimas de la Tortura: https://www.irct.org/	irct@irct.org
	Red europea para acabar con la MGF: https://www.endfgm.eu/who-we-are/vision-and-mission/	https://www.endfgm.eu/resources/resource-items/contact/
Víctimas de la trata de seres humanos	La Strada International: https://www.lastradainternational.org/	info@lastradainternational.org
Minorías religiosas	Minority Rights Group International: https://minorityrights.org/about-us/	minority.rights@minorityrights.org
Personas LGBTQIA+[1] y minorías sexuales	Aquí tienes una larga lista con ONG de diferentes países: https://www.ilga-europe.org/who-we-are/members	

Poblaciones transgénero	Europa transgénero: https://tgeu.org/	tgeu@tgeu.org
Prisioneros	Asociación Europea de Educación Penitenciaria: https://www.epea.org/epea/	secretary@epea.org
	Observatorio Penitenciario Europeo: http://www.prisonobservatory.org/	info@prisonobservatory.org
Personas que salen de la cárcel	Observatorio Penitenciario Europeo: http://www.prisonobservatory.org/	info@prisonobservatory.org
Personas con escasa o nula formación	Waag - https://waag.org/en	https://waag.org/en/contact
Personas que están fuera de la formación y/o educación	Waag - https://waag.org/en	https://waag.org/en/contact
Personas desinformadas, incluidas las que no son capaces de entender la información proporcionada	Asociación Europea para los Intereses de los Espectadores (EAVI): https://eavi.eu/about-us/	eavi@eavi.eu
Personas con dificultades de aprendizaje, como dislexia, disortografía, disgrafía y discalculia	Asociación Europea de Dislexia: https://eda-info.eu/about-the-eda/	eda-info@eda-info.eu
Grupos indígenas	Minority Rights Group International: https://minorityrights.org/about-us/	minority.rights@minorityrights.org
	Red Europea de Pueblos Indígenas: https://www.enip.eu/	enip@enip.eu
Los sami[2]	Consejo Sami: https://www.saamicouncil.net/en/the-saami-council	saamicouncil@saamicouncil.net
Minorías étnicas	Minority Rights Group International: https://minorityrights.org/about-us/	minority.rights@minorityrights.org
	Red Europea contra el Racismo: enar-eu.org/About-us	info@enar-eu.org
Refugiados	Consejo Europeo de Refugiados y Exiliados: https://ecre.org/	vzahle@ecre.org
	Cruz Roja Europa:	infoboard@redcross.eu

	https://redcross.eu/about	
Solicitantes de asilo	Consejo Europeo de Refugiados y Exiliados: https://ecre.org/	vzahle@ecre.org
	Cruz Roja Europa: https://redcross.eu/about	infoboard@redcross.eu
Migrantes	Plataforma Europea de ONG de Asilo y Migración: http://www.ngo-platform-asylum-migration.eu/	comms@migpolgroup.com
	Cruz Roja Europa: https://redcross.eu/about	infoboard@redcross.eu
Miembros de comunidades itinerantes	Waag - https://waag.org/en	https://waag.org/en/contact
Miembros de la comunidad gitana	Centro Europeo de Derechos de los Gitanos: http://www.errc.org/	office@errc.org
Personas enfermas o lesionadas, incluidos los pacientes hospitalizados y de larga duración	Personas con lesiones cerebrales y sus familias: https://bif-ec.com/about-2/	https://bif-ec.com/contact/
Personas con enfermedades crónicas y/o de larga duración, o con múltiples enfermedades crónicas	EUROFEA: https://www.euforea.eu/ngo	contact@euforea.eu
Personas que viven en residencias	EDAD: https://www.age-platform.eu/about-age	info@age-platform.eu
Personas con discapacidades y trastornos, ya sean físicos o mentales (o ambos), y tanto temporales como permanentes	Inclusión Europa: https://www.inclusion-europe.eu/what-we-do/	secretariat@inclusion-europe.org
Personas con capacidad de comunicación limitada, como impedimentos del habla	Inclusión Europa: https://www.inclusion-europe.eu/what-we-do/	secretariat@inclusion-europe.org
Personas con discapacidad visual o ciegas	Unión Europea de Ciegos: https://www.euroblind.org/	ebu@euroblind.org
Personas excluidas por el idioma, o que se enfrentan a barreras lingüísticas	Consejo Europeo de Refugiados y Exiliados: https://ecre.org/	vzahle@ecre.org
Personas que no dominan el inglés	Consejo Europeo de Refugiados y Exiliados: https://ecre.org/	vzahle@ecre.org
Hijos / dependientes / menores	Eurochild: https://www.eurochild.org/	info@eurochild.org

Adultos emergentes (18-25 años)	ERYICA - Agencia Europea de Información y Asesoramiento Juvenil: https://www.eryica.org/eryica	secretariat@eryica.org
Adultos tempranos (20-40)	ERYICA - Agencia Europea de Información y Asesoramiento Juvenil: https://www.eryica.org/eryica	secretariat@eryica.org
Personas mayores, frágiles o incapacitadas	EDAD: https://www.age-platform.eu/about-age	info@age-platform.eu
Personas en situación de desempleo o subempleo, tanto a corto como a largo plazo	La Red Europea de Lucha contra la Pobreza (EAPN): https://www.eapn.eu/who-we-are/what-is-eapn/	https://www.eapn.eu/who-we-are/contact-us/
Personas de bajo nivel económico	La Red Europea de Lucha contra la Pobreza (EAPN): https://www.eapn.eu/who-we-are/what-is-eapn/	https://www.eapn.eu/who-we-are/contact-us/
Clientes y beneficiarios de la asistencia social	Servicios Sociales Europa: https://www.socialserviceseurope.eu/why-we-do-it	info@socialserviceseurope.eu
Personas analfabetas	World Literacy Foundation (Esta ONG es mundial, no europea, pero tiene una oficina en el Reino Unido): https://worldliteracyfoundation.org/about-us/	Formulario de contacto al final de la página: https://worldliteracyfoundation.org/about-us/
Personas analfabetas digitales o con escasos conocimientos tecnológicos	Todo digital: https://all-digital.org/about-us/	contact@all-digital.org
	Red Europea de Aprendizaje Digital: http://dlearn.eu/	http://dlearn.eu/contact/
Comunidades offline	Oficina de la UE de la CRUZ ROJA	+32 (0) 2 230 54 64
Las personas con acceso limitado a las infraestructuras públicas	PREPARE - Asociación para la Europa Rural: http://www.preparenetwork.org/partnership/partners#ecovast	Kim.Smedslund@suomenkylat.fi
	Consejo Europeo para el Pueblo y la Ciudad Pequeña: http://www.ecovast.org/english/about_e.html	valeriecarter@ecovast.org
Comunidades que quedan al margen de los procesos de investigación	Centro Europeo para las Cuestiones de las Minorías: https://www.ecmi.de/	info@ecmi.de
Personas afectadas por fenómenos ajenos a su voluntad	Red de Acción Climática (CAN) Europa:	info@caneurope.org

	https://caneurope.org/about-us/	
Cualquier ciudadano que, por cualquier motivo, se considere vulnerable	Waag - https://waag.org/en	https://waag.org/en/contact

Personas y grupos vulnerables

Statewatch fomenta la publicación de periodismo de investigación e investigación crítica en Europa en los ámbitos del Estado, la justicia y los asuntos de interior, las libertades civiles, la responsabilidad y la apertura. Disponible en inglés. www.statewatch.org/about/

El sitio web de **Protección Social y Derechos Humanos** contiene una guía sobre los grupos desfavorecidos y vulnerables de la sociedad. Disponible en inglés.

https://socialprotection-humanrights.org/key-issues/disadvantaged-and-vulnerable-groups/

Estos vídeos de la Iniciativa de Accesibilidad a la Web exploran las repercusiones de una mayor accesibilidad a la web y los beneficios para todos, con ejemplos de diversas situaciones. Se encuentran disponibles en inglés.

www.w3.org/WAI/perspective-videos/

Cuestiones jurídicas y éticas en torno a las TIC, los datos y la privacidad

El proyecto **Global Data Justice** se centra en los diversos debates y procesos que se producen en torno a la gobernanza de los datos en diferentes regiones, extrayendo los principios y necesidades generales que pueden impulsar la gobernanza de la tecnología de datos en dirección a la justicia social. Disponible en inglés. https://globaldatajustice.org/

El **Laboratorio de Justicia de Datos** examina la relación entre la "dataficación" y la justicia social, como la política y las repercusiones de los procesos basados en datos y el Big Data. Su sitio web contiene muchas publicaciones útiles y noticias sobre próximos eventos. Disponible en inglés. https://datajusticelab.org/

La línea de ayuda para la seguridad digital de Access Now trabaja con individuos y organizaciones de todo el mundo para mantenerlos seguros en el entorno en línea. Si se encuentra en una situación de riesgo, pueden ayudarle a mejorar sus prácticas de seguridad digital. Si ya está siendo atacado, proporcionan asistencia de emergencia de respuesta rápida. Disponible en alemán, árabe, español, francés, inglés, italiano, portugués, ruso y tagalo. www.accessnow.org/help/

El kit de desintoxicación de datos de Tactical Tech ofrece medidas cotidianas que puedes tomar para controlar tu privacidad digital, tu seguridad y tu bienestar de la manera que te parezca más adecuada. Disponible en 35 idiomas. https://datadetoxkit.org/en/home

El **Foro sobre el Futuro de la Privacidad** y la **Fundación para la Educación y la Innovación del FPF** son catalizadores del liderazgo y la erudición en materia de privacidad, y promueven prácticas de datos basadas en principios en apoyo de las tecnologías emergentes. Disponible en inglés. https://fpf.org/resources/

La red de **Derechos Digitales Europeos** (EDRi) defiende los derechos fundamentales en la era digital, aboga por leyes y políticas apropiadas y sensibiliza sobre las cuestiones clave que afectan a los derechos digitales. Disponible en inglés. https://edri.org/

La Guía de Protección de Datos de **Privacy International** contiene una gran cantidad de información útil sobre cuestiones relacionadas con la protección de datos. Disponible en inglés.

https://privacyinternational.org/report/2255/data-protection-guide-complete

Más información

Si desea leer más sobre algunas de las cuestiones planteadas en esta guía, los colaboradores de la misma sugieren los siguientes artículos como un buen punto de partida.

Este artículo de **Privacy International** examina cómo las políticas de inmigración basadas en datos conducen habitualmente a un trato discriminatorio de los inmigrantes, centrándose en el Reino Unido. https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees

Este artículo del sitio web **de Data-Pop Alliance** es el resumen de un capítulo de un libro titulado "Group privacy in the age of Big Data". En él se analiza cómo el Big Data está difuminando los límites entre los datos individuales y los datos de grupo, y qué se puede hacer al respecto.

https://datapopalliance.org/item/group-privacy-in-the-age-of-big-data/

Este artículo de la **Red Europea de Periodismo de Datos**, sobre "Lo incontable: Cómo Covid-19 afectó a la salud de los inmigrantes y refugiados" ofrece un ejemplo de cómo las vulnerabilidades suelen agravarse unas con otras. Disponible en inglés, francés, alemán e italiano.

www.europeandatajournalism.eu/eng/News/Data-news/The-uncountable-How-Covid-19-affected-migrants-and-refugees-health

Seguir viendo y escuchando

Las charlas mensuales de PANELFIT abarcaron una amplia gama de temas relacionados con los datos, las TIC, la privacidad y los derechos. La serie completa puede volver a verse -o, si lo prefiere, escucharse- a través del sitio web de PANELFIT. Disponible en inglés.

www.panelfit.eu/2020/03/23/monthly-chats/

Agradecimientos

Fuentes de información utilizadas para esta guía

El proyecto PANELFIT ha recopilado la información de esta guía a partir de las siguientes fuentes (las fuentes específicas se indican en el texto).

Charlas y talleres

- Un taller de PANELFIT sobre "Creación de un paquete de información a los ciudadanos sobre cuestiones éticas y jurídicas en torno a las TIC: ¿qué debe incluirse? ', 9-10 de marzo de 2020 en Berlín, Alemania.
- Una charla sobre poblaciones vulnerables a cargo del Dr. Jedrzej Niklas, del Departamento de Medios y Comunicaciones, LSE, Reino Unido (antes Universidad de Leeds), en un taller de PANELFIT, el 5 de junio de 2019, en Bilbao, España.
- Comunicación personal con la profesora Anna Lydia Svalastog, Departamento de Salud y Estudios Sociales, Colegio Universitario de Østfold, Noruega.
- Comunicación personal con el profesor Iñigo de Miguel Beriain, Departamento de Derecho Público Universidad del País Vasco, España.
- Revisión de la versión final y comentarios constructivos: El profesor Gianclaudio Malgieri, de la escuela de negocios EDHEC; Aurelie Pols, miembro de la junta del Center for Privacy & Cybersecurity; la Dra. Anna Berti Suman, de la Comisión Europea JRC y Marko ŠijanAZOP.

Documentos

- Berti Suman, A y Pierce, R (2018) "Challenges for citizen science and the EU Open Science Agenda under the GDPR", *European Data Protection Law Review* 4(3): 284-95, https://doi.org/10.21552/edpl/2018/3/7 (acceso abierto)
- Malgieri, G y Niklas, J (2020) 'Vulnerable data subjects', *Computer Law & Security Review* 37: 105415, https://doi.org/10.1016/j.clsr.2020.105415 (acceso abierto).
- Milan, S y Treré, T (2017) 'Big Data del Sur: El comienzo de una conversación que debemos mantener', DataActive, 16 de octubre, https://data-activism.net/2017/10/bigdatasur/ (acceso abierto).
- Peroni, L y Timmer, A (2013) 'Vulnerable groups: The promise of an emerging concept in European Human Rights Convention law', *International Journal of Constitutional Law* 11(4): 1056-85, https://doi.org/10.1093/icon/mot042 (acceso abierto).
- Consorcio PANELFIT (2020) 'D5.2 Análisis crítico del marco normativo de protección de datos de las TIC (versión consolidada)', Bilbao, España.

Vídeos y podcasts

- Podcast de PANELFIT con Gianclaudio Malgieri, 'Vulnerable data subjects and EU Law', 27 de febrero de 2020. Disponible en: www.youtube.com/watch?v=fqLfvF-cS70&feature=emb_title

Fotos

Página 1: © pixabay.com; geralt-9301 / stocksnap-894430 / geralt-9301 / geralt-9301/ josemdelaa-2004715/ vipragen-13256880/

Colaboradores

Nos gustaría agradecer a las siguientes personas su ayuda en la redacción de esta guía:

Alexandra Castañeda, Andreas Matheus, Andrzej Klimczuk, Anna Berti Suman, Annelies Duerinckx, Carolina Doran, Christoforos Pavlakis, Corelia Baibarac-Duignan, Elisabetta Broglio, Federico Caruso, Gefion Thuermer, Helen Feord, Janice Asine, Jaume Peira, Karen Soacha, Katerina Zourou, Katherin Wagenknecht, Katrin Vohland, Linda Freyburg, Marcel Leppée, Marta Camara Oliveira, Mieke Sterken, Tim Woods

Descargo de responsabilidad

Este proyecto ha sido financiado por el programa de investigación e innovación Horizonte 2020 de la Unión Europea mediante el acuerdo de subvención nº 788039. Este documento refleja únicamente la opinión del autor y la Agencia no es responsable del uso que pueda hacerse de la información que contiene.

El taller celebrado en Berlín, en marzo de 2020, se organizó gracias a la colaboración entre: la Asociación Europea de Ciencia Ciudadana (ECSA), la Acción COST 15212, el Instituto de Ciencias del Mar (ICM-CSIC) y los proyectos PANELFIT y EU-Citizen.Science. El apoyo financiero fue proporcionado por PANELFIT (acuerdo de subvención de la UE 788039) y la Acción COST 15212 (apoyada por la Cooperación Europea en Ciencia y Tecnología).

Consorcio PANELFIT (2021)
Esta obra está bajo una licencia CC BY 4.0: https://creativecommons.org/licenses/by/4.0/

Expedientes temáticos

1. Comercialización de datos: operadoras telefónicas y datos personales

Tu otra factura de teléfono: así usan las operadoras todo lo que saben sobre ti

Abstract: Cuando se habla de explotar la información personal, todo el mundo piensa primero en Meta, Google o Amazon. Pero, cuando te das de alta en una tarifa, estás entregando muchísima información a las telecos.

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/How-phone-companies-use-our-personal-data

Author: Michael Mcloughlin, Marta Ley, María Zuil (El Confidencial)

Text:

Cuando se habla de la explotación de los datos de los usuarios, hay nombres que aparecen casi al instante en el imaginario colectivo. Facebook , la empresa ahora conocida como Meta, es una de ellas. Escándalos como el de Cambridge Analytica , que destapó una ingente maquinaria de manipulación electoral en el seno de la mayor red social del mundo, pusieron en la picota a esta multinacional. No es ni mucho menos la única que ha levantado un imperio planetario escrutando qué se hace y qué se ve en internet, analizando la información y el rastro que se deja con cada clic, construyendo anuncios más eficaces o mostrando productos con mayores posibilidades de acabar en nuestro carrito de la compra. Google o Amazon, por citar algunos, son gigantes que han adquirido esa condición por esta vía.

Prácticamente, cualquier cosa que te hayas descargado en tu móvil es capaz de convertirse en un caladero de datos personales. La normativa europea, vitaminada tras la aprobación del Reglamento General de Protección de Datos en 2019, pretende que todo esto se realice conscientemente, saber qué compartimos y qué no. En cambio, la realidad es que, a día de hoy, es prácticamente imposible saber exactamente qué hemos compartido y con quién. Información sobre nuestra edad, nuestros movimientos y los lugares que visitamos cada día; sobre nuestro hogar, nuestro trabajo, si visitamos páginas con productos de bebé que ayuden a intuir que pretendemos ser padres o dónde pensamos irnos de vacaciones. Incluso, si utilizas ciertas 'apps' de citas, nuestra orientación sexual o la fecha de nuestro último examen de ETS. Todo eso y mucho más puede acabar en manos de decenas o cientos de empresas.

No te fijes solo en Meta o Google

Las aplicaciones o el propio sistema operativo no son los únicos agujeros por los que se pueden observar y escapar datos personales. Para hacer funcionar un teléfono inteligente hace falta tener una tarifa contratada por un operador . Cuando uno se da de alta en una tarifa de fibra o de voz y datos para el móvil, está entregando un importante 'botín' que permite a estas compañías acceder a muchísimos detalles sobre los usuarios y su día a día.

Es cierto que en sus condiciones de uso estas empresas tratan de brindar un resumen en el que intentan dejar claro qué se está aceptando. Pero la realidad es que estos textos resultan farragosos y densos para el común de los mortales, haciendo de la lectura y la comprensión un laberinto casi imposible de superar. La situación no es excepcional. Ocurre prácticamente en cualquier rincón de internet. En otras ocasiones, la culpa también es de los clientes, que rápidamente rellenan la casilla de consentimiento sin prestar atención a lo que se está aceptando.

Bajo este párrafo se puede encontrar un análisis de las políticas de privacidad de las principales marcas que operan en el mercado español, en el que se examina no solo el tipo de datos, sino también la forma que se recogen o si los textos se exponen de forma íntegra. Se trata de un estudio sobre las políticas de las empresas de telecomunicaciones que se refieren a los servicios y aplicaciones que casi todos los operadores recomiendan instalar.

Cómo usan los datos personales las compañías de teléfono

Pulsa sobre las tarjetas para ver la información completa de la política de privacidad

- Datos recopilados o compartidos*
- Datos recopilados con consentimiento
- Datos no recopilados o información completa
- Sin especificar

Telefónica
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Orange S.A.
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Vodafone
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Grupo MÁSMÓVIL
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Orange S.A.
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Digi Spain Telecom SLU
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Fuente: Políticas de privacidad de las compañías de teléfono, elaboración propia, EDJNet •

Es de esperar que los datos personales se conviertan en un activo aún más valioso para las operadoras, que ahora se mueven en un entorno el que los servicios que tradicionalmente han comercializado, internet y teléfono, son cada vez menos rentables. La generalización de los planes y tarifas planas ha supuesto un misil directo a su línea de flotación . Los ingresos no aumentan y, en caso de que lo hagan, no ocurre al ritmo que ellos desearían. Mucho menos sucede al ritmo al que crece el consumo de banda ancha, que no deja de batir récords año tras año, con el gasto que ello conlleva en mantenimiento de equipos y renovación de los mismos.

A esto hay que sumar una regulación que ha fomentado un escenario ultra competitivo en el mercado común, donde actúan cientos de compañías. Una situación diametralmente opuesta a la de Estados Unidos o China, donde el negocio se concentra entre tres o cuatro actores. En este contexto, además

de pedir que los gigantes de internet que necesitan de su infraestructura para hacer negocio también paguen la factura , las empresas del gremio están explorando nuevas vías de ingresos y productos, donde la economía de datos puede resultar fundamental. Y, como ejemplo, un lunar. Recientemente, las grandes operadoras europeas pidieron a la Comisión Europea que prohibiese una función de iCloud que permitía ocultar el historial 'online' y que encripta ciertos elementos de la conexión .

Samuel Parra, abogado especializado en la vertiente tecnológica del derecho y privacidad de datos, pone ejemplo el caso de la Cuarta Plataforma , un proyecto que Telefónica puso en marcha en 2017 que pretendía utilizar todos los datos que se generaban con su actividad tradicional, anonimizando la información de los usuarios, para generar nuevos espacios de monetización. “Cuando plantean algo así, están reconociendo que tienen muchísimos datos sobre los clientes. Y, claro, ahí surgen preguntas y dudas”, remata este experto.

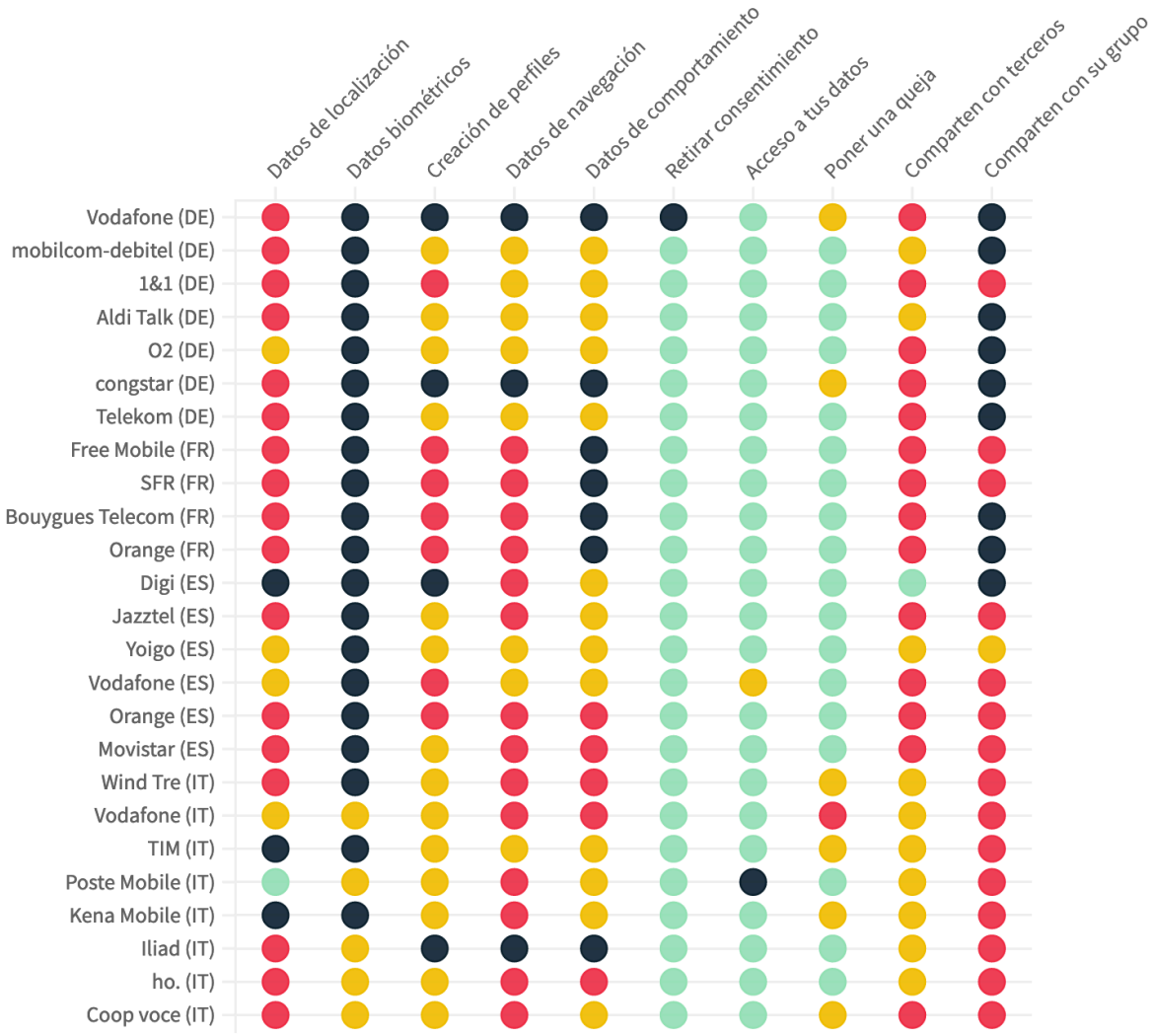
Recolección por mandato legal

Parra señala una diferencia importante de estas empresas con otros negocios digitales, como las empresas de redes sociales. “Hay que tener en cuenta que parte del volumen que estas compañías recopilan y almacenan es algo exigido por ley”. La norma que regula es la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. "Nuestro consentimiento no es la única base para poder recolectar datos. También lo es la ley. Pero, cuando eso ocurre, tiene que ser informado. Algo que en la práctica no se suele hacer".

Cómo recopilan y usan los datos personales las compañías telefónicas

Datos de las principales compañías de Alemania (DE), Francia (FR), España (ES) e Italia (IT)

Datos recopilados o compartidos* · Datos recopilados con consentimiento · Datos no recopilados o información completa · Sin especificar



Fuente: Políticas de privacidad de las de teléfono, elaboración propia, EDJNet •
*Recopilada sin consentimiento expreso o, cuando no es necesario, sin informar de la normativa que obliga a ello.

En el artículo 3 de dicho texto se recogen los registros que están obligados a almacenar tanto en el caso de llamadas telefónicas fijas, móviles, así como conexiones a internet. Datos que van desde el número de abonado, la dirección IP, la hora de inicio de la llamada hasta las referencias para geolocalizar desde qué punto (en el argot especializado, 'celda') se inicia la llamada desde el 'smartphone', entre muchas otras referencias,

Precisamente, la Generalitat Valenciana, junto al Ministerio de Fomento, puso en marcha durante lo más duro de la pandemia un estudio de movilidad en el que se utilizaban estos datos de los operadores

, agregándolos y anonimizándolos, con el que pretendía conocer los movimientos de la población para saber si las medidas de confinamiento estaban surtiendo efecto.

En otros países se ejecutaron pilotos parecidos. En todos casos, levantaron suspicacias entre los expertos, que mostraron su preocupación sobre la posibilidad de identificar a sujetos particulares incluso dentro de estos grandes conjuntos de datos, una posibilidad reafirmada por varios estudios recientes .

La norma española emana de una directiva europea, aprobada en 2006, que obligaba a todos los países de la Unión Europea a tomar medidas similares. “Existe cierta controversia, porque, en 2014, la Justicia comunitaria invalidó esta directiva porque vulneraba derechos fundamentales. Eso hizo que quedase la ley en una posición extraña. Se puede interpretar que, al anular la directiva, también debería quedar invalidada”.

Aunque no hay uniformidad, como se muestra en los diferentes gráficos que acompañan este artículo, las compañías recogen más información de la prevista en la legislación, como se puede observar en las condiciones de uso. Registros que pueden utilizar con fines de creación de perfiles, con el fin de crear servicios "a medida" o publicidad dirigida, o pueden proporcionar o vender dichos datos a terceras empresas, con las que tengan acuerdos. Por ejemplo, pueden proporcionar datos a centros de llamadas que luego contactarán al usuario para ofrecerles promociones y otros productos.

Aquí se pueden presentar algunos problemas. Muchas veces, al pasar de mano a mano, se pierde el rastro de quién tiene acceso y quién no e incluso se siguen usando más allá del fin con el que se recogieron. Algo que vulneraría la obligación de la RGPD, que establece que se deben recolectar con un fin concreto y durante un tiempo determinado. Otro problema que se suele presentar es que la aceptación de términos se presenta, a menudo, como un único bloque o en muy pocos. “Tiene que ser una presentación y una aceptación granular, no puede ser monolítica”.

Cómo usan los datos personales de las aplicaciones las compañías de teléfono

Movistar, Jazztel y Digi tienen la misma política para la App que para la línea telefónica. Pulsa sobre las tarjetas para ver la información completa.

- Datos recopilados o compartidos*
- Datos recopilados con consentimiento
- Datos no recopilados o información completa
- Sin especificar

Telefónica
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Orange S.A.
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Vodafone
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Grupo MÁSMÓVIL
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Orange S.A.
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Digi Spain Telecom SLU
- Datos de localización
- Datos biométricos
- Creación de perfiles
- Datos de navegación
- Datos de comportamiento
- Comparten con terceros
- Comparten con su grupo
- Retirar consentimiento
- Acceso a tus datos

Fuente: Políticas de privacidad de las de teléfono, elaboración propia, EDJNet •

Un sector con cuantiosas multas

Esos datos no siempre han sido empleados escrupulosamente por las compañías. Han sido varias las ocasiones en las que diferentes telecos han sido castigadas con duras multas dentro y fuera de nuestras fronteras. En el mercado patrio, en febrero de este mismo año, la Agencia de Protección de Datos sancionó con 5,8 millones de euros a Telefónica, MásMóvil, Orange y Vodafone por no proteger adecuadamente el tratamiento de la información de los usuarios a la hora de tramitar tarjetas SIM. La más castigada fue la operadora británica, que se llevó una gran parte de la sanción, con 3,94 millones. El motivo de esta severidad fue la tardanza en subsanar esos problemas.

Esto no es nada nuevo. Una investigación de Civio reveló que, entre 2015 y 2019, las operadoras fueron las que más penalizaciones recibieron de este supervisor, por una cuantía de 22 millones. Eso

supone prácticamente el 40% de los 57,6 millones de euros de los expedientes sancionadores que se publicaron en dicho periodo.

En el resto de Europa se han producido casos similares. En 2020, la Autoridad de Protección de Datos de Italia multó a TIM con casi 28 millones de euros después de repetidas quejas de los usuarios sobre la recepción de llamadas telefónicas comerciales no deseadas como resultado de violaciones en la gestión de los datos personales. En 2021, se impuso una multa de 4,5 millones de euros a Fastweb por motivos similares.

Metodología

La información recopilada en este artículo es fruto de una investigación coordinada por la European Datajournalism Network (EDJNet) en la que han participado OBC Transeuropa, Voxeurop y El Confidencial.

Hemos consultado las políticas de privacidad de los servicios móviles en la web de las principales empresas operadoras en cada país, así como las relativas al uso de las aplicaciones para 'smartphones' que permiten a los usuarios gestionar su perfil. La información fue recopilada entre finales de marzo y principios de febrero.

El objetivo era responder a 10 preguntas previamente formuladas (los 10 puntos que figuran en las infografías publicadas en este artículo) relacionadas con el tipo de datos recogidos, el modo en que se utilizan estos datos y la exhaustividad de cierta información. La información obtenida se recogió en dos conjuntos de datos: uno relativo a las políticas de privacidad de los servicios y otro a las aplicaciones.

2. La estrategia europea de ciberseguridad

El plan de Bruselas para blindar la Unión Europea contra los ciberataques

Abstract: La crisis de la covid-19 ha dado el empujón definitivo a la sociedad digital. Gran parte de nuestro día a día sucede ahora en el entorno digital, lo que provoca que los Estados miembros sean mucho más vulnerables a los ciberataques. Para neutralizarlos, la Comisión Europea presentó en diciembre de 2020 su nueva Estrategia de Ciberseguridad.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Brussel-s-plan-to-protect-the-EU-from-cyberattacks

Text:
"¿Quién es usted? Está en nuestro sistema. General, ¿qué sugiere que hagamos? General, tiene usted razón: tenemos que invertir en privacidad". Así reaccionó Josep Borrell, alto representante europeo para la Política Exterior, cuando se percató de que en una videoconferencia secreta de los ministros de Defensa de la UE de noviembre del año pasado se había colado un desconocido. En un descuido, la ministra de Países Bajos había compartido en Twitter una imagen donde se veía el código de acceso a la reunión, y un periodista de su país había aprovechado el error para conectarse a la videollamada y sacarle los colores a las instituciones comunitarias.

La escena, a pesar de ser disparatada, evidenció la gran debilidad de la Unión Europea en materia de ciberseguridad: en un club de 27 países, con reuniones y conversaciones que idealmente tendrían que ocurrir en persona pero que debido a motivos logísticos se trasladan al entorno digital, es muy difícil que ninguna puerta quede abierta. Y eso, en un mundo tan interconectado como el actual, es un riesgo enorme que obliga a la UE a armarse para hacer frente a cualquier ataque digital, tenga la forma que tenga, venga desde donde venga y ocurra cuando ocurra.

Es una amenaza silenciosa, pero no invisible. No en vano, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) identificó 304 ataques maliciosos significativos contra "sectores críticos" en 2020 , más del doble que el año anterior. Muchos de ellos tuvieron como objetivo hospitales y redes sanitarias, puntos que durante la pandemia gestionaron información muy valiosa sobre la evolución del coronavirus y la vacunación.

Sus objetivos pueden ser diversos, desde robar datos hasta paralizar infraestructuras claves, y sus consecuencias desastrosas para el país atacado. El mayor ejemplo reciente es el ataque que sufrió el oleoducto Colonial , el más grande de Estados Unidos, en mayo de este año. La agresión, perpetrada por un grupo apolítico de hackeadores profesionales llamado Darkside, obligó a los operadores a detener el flujo de crudo, dando lugar a una escasez de gasolina en toda la costa este, y a pagar a los atacantes 75 bitcoins, el equivalente a 3,8 millones de euros.

Afortunadamente para los ciudadanos europeos, la Unión Europea tiene un plan para que el incidente de la reunión secreta de Defensa se quede en una anécdota y ningún ciberataque comprometa la seguridad comunitaria. Así, en diciembre de 2020 la Comisión Europea presentó una nueva Estrategia de Ciberseguridad y una propuesta para reforzar la directiva sobre medidas para un alto nivel común de ciberseguridad en la Unión (Directiva NIS2).

Una nueva carrera nuclear

La Unión Europea lleva en realidad desde 2013 preparándose para poder responder a ataques digitales, y en los últimos años ha lanzado diversas iniciativas para avanzar en la creación de una estrategia de defensa y seguridad en la red común.

Entre ellas destacan el conjunto de instrumentos de ciberdiplomacia y el marco político de ciberdefensa, ambos aprobados en 2018 y orientados a mejorar la coordinación entre los Estados miembros; el Reglamento de Ciberseguridad de 2019 , que renovó el mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), convirtiéndola en la Agencia de Ciberseguridad de la UE; y la caja de herramientas para la seguridad de las redes 5G , también de 2019.

Pero en un mundo hiperconectado como el actual, donde las amenazas híbridas son cada vez más sofisticadas y las potencias compiten por lograr un desarrollo tecnológico diferencial que les permita blindar sus sistemas, el riesgo de quedarse descolgado de la carrera tecnológica es demasiado grande. En este sentido, la batalla de la ciberseguridad recuerda a la carrera nuclear de la Guerra Fría, cuando Estados Unidos, la Unión Soviética y sus respectivos aliados se enzarzaron en una guerra silenciosa por desarrollar armas nucleares. Al igual que sucede ahora, cualquier avance era ocultado recelosamente y cada paso adelante del rival obligaba a mover ficha al otro.

Y es por eso mismo por lo que la Unión Europea se ve obligada a actualizar su Estrategia de Ciberseguridad continuamente, para mantenerse siempre un paso por delante de los cibercriminales. Así, aunque la primera versión del documento fue publicada en 2013, la estrategia fue revisada en 2017 y de nuevo actualizada en diciembre de 2020.

Esta última versión supone, no obstante, un cambio de paradigma: ahora que el club europeo cuenta con medidas de seguridad unificadas y coordinadas, la UE quiere trabajar en la creación de herramientas que le permitan responder de forma inmediata y eficaz o incluso prevenir los ciberataques.

Una hoja de ruta ambiciosa

De esta manera, la nueva Estrategia de Ciberseguridad incide en tres áreas clave : en primer lugar, pretende mejorar la resiliencia comunitaria a los ciberataques a través, por un lado, de la creación de una red de centros de operaciones de seguridad en toda la UE que funcionen con tecnología de inteligencia artificial y, por otro, una reforma de las normas sobre seguridad de las redes y los sistemas de información, recogidas en la Directiva sobre medidas para un alto nivel común de ciberseguridad en la Unión (Directiva NIS revisada o NIS2).

La Directiva NIS, aprobada en 2016, provocó un cambio en el enfoque institucional para la ciberseguridad en los Estados miembros —los obligó, entre otras cosas, a elaborar una estrategia nacional de ciberseguridad y a establecer equipos de respuesta ante emergencias informáticas—, pero había empezado a mostrar limitaciones.

“La transformación digital de la sociedad, intensificada por la crisis de la covid-19, ha ampliado el panorama de amenazas y está generando nuevos desafíos que requieren respuestas adaptadas e innovadoras. Ahora, cualquier interrupción puede tener efectos en cascada en todo el mercado interior”, expuso la propia Comisión Europea en la presentación de su propuesta.

En resumen, la Directiva NIS2, que recibió el visto bueno del Parlamento Europeo este mes de octubre , expande los sectores que se consideran críticos y refuerza los requisitos de seguridad para las

160.000 empresas que pretende cubrir. El objetivo es reducir la brecha económica que separa a las compañías europeas de las estadounidenses, que invierten de media un 41% más en ciberseguridad.

En segundo lugar, con su nueva Estrategia de Ciberseguridad, la Comisión también quiere reforzar su capacidad operativa para prevenir, disuadir y responder a los ciberataques, para lo cual creará una unidad informática conjunta . Este equipo trabajará para garantizar una respuesta coordinada de la UE a los ciberincidentes y cibercrisis a gran escala y ofrecer asistencia para recuperarse de esos ataques. "Las amenazas suelen ser comunes, por lo que es necesario coordinarse, compartir conocimientos e incluso lanzar alertas por anticipado", argumentó la Comisión.

En tercer y último lugar, Bruselas propone promover un ciberespacio global y abierto, es decir, entablar una conversación con el resto de países para que su normativa sea replicada y contribuir con ello a la seguridad internacional. Es, en otras palabras, un intento por impedir que la defensa contra los ciberataques se convierta en una lucha de todos contra todos y, al contrario de lo que ocurrió con la carrera nuclear, dar lugar a una cooperación entre naciones que revierta en un blindaje global contra este tipo de amenazas.

ENISA, el pegamento de la estrategia de ciberseguridad de la UE

Abstract: La Agencia de Ciberseguridad es la encargada de construir una defensa común, sin fisuras, contra los ciberataques en la Unión Europea. Y aunque en sus inicios lo tenía todo en contra para lograrlo, remodelación tras remodelación ha conseguido erigirse en la punta de lanza de Bruselas contra los cibercriminales.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/ENISA-The-cornerstone-of-the-EU-s-cybersecurity-strategy

Text:
Cuando la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) fue fundada, allá por 2004, Facebook acababa de nacer y el prefijo "cíber" sonaba aún a ciencia ficción. Su mandato inicial fue de apenas cinco años, un límite al que la Comisión Europea le fue dando patadas hasta que en 2019 la convirtió por fin en una agencia permanente. Por si fuera poco, su sede se encuentra en las ciudades griegas de Heraclión y Atenas, en las antípodas europeas de Bruselas.

Y a pesar de ello, la ENISA se ha convertido en el elemento cohesionador de la estrategia de ciberseguridad comunitaria. De hecho, aunque conserva su acrónimo, tras su última remodelación pasó a llamarse Agencia de la Unión Europea para la Ciberseguridad, a la cual se le otorgó la función de "lograr un elevado nivel de ciberseguridad común en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros y a las instituciones, órganos y organismos de la Unión".

Es, en otras palabras, el punto de referencia, el timón del plan europeo de seguridad de la red y la información. Sin un nivel común de defensa, sin una protección armonizada, la UE sería un objetivo fácil para los cibercriminales, y es por eso por lo que la Comisión propuso la creación de la ENISA: para contar con un supervisor cuyo cometido principal sería asegurarse de que no quedaran cabos sueltos ni directrices sin implementar que hicieran vulnerable al grupo. Además, la agencia colabora estrechamente con Europol y el Centro Europeo de Ciberdelincuencia.

En 2004 se trataba de un proyecto prematuro, un paso por delante de la penetración de internet en la vida diaria de los ciudadanos, pero a medida que las tecnologías de la información y la comunicación

(TIC) se abrían paso los riesgos asociados a ellas crecían exponencialmente. Protegerse frente a ellos ya no era una medida de precaución visionaria, sino una obligación, y ahí la labor de la Agencia Europea de Ciberseguridad demostró ser fundamental.

Sin su trabajo, ciberataques como el sufrido por el Hospital Universitario de Brno (Chequia) en marzo de 2020 , en mitad de la pandemia, que obligó a posponer operaciones urgentes y reubicar a pacientes graves, serían mucho más frecuentes. La pandemia ha complicado más las cosas: al acelerar la transformación digital de la sociedad y la economía, las amenazas se han multiplicado. Desde el suministro de agua hasta el control de nuestros hogares, cada vez más conectados, el ámbito de actuación de los cibercriminales ya no tiene límites.

Un ascenso progresivo

La ENISA fue concebida como una agencia pequeña con una tarea muy concreta: ayudar a las instituciones y organizaciones de la Unión Europea y los Estados miembros a proteger sus conexiones. Un año antes de que venciera su mandato inicial, en 2008, el Parlamento y el Consejo europeos decidieron , a propuesta de la Comisión, prorrogar su vigencia hasta 2012, en tanto en cuanto la evaluación y la mejora de la protección de las redes europeas apenas había comenzado.

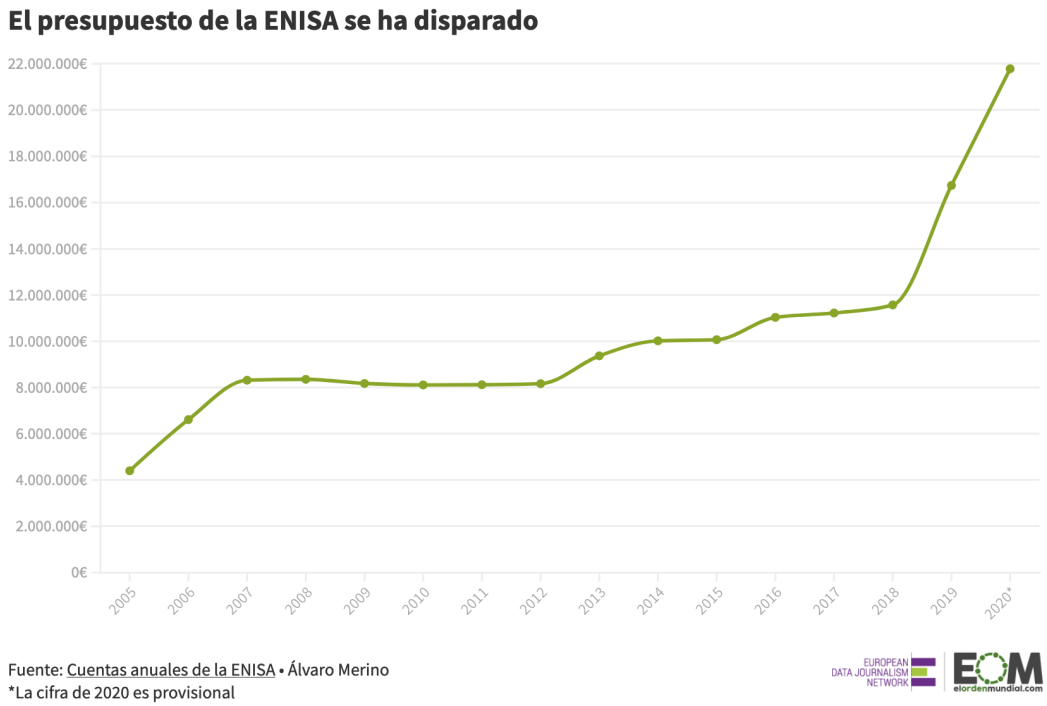
En 2011, de nuevo, el mandato fue renovado hasta 2013, y cuando esa fecha límite llegó, otra vez hasta 2020. A diferencia de los anteriores, ese último empujón vino acompañado de una ampliación de sus funciones. Coincidiendo con la publicación de la primera Estrategia de Ciberseguridad de la UE, las instituciones comunitarias también plantearon una modernización de la agencia, que desde 2013 brindaría asistencia en nuevas áreas. Entre ellas, destaca la coordinación de una futura red de equipos de respuesta ante emergencias informáticas (EU CERT) repartidos por todas las capitales.

Pero fue en 2019, con la entrada en vigor del Reglamento de Ciberseguridad, cuando la ENISA recibió el espaldarazo definitivo. Además de aumentar sus recursos, la nueva legislación convirtió en permanente el mandato que recibió en 2004, cambió su nombre a Agencia de Ciberseguridad de la UE, expandió su papel asesor y le otorgó por primera vez funciones operativas claras .

Así, entre otras cosas, la agencia comenzó a ayudar también a los Estados miembros a la hora de establecer prioridades para la inversión en investigación y desarrollo y, lo más importante, a trabajar en la creación de un sistema de certificados de seguridad para productos y servicios TIC en la Unión.

Para que las empresas y los consumidores puedan confiar en que su información online está a salvo necesitan utilizar dispositivos seguros, pero la falta de un sistema de certificación único en la UE mina esa confianza a la vez que limita el comercio transfronterizo. Por ello, ENISA debe establecer criterios comunes y unificar los mecanismos nacionales para emitir certificados de ciberseguridad, un sello que necesitan desde las tarjetas inteligentes —tarjetas de crédito, de transporte, SIM...— hasta los servicios de computación en la nube.

En cuanto a su financiación, la Agencia de Ciberseguridad ha ido aumentado su dotación año a año hasta alcanzar los casi 22 millones de euros de 2020 , cinco veces más que su partida inicial. La inmensa mayoría del dinero lo aporta la Comisión Europea, mientras que los países de la Asociación Europea de Libre Comercio que no pertenecen a la UE —Islandia, Liechtenstein, Noruega y Suiza— y el Gobierno griego —en concepto de ayuda al alquiler de las instalaciones— realizan también una pequeña aportación. En 2019, además, contaba con 75 empleados .



El creciente peso de la ENISA en la Estrategia de Ciberseguridad de la UE ha llevado a la Comisión Europea a querer tenerla más cerca de su centro de poder. Y para ello, en lugar de cambiar su sede, el pasado mes de junio autorizó la apertura de una tercera oficina en Bruselas con el objetivo de que la agencia pueda mantener "una cooperación regular y sistemática" con las instituciones europeas.

Así, reciclaje tras reciclaje, la Agencia Europea de Seguridad de las Redes y de la Información se ha mantenido como el pilar de la ciberseguridad europea desde que fuera fundada en 2004. La culminación de ese proceso llegará con su asentamiento en Bruselas y la consolidación de sus funciones operativas, un cambio que se enmarca dentro del intento de la UE de pasar a la ofensiva contra los ciberataques y convertirse en el enemigo número uno de los cibercriminales en todo el mundo.

La ciberseguridad: entre la coordinación europea y las agencias nacionales

Abstract: Las agencias europeas desempeñan un papel de apoyo y coordinación en la ciberseguridad a nivel europeo. Sin embargo, en relación con reglamentos específicos de la UE, cada Estado miembro puede establecer sus propias secciones tanto para entidades privadas como para intereses nacionales más importantes.

Author: Openpolis

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Cybersecurity-between-European-coordination-and-national-agencies

Text:
En los últimos años, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) se ha ido convirtiendo en un recurso cada vez más importante para abordar los crecientes desafíos de este sector. La competencia de la Unión Europea en materia de ciberseguridad deriva del Artículo 5 del

Tratado de la Unión Europea (TUE), que estipula la competencia compartida en áreas donde no hay competencia exclusiva.

En virtud del principio de subsidiariedad, en los ámbitos que no sean de su competencia exclusiva, la Unión intervendrá solo en caso de que, y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional y local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión. (TUE Art. 5.3)

Por lo tanto, la UE (y por extensión, la ENISA) deberían limitarse a los asuntos que los Estados miembros no puedan resolver de manera individual. Por esta razón, cada Estado miembro, junto con esta agencia europea, ha instaurado su propio marco institucional y organismos para lidiar con la ciberseguridad. Así, la ENISA se encarga de ayudar a los Estados miembros y a la Comisión, y de facilitar la cooperación y el intercambio de información.

Coordinación europea

Actualmente, el principal punto de referencia legislativo para la ciberseguridad europea es la directiva SRI, aunque también se está debatiendo un texto actualizado y se espera que conduzca a la aprobación de la SRI 2.

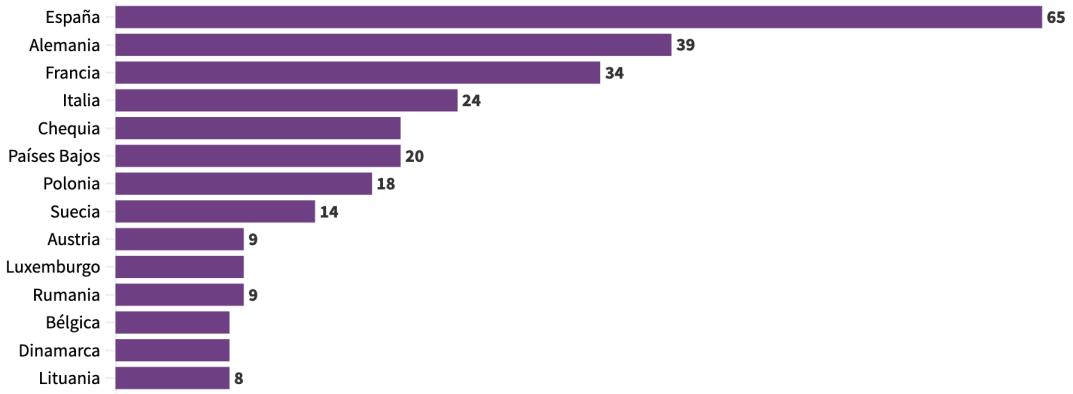
Dada la naturaleza de las directivas europeas (Artículo 288 del Tratado de Funcionamiento de la Unión Europea, TFUE), el texto se limita a indicar a los Estados miembros los resultados deseados, y les otorga autonomía suficiente como para diseñar sus propias agencias de ciberseguridad.

Los Estados miembros tienen, entre otras, la obligación de identificar unas agencias específicas para que coordinen las políticas adoptadas y mantengan un nivel alto de ciberseguridad. Se trata de las autoridades nacionales competentes, los únicos puntos de contacto y los CSIRT (equipos de respuesta a incidentes de seguridad informática).

Los CSIRT, creados en 1990, son las organizaciones encargadas de recopilar y gestionar informes sobre incidencias y potenciales vulnerabilidades de software. Cada país tiene un número diferente de CSIRT que pueden ser acreditados por varios consorcios internacionales, como Trusted Introducer, First (Forum of Incident Response and Security Teams) y la Red CSIRT europea.

Los primeros 15 países de la UE por número de CSIRT

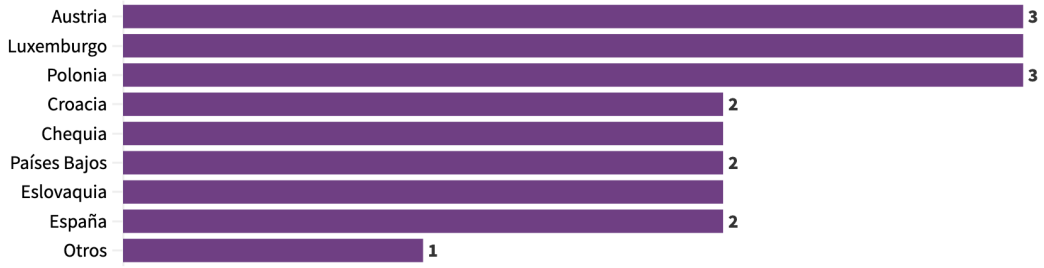
Los países europeos con el mayor número de equipos de respuesta a incidentes de seguridad informática (CSIRT) acreditados por los tres principales consorcios internacionales



La directiva SRI obliga a los Estados miembros a designar al menos un CSIRT para poder unirse a la Red Europea CSIRT. La mayoría solo ha designado un único CSIRT, aunque no todos: algunos países han escogido dos o tres.

CSIRT nacionales designados por los Estados miembros

El número de CSIRT nacionales designados por cada Estado miembro de la Unión Europea como parte de la Red CSIRT



Los CSIRT se encargan de los incidentes y las posibles vulnerabilidades de las TI, mientras que las autoridades SRI competentes operan a nivel legislativo y de gestión. Estos son los organismos nacionales responsables de la seguridad de las redes y los sistemas de información en los sectores indicados en la directiva. También en este caso, cada Estado puede designar uno o más órganos competentes.

13 países escogieron una única autoridad SRI competente.

Si solo se designa una autoridad, esta se convierte automáticamente en el único punto de contacto. De lo contrario, el país debe indicar el organismo que actuará de intermediario para asegurar la cooperación con las autoridades de otros Estados miembros, la ENISA y la Red CSIRT.

Autoridades SRI competentes: el caso de Alemania, Francia e Italia

Como hemos podido comprobar, cada país tiene derecho a diseñar como quiera la estructura de sus organismos siempre y cuando respete las obligaciones de la directiva europea. Tomando como ejemplo a los tres países más poblados de la UE, lo primero que llama la atención es que los tres, hasta la fecha, han identificado una sola autoridad SRI.

En Italia, la autoridad SRI es la nueva Agencia de Ciberseguridad. Antes de su creación en mayo de 2021, se habían señalado cinco autoridades: los ministerios de desarrollo económico, infraestructura, economía, salud y medioambiente; ahora definidos como "autoridades del sector" (Artículo 7 del Decreto legislativo 65/2018). Por tanto, la Agencia de Ciberseguridad constituye el único punto de contacto, y al mismo tiempo incluye al CSIRT italiano, que anteriormente formaba parte del departamento de información para la seguridad de la República (y que en consecuencia entraba dentro de la categoría de inteligencia).

Como ya explicamos en otros artículos, la Agencia de Seguridad es autónoma en muchos sentidos. Sin embargo, está bajo la supervisión de la Presidencia del Consejo, que controla tanto la gestión del sector como el nombramiento del director (Roberto Baldoni) y subdirector (Nunzia Ciardi). Por su parte, la propia agencia está formada por ocho servicios generales, y estos a su vez se distribuyen en divisiones. La plantilla máxima prevista actualmente es de unas 300 personas, mientras que el presupuesto para 2022 alcanza los 41 millones de euros. No obstante, se espera que en los próximos años se produzca un aumento considerable de recursos.

> El presupuesto previsto para la agencia de ciberseguridad italiana a partir de 2026 es de 122 millones de euros.

En Francia, la autoridad competente es la Agencia nacional de la seguridad de los sistemas de información (ANSSI). Al igual que en Italia, la agencia forma parte de la Presidencia del Consejo. Concretamente, la agencia francesa forma parte de la Secretaría General de Defensa, un organismo que ayuda al Primer Ministro en el ejercicio de sus responsabilidades en cuestiones de defensa y seguridad nacional. Fundada por ley en 2009, la ANSSI se fijó inmediatamente unos objetivos ambiciosos, entre ellos, convertirse en la líder mundial en materia de ciberseguridad. Esta formulación ya no aparece en la mayoría de las versiones recientes de la estrategia francesa sobre ciberseguridad.

En la cúspide de la ANSSI se encuentra la Dirección General, que incluye al Director General, Guillaume Poupard, así como al Director General Adjunto y al Jefe de Personal. Por debajo hay cuatro subdirecciones, y estas a su vez están formadas por divisiones. Sin contar con los salarios, el presupuesto de la ANSSI ascendió a unos 21 millones de euros en 2020, mientras que la plantilla incluía más de 500 funcionarios y 100 empleados.

> El presupuesto de la ANSSI para 2020 fue de 21 millones de euros, sin contar con los gastos de personal.

Alemania también ha designado a una sola autoridad competente, la Autoridad Federal de Ciberseguridad (BSI). Al contrario que en Francia e Italia, este organismo no está bajo el mando del Primer Ministro (o Canciller, en este caso), sino que forma parte de la Dirección General de Ciberseguridad e Información, en el Ministerio de Interior. El órgano se creó en 1991, aunque hoy en día sus funciones están reguladas por una ley de 2009. También se adoptaron medidas en años posteriores, una en 2015, que anticipaba muchos elementos de la directiva europea promulgada el año siguiente, y otra tan solo hace unos meses. Con la última legislación, el gobierno alemán pretende fortalecer la BSI, especialmente en lo relativo a la protección del consumidor, la seguridad comercial y las redes móviles.

En la cúspide de la BSI se encuentran el presidente, Arne Schönbohm, y el vicepresidente. La agencia se divide internamente en ocho divisiones, y estas a su vez se dividen en 18 filiales y varias secciones. Su presupuesto para 2021 ascendió a casi 200 millones de euros, y cuenta con una plantilla de 1550 personas.

> El presupuesto de la Autoridad Federal de Ciberseguridad alemana ascendió a 200 millones de euros en 2021.

Si bien es interesante, es difícil comparar los datos sobre los presupuestos y el número de trabajadores en estos organismos. No se debe únicamente a que los datos se han recopilado de diferentes fuentes con diferentes metodologías, sino también a que la ciberseguridad no constituye una responsabilidad exclusiva de una única organización en ningún país. Existen diferentes estructuras, como los ministerios o los sectores de defensa e inteligencia, que desempeñan un papel fundamental en este ámbito y por ello es complicado evaluar la voluntad de los países en materia de seguridad.

La relación entre los sectores de defensa e inteligencia

Como se ha mencionado más arriba, antes de la creación de la Agencia de Ciberseguridad italiana, el sector era competencia del Departamento de Información para la Seguridad de la República (DIS). Sin embargo, la nueva ley ha situado la agencia fuera del sector de inteligencia, aunque siguen quedando muchos vínculos entre estas dos secciones. Por otra parte, el subsecretario del gobierno a cargo de inteligencia está ahora, por ley, a cargo de la misma competencia en ciberseguridad. Asimismo, se asegura la coordinación con inteligencia mediante la presencia de representantes de agencias de inteligencia en el núcleo de la ciberseguridad, donde también participan representantes de varios ministerios. También se prevé la presencia de representantes del Ministerio de Defensa, garantizando así el nexo entre la Agencia y el Mando de Operaciones de Red (COR), el órgano de ciberseguridad bajo las órdenes del Jefe de Gabinete de Defensa. No obstante, en las normativas publicadas hasta ahora, no se menciona un vínculo explícito entre la agencia y el COR.

La Autoridad Federal de Ciberseguridad alemana también surgió del sector de inteligencia. En sus inicios a principios de la década de los 90, el organismo lidiaba con la protección tecnológica de secretos de Estado. Pero con los años, la BSI se ha convertido en un órgano completamente independiente. Las relaciones con inteligencia se mantienen mediante el Centro Nacional para la Ciberdefensa, un órgano interinstitucional que incluye varias estructuras federales interesadas en la ciberseguridad. La BSI también mantiene relaciones con el ejército, que ostenta una importancia considerable en este sector en Alemania. De hecho, la ciberdefensa está asignada constitucionalmente a las fuerzas armadas. En 2017, se creó el Kommando Cyber -und Informationsraum (CIR), un órgano estimado a la altura de otros comandos de las fuerzas armadas alemanas, y encargado de la seguridad de las infraestructuras de ciberdefensa y de sistemas armamentísticos. Dada la estrecha relación entre defensa y ciberseguridad, el CIR apoya a la BSI en caso de necesidad. Sin embargo, debido a los estrictos límites constitucionales a los que está sometido el ejército alemán, solo puede proporcionar ayuda "administrativa". De hecho, en caso de que se necesite desplegar personal militar en respuesta a un ciberataque a escala nacional, la constitución requiere una autorización previa por parte del parlamento.

Como hemos podido comprobar, en Francia la ANSSI forma parte de la Secretaría General de Defensa. La estructura garantiza la coordinación con el ejército e inteligencia. De hecho, la Secretaría General de Defensa tiene diversas competencias tanto en materia de defensa como de inteligencia, y se encarga de la dirección, propuesta, coordinación y reglamentación de los asuntos generales de defensa y seguridad nacional para el Presidente del Consejo de Ministros. Como también hemos podido observar, la Secretaría General de Defensa también responde ante el Presidente del Consejo de Ministros, quien a su vez también es responsable de las actividades de los servicios de inteligencia domésticos y extranjeros, aunque estos estén bajo las órdenes de los Ministerios de Interior y de Defensa, respectivamente.

Links:

Protección de datos en la UE: estudio comparativo de informes nacionales. Leer
Ciberdefensa en los países de la OTAN: modelos comparativos. Leer

Rusia quiere tus datos: los ciberataques se multiplican en la Unión Europea

Abstract: Los ciberataques contra sectores críticos en Europa se duplicaron en 2020 ayudados por la digitalización que trajo la pandemia. La mayoría de incursiones siguen viniendo de Rusia. Y aunque la UE trabaja para cerrar agujeros, la invasión de Ucrania amenaza con intensificar la ciberguerra.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Russia-wants-your-data-cyber-attacks-are-growing-in-the-European-Union

Text:

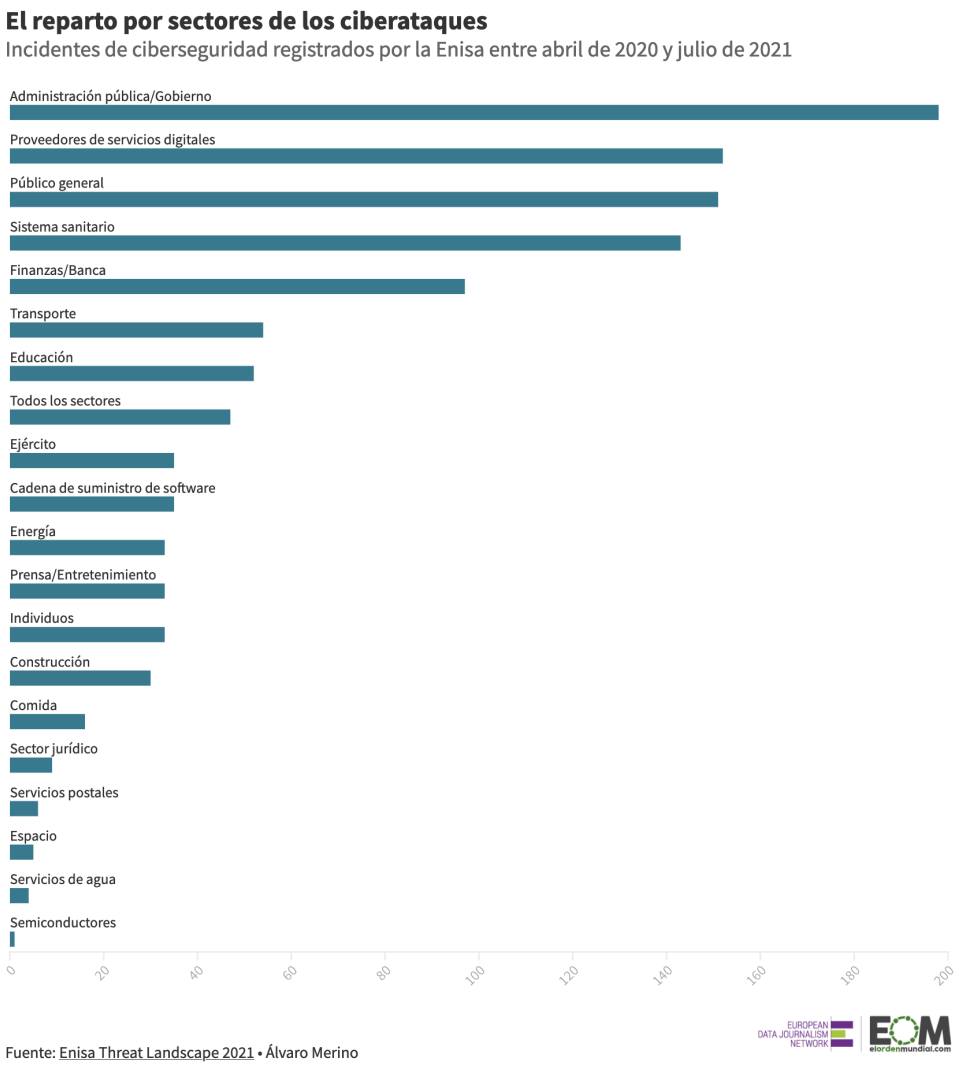
El 14 de mayo de 2021 Donna-Marie Cullen estaba esperando a que llegara la hora de su cita de radioterapia, con la que combatía un agresivo tumor cerebral, cuando recibió una inesperada llamada : un ciberataque había tumbado la red informática del sistema sanitario irlandés y su tratamiento tenía que ser suspendido temporalmente. Tras un año de intensa lucha contra el coronavirus, la Sanidad irlandesa había sucumbido, pero el culpable no era la pandemia, sino un ataque invisible que provenía de cientos de kilómetros de distancia.
Las investigaciones concluyeron que el causante había sido un *ransonware*, o 'secuestro de datos', perpetrado por Wizard Spider , un grupo cibercriminal basado en San Petersburgo que exigió catorce millones de libras a cambio de detener el ataque. Las autoridades irlandesas optaron por tratar de repelerlo, lo que acabó acarreando la suspensión de miles de citas, la vuelta al papel y lápiz en los centros sanitarios durante meses, una filtración de información médica confidencial de 520 pacientes y un gasto de cerca de cien millones de euros .

Lejos de ser un caso aislado, la agresión sufrida por el sistema sanitario irlandés se enmarca dentro de una avalancha de ciberataques que tienen como objetivo instituciones y empresas de la Unión Europea. La sombra de Rusia siempre ha planeado sobre las redes comunitarias, pero con la pandemia la frecuencia y la virulencia de esos ataques no ha hecho sino aumentar. Los incidentes maliciosos significativos contra sectores críticos se duplicaron en Europa en 2020 —304 incidentes frente a 146 en 2019—, según la Agencia de la Unión Europea para la Ciberseguridad (Enisa). Los ciberataques a hospitales y redes de atención sanitaria también aumentaron un 47%.

La nueva normalidad, campo abonado para los cibercriminales

En cuestión de días, a medida que los contagios de coronavirus se multiplicaban sin control a principios de 2020, la vida de los europeos se trasladó al entorno online. De repente el teletrabajo, las compras en internet y la socialización a través de una pantalla se convirtieron en rutina. Y si bien las soluciones digitales permitieron que el mundo no se detuviera, también brindaron una oportunidad de oro a los ciberdelincuentes.

Más allá de la pandemia, la transición desde infraestructuras tradicionales a plataformas basadas en la nube, la creciente interconectividad y la aparición de nuevas tecnologías como la inteligencia artificial ha provocado un crecimiento de los ciberataques "en términos de sofisticación, complejidad e impacto", según Enisa. En su informe de 2021 , la agencia avisó de que "esta tendencia [la aceleración de la transformación digital] ha aumentado la superficie de ataque y, como resultado, el número de ataques cibernéticos dirigidos a organizaciones y empresas a través de oficinas en el hogar".



La Administración pública, las cadenas de suministro y las redes sanitarias se convirtieron en prioridades para los cibercriminales durante la pandemia. Como en el caso de Irlanda, otra institución que sufrió el impacto de los ciberataques fue el Hospital Universitario de Brno, en Chequia, que en marzo de 2020 se vio obligado a cerrar su red informática, teniendo que posponer operaciones urgentes y reubicar pacientes graves. Incluso las propias instituciones europeas sufrieron un ciberataque en marzo de 2021, aunque sin brecha de seguridad aparente.

Rusia quiere tus datos

El anonimato que caracteriza este tipo de agresiones dificulta identificar al enemigo y responder de manera proporcional. Mucho más cuando se trata de grupos no estatales detrás de los que se esconden Gobiernos que no dudan en condenar en público este tipo de actos. Resulta difícil establecer la *cibercapacidad* de cada país, pero no hay duda de que Rusia es uno de las grandes potencias del sector. Moscú utiliza el ciberespacio para impulsar sus aspiraciones geopolíticas: desde reforzar su papel de potencia global o consolidar el control de su área de influencia hasta desestabilizar y debilitar organizaciones que considera enemigas como la UE o la OTAN.

Los ejemplos se cuentan por decenas: Alemania, Italia, Países Bajos y Dinamarca han denunciado en los últimos años haber sido víctimas de ciberespionaje ruso. Francia, por su parte, comunicó a

comienzos de 2021 que varias de sus empresas, entre ellas Airbus y Orange, se habían visto comprometidas por un ataque a manos de hackers vinculados a Rusia. Y el pasado mes de septiembre Josep Borrell, Alto Representante de la Unión Europea para la Política Exterior, acusó a Moscú de tratar de internarse en los ordenadores de numerosos políticos europeos, periodistas, altos cargos de empresas energéticas y otros ciudadanos con cierta relevancia social.

Aparte de acceder a información sensible, los cibercriminales rusos buscan extraer información personal de ciudadanos europeos para bien exigir un pago o poner en jaque el sistema de protección de datos de Europa, demostrando la vulnerabilidad de sus sociedades. El problema es que resulta muy complicado demostrar que esos ataques cuentan con el respaldo del Kremlin, por lo que en la mayoría de ocasiones las acusaciones se basan en indicios que no son suficientes para exigir explicaciones a Rusia.

Bruselas se protege

La Unión Europea es consciente de que se ha convertido en el centro de la diana de los ciberataques rusos y de que existen brechas de seguridad en las redes europeas. Para sellarlas, la Comisión actualizó en diciembre de 2020 su estrategia de ciberseguridad y presentó una nueva directiva sobre medidas para un alto nivel común de ciberseguridad en la Unión. Ambos pasos pretenden reforzar la capacidad operativa comunitaria para repeler ciberataques y extender la red de protección a nuevos sectores, además de promover la inversión en ciberseguridad de las organizaciones europeas, que es un 41% inferior a la de Estados Unidos .

Por si fuera poco, en las últimas semanas el conflicto entre Rusia y Ucrania ha alertado más si cabe a la Unión Europea: el Banco Central Europeo ha pedido a los bancos nacionales de los Veintisiete que se preparen para contrarrestar ciberataques rusos. Además, la presidencia francesa del Consejo de la Unión Europea ha promovido la realización de un simulacro de ciberataque a gran escala en las cadenas de suministro de los Estados miembros.

Todos estos movimientos apuntan en la misma dirección: la ciberguerra ya está en marcha . Y aunque no se derrame sangre, lo cierto es que también tiene un impacto directo en la vida de los ciudadanos. Con las espadas —u ordenadores— por todo lo alto y con Rusia y la transformación digital como principales amenazas, la Unión Europea libra su particular batalla para poner de acuerdo al mundo y hacer del ciberespacio un entorno seguro.

3. Desequilibrios de poder y libertad de consentimiento: La Europa de la fortaleza digital

El ecosistema de los datos biométricos europeos de seguimiento y vigilancia

Resumen: Descripción de los principales sistemas que se utilizan en Europa para gestionar la movilidad de las personas a través de las fronteras europeas y entre sus países, centrándose en los aspectos mejorables de los mecanismos actuales.

Autor: Instituto Mediterráneo de Investigación Periodística (MIIR)

Enlace: Disponible a partir del 26 de abril de 2022

Texto:

La digitalización y la transición en línea de cada vez más aspectos de nuestras vidas es una tendencia a largo plazo acelerada por la pandemia del COVID-19. Sin embargo, lo que pasa desapercibido es la misma tendencia que implica a los superpoderes de recopilación de datos y vigilancia de los Estados de la UE.

Las autoridades nacionales de los Estados miembros, como la policía, los servicios de seguridad interior, los guardias fronterizos, las autoridades de inmigración y los organismos europeos como Europol y Frontex, gestionan infraestructuras de recogida y almacenamiento de datos a gran escala. Con el pretexto de la "seguridad nacional", se está creando un espacio para posibles violaciones de los derechos humanos fundamentales, en un momento en el que la seguridad fronteriza "militarizada" ya ha provocado violencia contra los refugiados, retrocesos con el riesgo de que las personas regresen a países inseguros y en condiciones inhumanas, y un alarmante aumento de las muertes evitables.

Los países están cerrando las rutas migratorias -con la reciente y discriminatoria excepción de los refugiados ucranianos-, lo que obliga a los migrantes y refugiados a buscar otras alternativas, a menudo más peligrosas, y los empuja a los brazos de las redes de contrabando de delincuentes.

Pero no sólo se están levantando muros físicos; como informa el Instituto Transnacional independiente TNI (Border War Series), una parte fundamental de la llamada "Fortaleza Europa" consiste en "muros virtuales" que pretenden restringir la entrada de los inmigrantes en el espacio Schengen o vigilar sus movimientos dentro de él. Estos "muros virtuales" tienen muchas formas: desde sistemas avanzados de vigilancia que controlan los flujos migratorios y rastrean los movimientos de las personas en las fronteras exteriores (y a veces antes de ellas) hasta bases de datos de IA "inteligentes" e interoperables que pretenden identificar, registrar y elaborar perfiles de los migrantes en las fronteras y dentro de ellas.

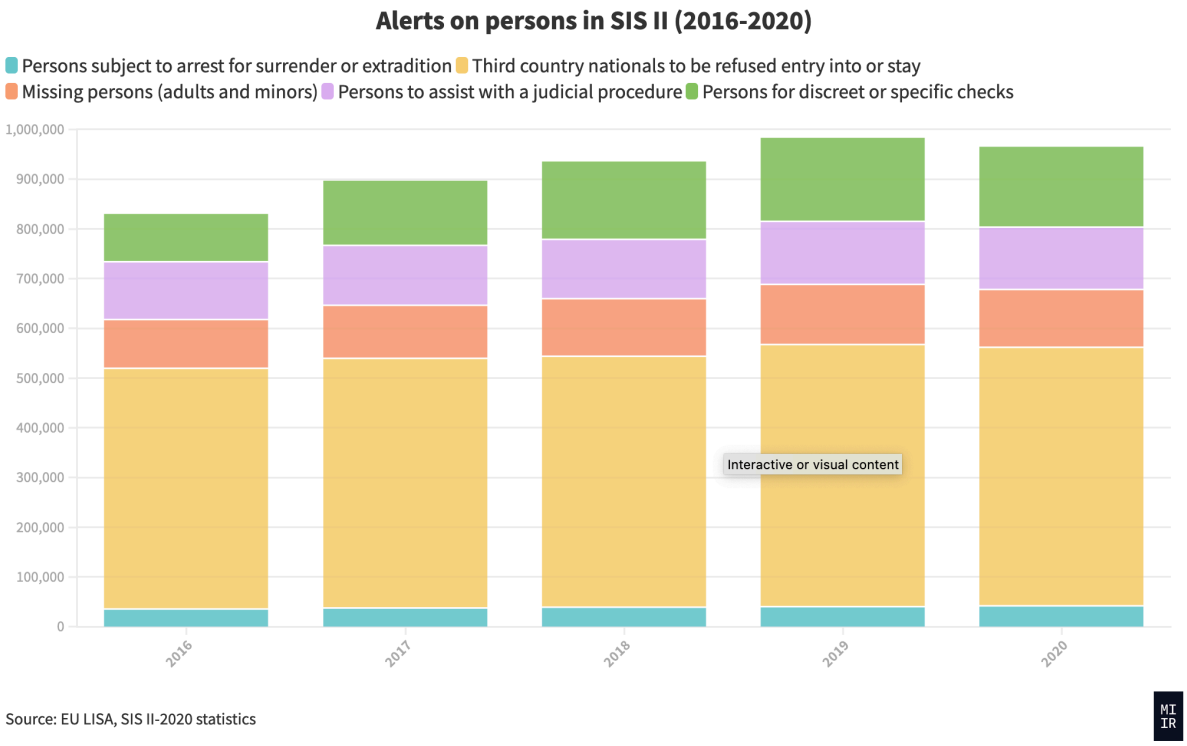
El denominador común de los muros físicos y virtuales es la propia construcción social del "hombre en movimiento" como amenaza potencial para la UE y sus Estados miembros. Las personas que intentan llegar a la UE y entrar en ella, huyendo de catástrofes, violencia, guerra o persecución política, se consideran factores de riesgo que deben ser evaluados y categorizados.

El equipo periodístico del MIIR, en el marco del proyecto Panelfit (Enfoques participativos para un nuevo marco ético y jurídico de las TIC), se propuso penetrar en los diferentes sistemas de registro y vigilancia de datos de la UE, estudiar su legislación y los datos recogidos en las diferentes bases de datos, para identificar los riesgos para los derechos humanos que también crea la interoperabilidad de estos sistemas, basándose en numerosas entrevistas con expertos en la materia, investigadores, activistas, abogados, ONG y migrantes. En la primera parte de la investigación presentamos una breve descripción de los principales sistemas de vigilancia.

Descripción de los sistemas de registro y de las bases de datos personales

1. SIS-II Sistema de Información de Schengen

Es la base de datos más antigua. Su objetivo es controlar los movimientos de los nacionales de terceros países en los espacios Schengen. Se creó originalmente en 1995 para ser actualizada en su segunda versión en 2013 y a partir de los próximos meses entrarán en vigor las disposiciones incorporadas en 2018. Es el mayor sistema informático de Europa, que funciona en 26 Estados miembros de la UE (Chipre no está incluido pero se espera que se incorpore) y en Suiza, Noruega, Liechtenstein e Islandia. En virtud de la normativa del SIS II, se recogen y procesan datos (nombres, apellidos, fechas de nacimiento y otra información alfanumérica) de nacionales de terceros países sujetos a decisiones de retorno, datos sobre la denegación de entrada o estancia de personas en el espacio Schengen y objetos (por ejemplo, coches, armas, documentos perdidos, pasaportes, etc.) con fines de cooperación policial y judicial. Las disposiciones del Reglamento SIS II permiten la aplicación de la identificación biométrica de personas basada en la tecnología de reconocimiento facial. La utilizan tanto las autoridades policiales como las de inmigración y asilo. Si una persona solicita asilo, las autoridades pueden buscar en el SIS para ver si existe una descripción sobre ella. Se pueden introducir descripciones de personas buscadas para ser detenidas o controladas, personas vigiladas por las autoridades policiales, personas que no tienen derecho a entrar o permanecer en la UE, personas buscadas para asistencia judicial y personas desaparecidas (adultos y niños).



El sistema SIS II batió en 2019 un récord con 18 millones de búsquedas diarias por parte de todas las autoridades competentes con derecho a acceder a él. De hecho, esta cifra es tres veces superior a la de 2014 (6 millones de búsquedas diarias). Indicativo del uso generalizado es la introducción a finales de 2020 de la aplicación del Sistema Automático de Identificación Dactilar (AFIS), que permite realizar búsquedas por Estados y a través de las huellas dactilares e introduce la comprobación y comparación automáticas con las búsquedas existentes.

Sin embargo, un indicio del uso ampliado del sistema para identificar a los inmigrantes indocumentados es que de las 964.720 descripciones emitidas en el SIS II en 2020, más de la mitad correspondían a nacionales de terceros países a los que se había denegado la entrada y la estancia en Schengen. Este ha sido el caso de forma constante a lo largo de los años, como muestra el cuadro de descripciones 2016-2020.

2. VIS - Sistema de Información de Visados

Se puso en marcha gradualmente a partir de 2011 y el desarrollo del sistema se completó en 2016. El sistema lo utilizan los 30 Estados de Schengen junto con Bulgaria, Croacia, Chipre y Rumanía. El objetivo es permitir a estos países intercambiar datos sobre visados de corta duración y facilitar los controles de visado en los pasos fronterizos. Las autoridades de asilo competentes pueden acceder al VIS. En 2018, la Comisión Europea presentó una propuesta de revisión del VIS para ampliar su alcance. Las normas propuestas sugieren que el VIS incluya también datos sobre los visados de larga duración.

VIS: Use of biometrics, searches and access

68 million facial images stored in the VIS
By the end of 2019

69 million fingerprints sets stored
By the end of 2019

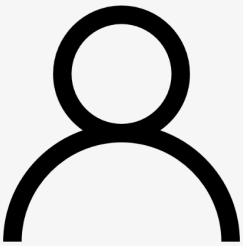
100 million records capacity
By the end of 2019

7 million biometric searches in 2019 (2018: 8 million)
Searches in 2019

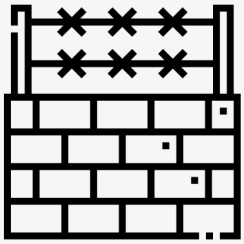
17 million biometric authentications in 2019 (2018: unchanged)
Searches in 2019

25 million alphanumeric searches in 2019 (2018: 23 million)
Searches in 2019

116 national authorities granted access
Access



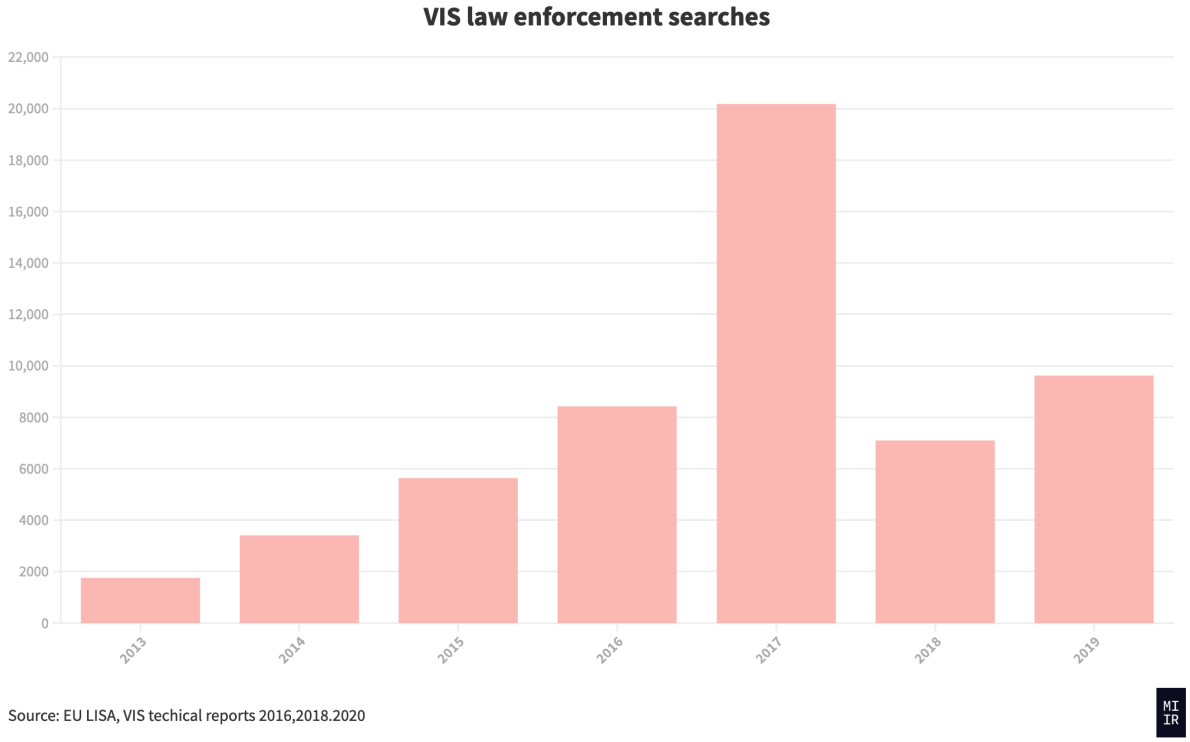
458.000, total number of end-users accessing VIS
Access



84 million border checks (visa verification and identification)
Border checks

El sistema almacena las huellas dactilares y una fotografía de los solicitantes/titulares de visado, así como los datos personales incluidos en sus solicitudes, como el apellido, la dirección del domicilio, la información sobre la situación del visado y los datos bancarios (prueba de depósito). "Sin esto no se concederá el visado. Se trata de una discriminación de clase implícita: si eres rico puedes viajar, si no tienes dinero no te darán razonablemente el visado ("discriminación de baja tecnología"). La cuantía depende de cada Estado miembro", dice el investigador Georgios Glouftios.

La identificación biométrica automatizada ya se utiliza en el VIS a partir de las huellas dactilares recogidas. En 2019, se realizaron 7 millones de registros biométricos y 17 millones de controles de identidad biométricos, estos últimos principalmente en los puestos fronterizos. En los aeropuertos, las autoridades comprueban a los nacionales de terceros países que viajan a Europa para asegurarse de que sus huellas dactilares coinciden con las de su expediente individual en el sistema VIS, que se establece obligatoriamente antes del viaje. Las autoridades policiales pueden consultar el VIS para ver si una persona que ha solicitado previamente un visado está implicada en actividades delictivas. También puede ser utilizado por las autoridades de asilo.



Otro elemento que agrava la preocupación de los ciudadanos y las organizaciones por la privacidad de estos sistemas es el acceso ampliado de los organismos y personas de todos los servicios. Es cierto que cada año se publican en el Diario de la UE las autoridades de cada país que tienen derecho a acceder a la base de datos. Pero esto no es suficiente, ya que el número de usuarios finales que pueden tener acceso a los datos personales de los individuos es incierto. Por ejemplo, en el sistema VIS, un total de 116 servicios y autoridades nacionales, incluidas las autoridades policiales, tienen permiso para crear, modificar y borrar datos, y el número de usuarios finales alcanza la astronómica cifra de 458.000 empleados, todos ellos con acceso a estos datos personales sensibles.

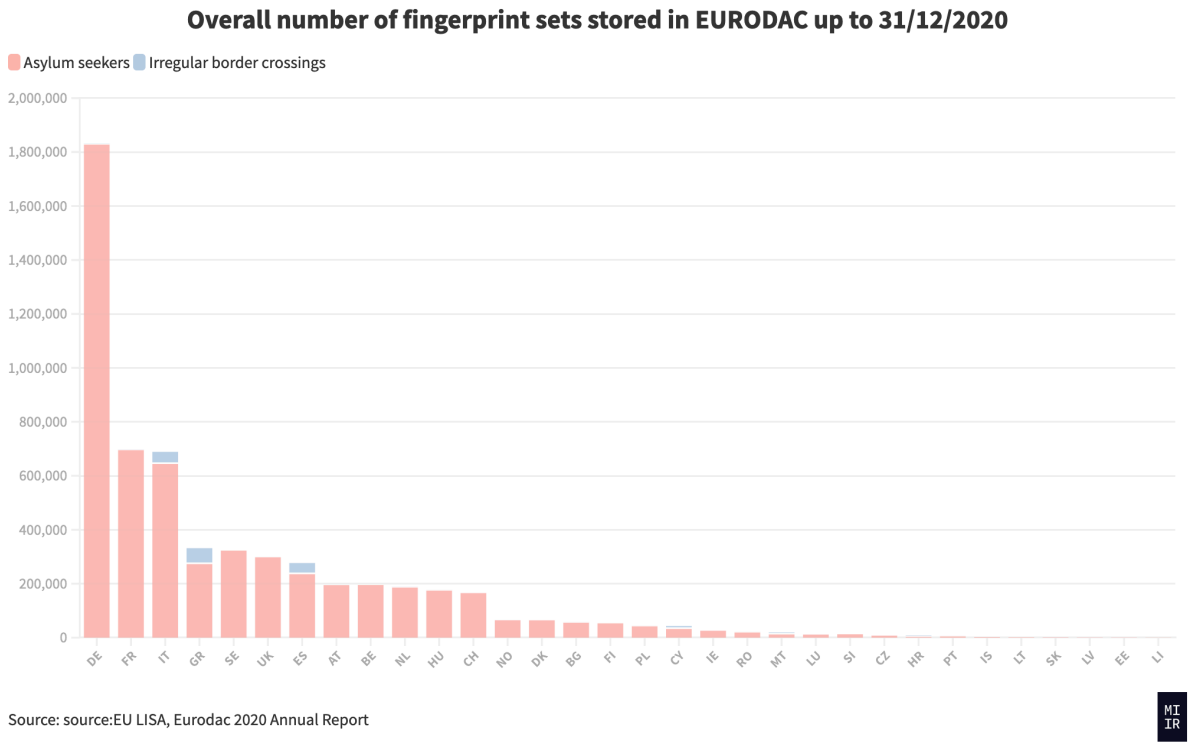
3.Eurodac

El sistema europeo de comparación de las impresiones dactilares de los solicitantes de asilo (EURODAC) entró en funcionamiento en 2003, siendo el primer sistema informático que permite almacenar las impresiones dactilares en una base de datos a nivel de la UE. El objetivo del sistema era facilitar a los países de la UE la determinación de la responsabilidad del examen de una solicitud de asilo mediante la comparación de las huellas dactilares de los solicitantes de asilo y de los nacionales de terceros países/no pertenecientes al EEE con una base de datos central. Además, el objetivo era permitir a las autoridades policiales, en condiciones estrictas, buscar en Eurodac para la investigación, detección y prevención de delitos terroristas o graves. Hasta ahora sólo almacena características biométricas, y ni siquiera registra el nombre de alguien. Cuando un solicitante de asilo o un nacional de un tercer país o del EEE es encontrado ilegalmente en un país de la UE, el país de la UE puede consultar Eurodac para ver si la persona ha solicitado asilo previamente en un país de la UE o si ya ha sido detenida al intentar entrar ilegalmente en la UE.

EURODAC está actualmente en revisión. Las revisiones propuestas prevén la interacción de EURODAC con otros sistemas informáticos de la UE en los procedimientos de asilo, retorno y reasentamiento. En este contexto, EURODAC se utilizará, entre otras cosas, para el control de los flujos migratorios y la detección de movimientos secundarios de nacionales de terceros países en situación irregular.

Sin embargo, las cifras muestran que la recogida y el almacenamiento de huellas dactilares de nacionales de terceros países o apátridas es también una práctica habitual. En concreto, los Estados miembros transmitieron un total de 644.926 conjuntos de huellas dactilares a EURODAC en 2020. De ellos, el 62% representan conjuntos de datos de huellas dactilares de solicitantes de protección internacional, el 25% representan huellas dactilares de un nacional de un tercer país o de un apátrida que se encuentra ilegalmente en un Estado miembro, mientras que el 13% son las de los mismos grupos que se encuentran cruzando ilegalmente la frontera exterior.

La nueva propuesta, si se aprueba, introducirá la obligación de recoger y almacenar las huellas dactilares de los nacionales de terceros países o apátridas que se encuentren en situación ilegal en Europa. Además, el volumen de datos personales recogidos aumentará radicalmente. Las disposiciones propuestas permitirán recoger una amplia variedad de información biográfica y biométrica además de la que ya se recoge, como imágenes de personas, nombres, fecha y lugar de nacimiento y nacionalidad.



Los casi 6 millones de huellas dactilares acumuladas en EURODAC a finales de 2020 no pertenecen exclusivamente a los solicitantes de asilo, sino también a los migrantes que los Estados de acogida han clasificado como "cruzadores de fronteras irregulares", que no tienen derecho a acceder a los procedimientos de asilo. A 31/12/2020, cuando se realizó el registro, sólo representaban casi 155.000 (3%), pero las huellas dactilares de esta categoría se borran automáticamente de la base de datos al cabo de 18 meses, a diferencia de las de los solicitantes de asilo, que se conservan durante 10 años. Por ejemplo, la proporción correspondiente a ellos a finales de 2016 era del 13%. Cabe señalar que, desde julio de 2015, la base de datos EURODAC también es accesible a los servicios policiales de los países y a Europol en nombre de la prevención e investigación de los delitos relacionados con el terrorismo y la delincuencia grave.

Cabe destacar cómo Alemania, aunque no es un país de primera acogida como Italia y Grecia, parece acumular la gran mayoría de los datos biométricos entre los 32 países de Segen. Esto se debe a que una gran mayoría de los migrantes que llegaron a Europa especialmente con la crisis de los refugiados de 2015 solicitaron asilo por primera vez en Alemania, y no en los países situados en los puntos de entrada de las fronteras europeas. En el ranking de almacenamiento biométrico, los países que siguen a Alemania son Francia, Italia, Grecia, Serbia, Reino Unido y España.

También es llamativo que Grecia sea el "líder" entre los 32 países en la recogida de huellas dactilares de los migrantes que no tienen derecho a acceder al asilo. Se trata de 56.000 (es decir, un tercio del total de esta categoría en EURODAC) de un total de 331.609 huellas dactilares registradas por Grecia a finales de 2020. El notable primer puesto griego está relacionado con el proceso de registro de datos y de cribado en los centros de acogida griegos para los migrantes que entran en el país.

La primera etapa oficial del registro, además de la comprobación de los documentos pertinentes que pueda llevar la persona (pasaporte, tarjeta de identidad, otros documentos) es el examen/entrevista/interrogatorio por parte de la policía griega o del personal de FRONTEX, el llamado screening. "El objetivo de este procedimiento es "calibrar" la identidad de la persona, es decir, datos como la edad, la nacionalidad, el lugar de origen, las relaciones familiares, y se realiza en colaboración con los traductores de FRONTEX", afirma Vassilis Vlassis, investigador postdoctoral sobre tecnologías de vigilancia en la Universidad de Informática de Copenhague. Ha realizado un estudio de campo sobre el asilo y los procedimientos de detección en los centros de acogida de Quíos y Lesbos. "En las entrevistas que he realizado", prosigue, "con personas que han sido inspectores en VIAL, en Quíos, resultó que se examinan muchos datos: el habla, la pronunciación, la ortografía, la ropa, las joyas, por supuesto las fotos del teléfono móvil, etc., todo se examina y se tiene en cuenta en la conclusión que sacará el inspector: 'Sé que los sirios escriben Mohamad así y nunca así, mientras que los marroquíes lo escriben así, pero nunca así' me dijeron. El instinto y la intuición también juegan su papel. A veces, en cuanto entran por la puerta, tienes inmediatamente una opinión, y luego buscas validarla, como dijo también uno de los auditores", relata Vlasis. En conclusión, la forma en que estos datos toman forma es multifactorial y tiene fuertes elementos performativos, y sin embargo puede tener un impacto decisivo en el futuro del migrante que se incorpora a EURODAC. "El propio coordinador de la misión FRONTEX en las islas griegas en 2016 me dijo: "el resultado del cribado no constituye un hecho científico. Es una hipótesis de trabajo, lo mejor que podemos hacer y con lo que estamos trabajando'", relata Vlassis.

4. Sistema Europeo de Entradas y Salidas (EES)

Se creó en 2017 y se espera que sea plenamente operativo en mayo de 2022. Recoge datos sobre todos los nacionales de terceros países, independientemente de si necesitan o no solicitar un visado. Registra y almacena la fecha, hora y lugar de entrada y salida de los titulares de visados de corta duración y de los viajeros exentos de la obligación de visado al cruzar la frontera de la UE. El sistema pretende sustituir el procedimiento de sellado del pasaporte permitiendo el tratamiento de los datos biométricos de las personas. También registrará la duración de la estancia de una persona y creará alertas automáticas para situaciones de "estancia excesiva" en un país. Las autoridades policiales nacionales y Europol podrán acceder a esta base de datos.

5. ETIAS - (Sistema Europeo de Información y Autorización de Viajes)

Se creó en 2018 y el objetivo es que esté plenamente operativo en diciembre de 2022. Según las declaraciones de la UE, se trata de "un sistema informático ampliamente automatizado que se creará para identificar los riesgos de seguridad, de migración irregular o de epidemia elevada que plantean los visitantes que viajan a los Estados Schengen y que no están sujetos a la obligación de visado. [...] Los nacionales de terceros países que no necesiten visado para viajar al espacio Schengen deberán solicitar una autorización de viaje a través del sistema ETIAS antes de viajar". Es un ejemplo más de que la UE trata a las personas que planean viajar a Europa como factores de riesgo. No almacenará

ningún tipo de información biométrica. Sin embargo, se recogerán diferentes categorías de datos, como el apellido del solicitante, su nacionalidad, su país y ciudad de residencia, su domicilio, su dirección de correo electrónico y su número de teléfono, y su situación educativa (primaria, secundaria, superior o sin estudios).

En la práctica, el sistema ETIAS funcionará de forma muy parecida al sistema ESTA de Estados Unidos.

6. ECRIS-TCN (Sistema Europeo de Información de Antecedentes Penales para Nacionales de Terceros Países)

Creado originalmente en 2012, ECRIS permite el intercambio eficaz de información entre los Estados miembros sobre condenas penales en la UE. La mayor parte de la información intercambiada se refiere a ciudadanos europeos. El Sistema Europeo de Información de Antecedentes Penales revisado incluirá ahora una base de datos central de información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) y se espera que esté operativo en 2022. Los datos biográficos y biométricos de los nacionales de terceros países condenados, los apátridas y los ciudadanos de la UE que son nacionales de terceros países y han sido condenados en un Estado miembro se almacenan en ECRIS-TCN. Estos datos incluyen categorías como el nombre completo, el lugar y la fecha de nacimiento, la nacionalidad, el sexo, los números de identidad, así como los datos dactiloscópicos recogidos de conformidad con la legislación del Estado miembro durante el proceso penal. Las imágenes faciales de los condenados también se almacenarán en el sistema si la legislación del Estado miembro de condena permite la recogida y el almacenamiento de imágenes faciales de los condenados. La base de datos estará disponible en Internet y las autoridades podrán buscarla fácilmente con un mecanismo de búsqueda positiva/negativa: un resultado de búsqueda positivo identificará los Estados miembros de los que se puede obtener información completa sobre los antecedentes penales de una persona concreta.

ECRIS se ha utilizado alrededor de 3 millones de veces al año para intercambiar información sobre condenas penales anteriores. Alrededor del 30 % de los casos en los que se solicita información sobre antecedentes penales reciben una respuesta positiva.

Según la Comisión Meijers, un grupo de profesores de derecho, investigadores, jueces y abogados que trabajan para que la legislación europea respete el Estado de Derecho y garantice los derechos fundamentales de todos, el reglamento ECRIS-TCN es la primera legislación europea que trata como nacionales de terceros países a los ciudadanos europeos que también son nacionales de un tercer país.

Interoperabilidad de los sistemas

Los servidores de todos estos sistemas se encuentran en Estrasburgo. Allí los servidores son gestionados por el servicio EU-Lisa. Cuando pensamos en controles fronterizos y de movilidad solemos pensar en Frontex, pero Frontex no es el protagonista de estas bases de datos. EU-Lisa, la Agencia Europea para la Gestión Operativa de Sistemas a Gran Escala en el Espacio de Libertad, Seguridad y Justicia, funciona desde 2012, tiene su sede en Tallin (Estonia), pero su centro operativo está en Estrasburgo. Ha coordinado las pruebas del proyecto piloto Smart Borders y las acciones posteriores, el análisis de los resultados y la elaboración de informes sobre este proyecto, en estrecha colaboración con los países de la UE participantes y las instituciones europeas. EU-Lisa es responsable de la gestión operativa de EURODAC, SIS II, VIS y Entry-ExitSystem, al tiempo que garantiza la seguridad de la información y la protección de los datos.

En 2019, la UE adoptó dos reglamentos que establecen un marco jurídico que exige la interoperabilidad de 6 de las bases de datos descritas anteriormente (VIS, SIS II, Eurodac, Sistema de Entrada-Salida, ECRIS-TCN y ETIAS). El objetivo es implantar el sistema general de interconexión de datos para finales de 2023.

Aunque la Comisión Europea presenta la interoperabilidad como una progresión natural, en la práctica no es así, ya que muchas de las bases de datos existentes aún no son plenamente operativas.

"Punto de no retorno"

Según el Supervisor Europeo de Protección de Datos, la decisión del legislador de la UE de hacer interoperables estos sistemas supondría un "punto de no retorno", con profundas implicaciones para el derecho a la intimidad de las personas que entran en la UE. Una nueva base de datos central que contiene información sobre millones de nacionales de terceros países, incluidos sus datos biométricos, tendría un nuevo y mejor acceso a los sistemas de información.

Otras cuatro plataformas de recogida de datos en la UE entrarán en funcionamiento o está previsto que amplíen su alcance en los próximos dos años. El Portal Europeo de Búsqueda (PES) permitirá a las autoridades nacionales y competentes de la UE, cuando no puedan identificar a una persona o tengan dudas sobre la identidad facilitada, poder iniciar una consulta presentando datos biográficos o biométricos al PES, que buscará en las 6 bases de datos simultáneamente. El Servicio de Comparación Biométrica creará y almacenará plantillas a partir de todos los datos biométricos registrados en los sistemas subyacentes. El Depósito Común de Identidad (CIR) almacenará un registro individual para cada persona inscrita en los sistemas, que contendrá datos biométricos y biográficos. Por último, el Detector de Identidades Múltiples podrá cotejar las identidades en todos los sistemas.

Como se indica en el informe Technological Testing Grounds de la Red EDRI y el Refugee Law Lab, cuya autora es Petra Molnar, este marco único de interoperabilidad proporciona una infraestructura favorable para muchos procesos de toma de decisiones automatizados que ponen en peligro los derechos humanos. El director de Statewatch, Chris Jones, autor del informe "Sospecha automatizada: las nuevas iniciativas de vigilancia de los viajes de la UE", dijo: "El entusiasmo de los funcionarios de la UE y de los Estados miembros por utilizar nuevas técnicas y herramientas sobre viajeros desprevenidos es preocupante, ya que aumentan el riesgo de discriminación, pueden dar lugar a más

errores en la toma de decisiones y entregarán más datos personales a los gobiernos. La gente debería pensar más en cómo tratan sus gobiernos a los extranjeros; de lo contrario, ellos también podrían ser tratados como sospechosos en lugar de ciudadanos."

También llama la atención la ausencia total de una evaluación de impacto por parte del legislador sobre el impacto en los derechos humanos de los nuevos sistemas interoperables y sobre los recursos y el alcance de las autoridades independientes que controlan estos sistemas, para exigirles responsabilidades.

Uno de los escollos del desarrollo tecnológico es que tendemos a creer que aumentará la eficiencia y ayudará a alcanzar los objetivos para los que fue diseñado. Con demasiada frecuencia, esto no es así. Un primer problema importante que se plantea tiene que ver con la calidad de los datos que se introducen en algunas de las bases de datos mencionadas que hemos presentado. "Por ejemplo, según un informe publicado recientemente por el Tribunal de Cuentas Europeo, hay un problema importante con la calidad de los datos introducidos en el Sistema de Información de Schengen. Y la calidad aquí puede referirse tanto a los datos biométricos como a los alfanuméricos. Por ejemplo, puede ocurrir que un agente de policía de un Estado miembro escriba mal el nombre de una persona buscada al introducir una alerta en el sistema o que introduzca el nombre de una persona en el campo de datos dedicado a los apellidos", afirma el investigador Georgios Glouftios. Si una persona se registra en una base de datos con un nombre incorrecto o con otros datos de mala calidad, pueden surgir dos problemas. El primero se refiere a los falsos negativos: las personas buscadas o sospechosas no son identificadas por el sistema simplemente porque sus nombres no están correctamente almacenados en la base de datos. El otro problema son los falsos positivos, es decir, la identificación incorrecta de una persona. Por ejemplo, alguien es controlado por la policía por cualquier motivo y por error su nombre se parece mucho o es el mismo que el de una alerta errónea almacenada en el sistema. En este caso, puede tener problemas precisamente porque el sistema lo identifica incorrectamente como una persona buscada.

"Creo que hay tres problemas principales en cuanto a la precisión de las tecnologías aplicadas para la seguridad de las fronteras. En primer lugar, la mala calidad de los datos. Segundo, la falta de exhaustividad de los datos. Y tercero, y esto se refiere más a la evolución futura, datos sesgados y decisiones de seguridad potencialmente sesgadas", afirma Georgios Glouftios.

* Cita de "Technological Testing Grounds, Migration Management Experiments and Reflections from the Ground Up" (EDRi, laboratorio de derecho de los refugiados, noviembre de 2020, autora Petra Molnar)

Atrapado en un sistema de vigilancia digital

Resumen: El impacto de los sistemas de vigilancia en las poblaciones vulnerables, el dinero para los drones de Frontex y el control de los movimientos de los ciudadanos dentro del espacio europeo.

Autor: Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

Enlace: Disponible a partir del 26 de abril de 2022

Texto:

En el consulado griego de Estambul, una mañana de 2016, Erkan, ciudadano turco de origen kurdo, cruza el umbral del edificio para dirigirse a las autoridades griegas. Solicitaba un visado para entrar en Grecia con el fin de huir de Turquía en un momento en el que el régimen de Erdogan intensificaba la persecución, especialmente contra los dirigentes y miembros del partido de la oposición HDP y sus partidarios kurdos. Sin embargo, la autoridad consular griega rechazó la solicitud de visado y Erkan se vio obligado a permanecer en Turquía.

Orestiada Evros, 4 años después. Erkan fue detenido en la frontera greco-turca cuando intentaba entrar en territorio griego y fue llevado al tribunal. El tribunal le condenó a 4 años de prisión sin suspensión y a una multa de 10.000 euros por entrar de nuevo en el país. Pero Erkan no había vuelto a entrar en Grecia.

¿Qué había pasado? Ante los jueces griegos, Erkan pidió asilo a Grecia por la persecución del régimen de Erdogan, pero se le comunicó que su nombre figuraba en la Lista Nacional de Extranjeros No Deseados (EKANA) y en el Sistema de Información de Schengen (SIS II, el mayor sistema de intercambio de información entre los países de Schengen), con una nota en la que se le prohibía entrar en el país durante 7 años. Debido a su inclusión en estas listas, fue llevado primero a la prisión de Komotini y luego a la de Corfú.

"Intentábamos averiguar qué había pasado realmente", cuenta la abogada de Erkan y de Human Rights 360, Eugenia Kouniaki. "Mi cliente nunca había entrado en Grecia y, de repente, fue condenado por volver a entrar en el país. Inicialmente, me puse en contacto con las autoridades policiales, con el director del Servicio de Asilo en Atenas, donde me respondió que mi cliente había sido incluido en el EKANA y el SIS II porque su visado había sido rechazado por el Consulado en Estambul".

La verdad se encuentra sencillamente en el funcionamiento del Sistema Único de Información de Visados Europeos (VISA-VIS) y del SIS II. El consulado griego que tramitó la solicitud de Erkan introdujo la denegación de visado en el sistema VIS y en el SIS II al mismo tiempo. A partir de ese momento, este registro fue suficiente para que fuera a la cárcel, incluso si solicitaba protección internacional.

"Incluso cuando pedí que lo sacaran de la lista de indeseables y del SIS II, ya que Erkan era un solicitante de asilo, la policía griega se negó", describe Kouniaki. "Aparte de que mi cliente no sabía que estaba en la lista, cuando intentamos averiguar por qué se le denegó el visado en 2016, recibimos la vaga respuesta de 'por falsificar algunos documentos'. Cuando intentamos averiguar qué documentos se alegaba que habían sido falsificados, no pudimos comprobar cuáles eran.

Afortunadamente, en el recurso que presentamos para que se retrasara la ejecución de la sentencia, los jueces aceptaron nuestros argumentos, y al cabo de un año salió de la cárcel."

Sin embargo, después de todo este trato injusto y el encarcelamiento, prefirió abandonar el país "porque creía que nunca encontraría justicia", concluye Kouniaki.

Quemarse los dedos para evitar la identificación en EURODAC

La historia de Erkan puede parecer escandalosa, pero por desgracia no es la única relacionada con las consecuencias de las tecnologías de vigilancia y los sistemas de datos biométricos para los migrantes. En el informe "Technological Testing Grounds: migration management experiments and reflections from the ground up" (EDRi, Refugee Law Lab, noviembre de 2020), la autora Petra Molnar, abogada y miembro de EDRi (European Digital Rights), ha recogido multitud de entrevistas con solicitantes de asilo en Bruselas que entraron en contacto con los sistemas de control de la movilidad durante su viaje hacia la seguridad en Europa.

Caleb, un hombre casado de unos 30 años, describe su experiencia en el proceso de asilo diciendo que se sintió "como un trozo de carne sin vida, sólo huellas dactilares y escáneres de iris". Otra migrante, Esche, describe su encuentro con los drones en el Mediterráneo y el Canal de la Mancha con una frase demoledora en el momento en que los vio en el cielo: "ahora tenemos ordenadores voladores en lugar de más asilo".

La historia más desagradable la cuenta Negassi, un joven etíope de 20 años: "Estoy cansado y quiero ir a Inglaterra", dice después de haber estado varado en Bruselas durante casi dos años, indocumentado, y antes lo mismo en Núremberg durante 5 años. Pero esta no es su primera vez en Bélgica, ya que antes fue deportado a Alemania cuando fue detenido en un parque de Bruselas, donde dormía a la intemperie. Cuando la policía belga le tomó los datos biométricos, sus huellas dactilares arrojaron un resultado positivo en el sistema EURODAC, que almacena e identifica las huellas dactilares de los solicitantes de asilo, identificándolo como solicitante de asilo por primera vez en Alemania. Así que le devolvieron a causa de Dublín II, que estipula que el primer país de acogida debe tramitar la solicitud.

Negassi reconoce que el proceso de recogida de datos biométricos es invasivo para el cuerpo, pero se pregunta: "¿Cómo voy a negarme si la policía me esposa, me lleva a la comisaría y me obliga a dar mis huellas dactilares?", dice a Molnar. Tiene amigos que han llegado a quemarse los dedos para alterar sus huellas dactilares y evitar la identificación. "Sin embargo, eso no resuelve el problema" para Negassi, ya que la no identificación suele suponer un periodo de detención más largo.

"Hay un aspecto muy importante que no se discute lo suficiente en el debate público", nos dice Petra Molnar, "y se refiere al hecho de que estas tecnologías de vigilancia causan traumas a personas que ni

siquiera están familiarizadas con la tecnología. Todos los inmigrantes con los que hablé tenían la firme convicción de que estaban experimentando un trato racista y discriminatorio a través de su contacto con estos sistemas."

Por eso es aún más importante, continúa, "en cuanto al uso desenfrenado de estas tecnologías, que haya responsabilidad, supervisión y gobernanza. Tenemos que centrarnos en qué tipo de estructuras de gobernanza hay que desarrollar para garantizar que estas tecnologías, que suponen un riesgo para los derechos humanos, no causen traumas a las personas".

Sin embargo, la parte de la responsabilidad no parece mejorar por la forma en que se desarrollan estos sistemas. La participación de empresas privadas en las industrias de seguridad y defensa complica aún más las cosas. "Hay una relación muy problemática de empresas privadas e instituciones estatales que trabajan juntas bajo el pretexto de que los propios Estados no pueden desarrollar estas tecnologías internamente", señala Molnar. "Así que se destinan enormes recursos públicos a las grandes empresas para que las desarrollen. Pero también desde el punto de vista legal, se crea el problema de lo que algunos llaman 'blanqueo de responsabilidades' cuando algo sale mal. En estos casos, como hemos visto, el Estado dice 'no es nuestro problema porque no hemos desarrollado esta tecnología'. Y la empresa privada, por su parte, replica que 'la culpa es de la gestión estatal de las herramientas'".

Pero los presupuestos públicos para el complejo industrial de la gestión de la migración y el control de las fronteras son considerables, señala Molnar. "De todo ese dinero en una tecnología tan problemática que inflige traumas, imaginemos que se destinara a la educación, a los servicios jurídicos, a la vivienda. ¿Por qué los Estados, en lugar de invertir tanto dinero en tecnologías de vigilancia, no piensan en cómo utilizarlo para la inclusión social?"

El sistema europeo de vigilancia de fronteras (Eurosur) y el dinero para los drones

Quizás el sistema más interesante para las cuestiones migratorias sea Eurosur, que elabora mapas de las fronteras territoriales/terrestres y marítimas. Está operado por Frontex y permite el intercambio de mapas entre Estados en relación con los controles fronterizos en el mar. "El desarrollo de Eurosur se puso en marcha en 2007, pero llega al Parlamento Europeo por primera vez a finales de 2012, después de que se hayan gastado cientos de millones y se haya completado su diseño, presentando efectivamente a la institución un hecho consumado. Debido a la falta de transparencia, la investigación en las direcciones pertinentes de la Comisión Europea está en gran medida capturada por las prioridades del complejo de seguridad-industria", informó el periodista Apostolis Fotiadis en su libro "Border Merchants".

Cuando se desarrolló por primera vez se promocionó como una "tecnología humanitaria", un sistema que permitiría a las autoridades de cada estado miembro realizar operaciones de búsqueda y rescate. La idea era que "utilizamos los mapas, obtenemos información de los satélites y también de los

drones, para percibir los flujos migratorios, por ejemplo de África a Europa, y así poder rescatar a las personas en el mar". El problema es que Eurosur crea las llamadas imágenes prefronterizas. Son mapas que se centran en la zona anterior a la frontera, antes de que un barco llegue a la frontera marítima, por ejemplo, Grecia. "Principalmente lo hacen para organizar operaciones de retirada, porque por ejemplo las autoridades italianas pueden compartir datos con las autoridades libias para que éstas puedan retirar a los migrantes. Saben que las devoluciones no están permitidas, así que la solución es la retirada. Por eso se financia a Libia", explica al MIIR Georgios Glouftios, profesor de la Universidad de Trento.

Para la creación de los mapas prefronterizos, Frontex también coopera con el Centro de Satélites de la Unión Europea (EU SatCen), que le proporciona imágenes de satélite, fotografías aéreas y otros servicios relacionados. La base de datos Eurosur también registra los incidentes que se producen en las fronteras marítimas de la UE, aunque los Estados miembros no estaban obligados hasta ahora a cargar los datos de los incidentes en los puestos de control fronterizos de forma sistemática y organizada (esto cambió con un reglamento de aplicación en abril de 2021). Lo que significa que no existe un registro completo y metódico de los incidentes, desdibujando la imagen global de los incidentes en las fronteras exteriores. Un hecho que también admite la Comisión Europea en el informe de evaluación de Eurosur (septiembre de 2018).

El segundo informe de Frontex en 2018 sobre el funcionamiento de Eurosur registró más de 184.000 incidentes en el periodo comprendido entre diciembre de 2013 y principios de 2018, la gran mayoría (147.827) relacionados con flujos migratorios.

Events inserted in Eurosur 2013-2018

Eurosur Node	Crisis	Irregular migration	Related crossborder crime	Other	Total events
Member State	66	83,845	20,641	686	105,238
Frontex	80	63,982	12,231	3029	79,322
Total	146	147,827	32,872	3715	184,560

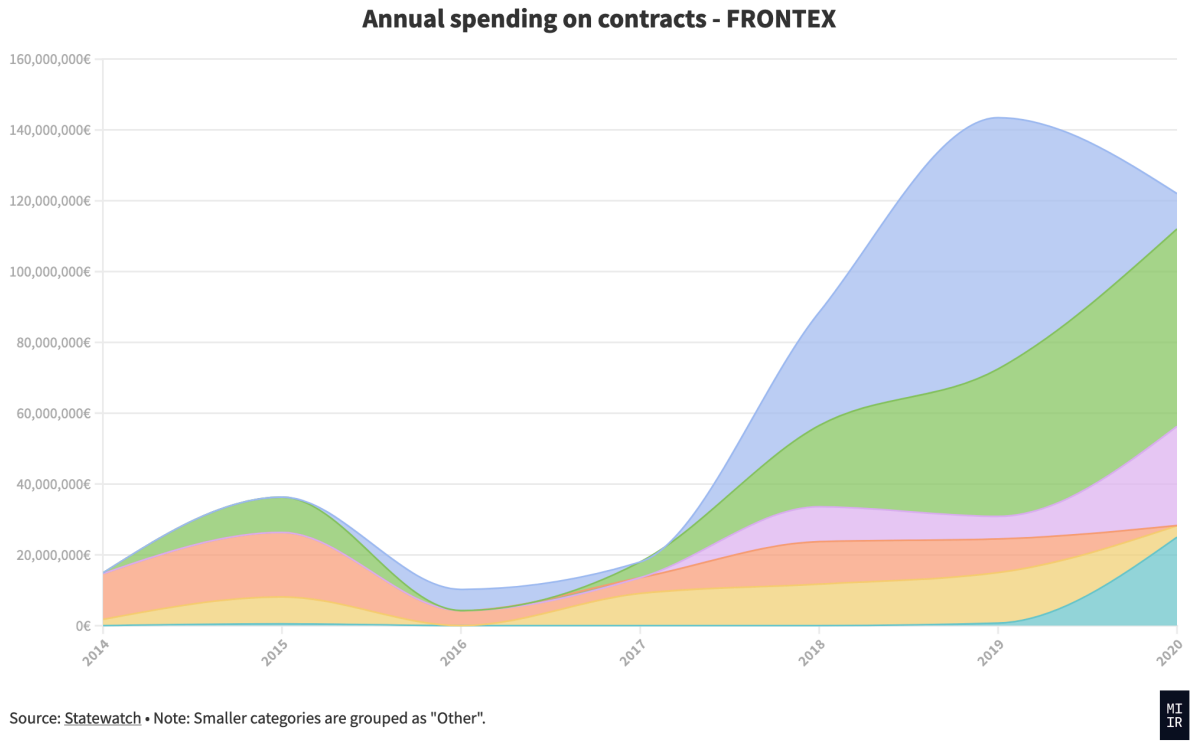
Source: Frontex

En febrero de 2022, el gobierno francés anunció que instalaría más cámaras a lo largo de la costa del Canal de la Mancha para ayudar a controlar a los migrantes que esperan cruzar el tramo de agua hacia el Reino Unido. Las cámaras están siendo pagadas por el gobierno británico. En diciembre de 2021, la marina italiana entregó a Libia un nuevo cargamento de contenedores con equipos de vigilancia para controlar la migración en el Mediterráneo (fuente: revista de investigación Altreconomia, número de febrero de 2021). También se han colocado otras "cámaras trampa" para coches y personas en la frontera entre Italia y Eslovenia, o cerca de ella, a lo largo de la llamada ruta de los Balcanes.

Ojos en el cielo

Frontex confirma que utiliza "un conjunto de servicios incluidos en Eurosur, el marco de intercambio de información diseñado para mejorar la gestión de las fronteras exteriores de Europa" (fuente: infomigrants.net, "Fronteras digitales: La UE aumenta el uso de la tecnología para controlar la migración", 18.2.2022). Afirma que la mayor parte de esta vigilancia se lleva a cabo "mediante la vigilancia aérea con aviones tripulados y no tripulados, con dispositivos de imágenes por satélite y la recogida de las posiciones de los buques mediante sistemas de posicionamiento".

Según un reciente estudio en profundidad ("Fondos para la fortaleza de Europa: gasto de Frontex y EU-LISA", enero de 2022) realizado por la organización sin ánimo de lucro Statewatch, Frontex gasta la mayor parte de su presupuesto anual en vigilancia marítima y aérea, junto con las deportaciones (vuelos fletados y programados para la devolución de migrantes). Según el análisis de datos realizado por Statewatch, entre 2014 y 2020 Frontex, junto con la agencia europea EU-LISA (que supervisa los sistemas de información de control de la movilidad a gran escala), gastó un total de 1.900 millones de euros en contratos con empresas privadas de TI y la industria de seguridad y defensa. De este dinero, unos 500 millones (434 millones de euros) fueron gestionados por Frontex, y más de 100 millones se destinaron a contratos con empresas privadas relacionados con la vigilancia aérea. Esto incluye un contrato de 50 millones de euros con el consorcio Airbus -una de las principales empresas transeuropeas de la industria aeroespacial y de defensa- y la empresa israelí Albeit, que suministra el 85% de los drones del ejército israelí.



https://public.flourish.studio/visualisation/9014574/

En el mismo periodo, Frontex parece haber mantenido una relación provechosa con otros tres proveedores de servicios de vigilancia aérea: la canadiense CAE Aviation, la británica Diamond-Executive Aviation (DEA) y la holandesa EASP Air. Como consorcio, obtuvieron 8 contratos por un valor total de 57 millones de euros (sin contar los contratos que han firmado por sí solos para otros servicios de seguridad y control para Frontex).

La misma tendencia continuó en 2021, con 84 millones de euros -es decir, una sexta parte del presupuesto anual de Frontex- destinados a los servicios de vigilancia aérea.

En el proceso de deportación, Frontex ha trabajado con la empresa polaca eTravel SA en un contrato de 30 millones de euros para prestar servicios de viaje (servicios de reserva y emisión de billetes) para los vuelos regulares de regreso. También ha trabajado con la multinacional británica Air Charter Service Limited y la noruega AS Aircontact en el fletamento de vuelos con el mismo fin.

La organización londinense Privacy International publicó en julio de 2021 sus conclusiones sobre cómo un número cada vez mayor de empresas están "desarrollando satélites capaces de rastrear y vender sus datos a las agencias fronterizas". La organización concluyó que si bien "esta vigilancia puede salvar vidas, también puede facilitar las retiradas o utilizarse para perseguir a los solicitantes de asilo".

El uso de todas estas tecnologías de vigilancia tiene también una consecuencia más profunda, subraya Antonella Napolitano, coordinadora de la red de Privacy International. "Por un lado, contribuye a la criminalización de la persona del migrante, y al mismo tiempo lo convierte en un centro de datos, desde el inicio del viaje desde el país de origen hasta la evaluación de los datos biométricos en la UE. El objetivo es registrar íntegramente sus movimientos y seguirle la pista hasta los siguientes pasos dentro del espacio europeo. De hecho, si se encuentra atrapado debido a un registro o decisión errónea dentro de estos sistemas donde se almacenan sus datos, este error le sigue durante el resto de su vida".

Esta noción no es ajena al riesgo de extender la vigilancia a toda la gama de viajes, ya sea por turismo o por trabajo. Además, señala Napolitano, "la propia interoperabilidad de los sistemas es un buen ejemplo de cómo un sistema desarrollado para vigilar los movimientos migratorios puede luego extenderse a todo el mundo, ya que estos sistemas se amplían progresivamente a todos los viajeros que entran en el espacio europeo, pero también a los ciudadanos de la UE que se desplazan dentro de ella".

"Ser considerado potencialmente un 'delincuente por defecto', un concepto que se refleja en la gestión de las tecnologías de vigilancia, no puede dejar indiferente a nadie", concluye Napolitano.

Registro de nombres de pasajeros: el seguimiento de los movimientos intracomunitarios

El Registro de Nombres de Pasajeros (PNR) se refiere al registro de todos los datos de los pasajeros que se desplazan por el territorio europeo, independientemente de que procedan de un tercer país. ¿Qué recoge este sistema? El nombre, la nacionalidad, cuándo hemos viajado, de dónde, a dónde, nuestro correo electrónico, nuestra dirección. Aparte de eso, puede averiguar nuestros compañeros de viaje, posiblemente algunos datos relacionados con nuestra estancia, como las reservas de hotel, si viajamos por motivos de negocios o personales. Probablemente pueda incluso averiguar en un caso extremo nuestra religión, ya que el sistema registra incluso la comida que hemos tomado durante nuestro vuelo. Esta comida puede contener datos "interesantes" sobre nosotros, por ejemplo, si comemos kosher somos judíos, si no comemos cerdo significa que somos musulmanes. También puede revelar si alguien es alérgico.

El PNR es accesible para las autoridades policiales de cada país. "Y aquí es donde empiezan los problemas. Existe una directiva europea sobre cómo se pueden tratar los datos personales a través del sistema PNR. Esta legislación europea debe ser transpuesta a la legislación nacional de cada país. El problema es que hay algunos fallos en la transposición de esta directiva en diferentes países, como en Grecia", dice al MIIR el abogado Kostas Kakavoulis, miembro de Homo Digitalis. Según explica, "la directiva europea dice que cada Estado miembro debe establecer o designar una autoridad responsable de la prevención, detección, investigación y persecución de los delitos graves de terrorismo. Por lo tanto, se trata de una autoridad que, o bien se establece desde el principio, o bien existe y se le otorga esta competencia. En Grecia, el legislador ha otorgado esta competencia a un departamento de la Dirección de Gestión y Análisis de la Información de la Policía griega. Por lo tanto, no estamos hablando de una autoridad sino de una dirección de la policía griega. Es absurdo que el organismo que tiene los datos, la policía, pida el acceso a estos datos a un departamento dentro de la policía. Si está sometido a un control jerárquico o si hay presiones en general, es bastante dudoso que un departamento de la policía griega se niegue a proporcionar a otros departamentos de la policía griega los datos que necesitan, incluso si fuera necesario hacerlo. En Francia no es así, ya que se ha creado una autoridad especial independiente para los datos PNR. En Grecia, cualquier fuerza policial puede tener acceso incontrolado a los datos del PNR en cualquier momento y lugar. No hay ningún registro de quién solicitó qué datos, cuándo y con qué fin. Y no existe una política de acceso clasificada. Basta con ser miembro del cuerpo de policía para acceder a estos datos".

En Grecia, la organización Homo Digitalis (miembro de EDRi), en una carta abierta al parlamento, subraya que "los datos en cuestión pueden revelar el patrón de los movimientos de una persona, como la hora del viaje, el lugar de salida y llegada, su correo electrónico y dirección, así como los compañeros de viaje de una persona, pero posiblemente incluso los datos relacionados con la reserva de hotel, etc., revelando así información sobre viajes de negocios o personales e incluso el círculo social de la persona, como amigos o compañeros".

La organización señala que en el proyecto de ley presentado en 2018 en Grecia había:

- falta de un sistema de registro de acceso a los datos del PNR
- falta de control judicial previo sobre el suministro de datos del PNR a las autoridades previas al juicio y a otras autoridades
- el período de conservación de los datos PNR no se limita al período estrictamente necesario

Cuatro años más tarde, siguen existiendo las mismas deficiencias.

La organización subrayó que los datos PNR de los menores transferidos deben describirse con claridad y precisión, y que los datos transferidos no deben revelar ni las creencias religiosas ni la información sobre la salud del pasajero.

Automatización y vigilancia en la Fortaleza Europa

Resumen: La inteligencia artificial y los algoritmos están en el centro del nuevo régimen de control de la movilidad de la UE. Se están tomando decisiones automatizadas de alto riesgo sobre vidas humanas. Se trata de un mercado emergente no regulado de miles de millones de euros con aplicaciones "inteligentes" distópicas.

Autor: Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

Enlace: Disponible a partir del 26 de abril de 2022

Texto:

A finales de junio de 2020, Robert Williams, un afroamericano residente en Detroit, fue detenido en la entrada de su casa delante de sus dos hijas pequeñas. Nadie pudo decirle por qué. En la comisaría le informaron de que se le consideraba sospechoso del robo de una tienda en 2018, ya que su rostro fue identificado por las imágenes de vigilancia de la tienda. La identificación se basaba en la foto de un antiguo permiso de conducir. Tras treinta horas detenido, Robert Williams fue finalmente puesto en libertad. La cínica confesión de los policías de Detroit fue desarmante: "probablemente el ordenador se equivocó".

Un incidente similar le ocurrió en junio de 2019 a Michael Oliver, también residente afroamericano de Detroit, que fue detenido tras la supuesta identificación de su rostro en un vídeo de una cámara de seguridad. Fue llevado a juicio, donde finalmente fue absuelto tres meses después de su detención.

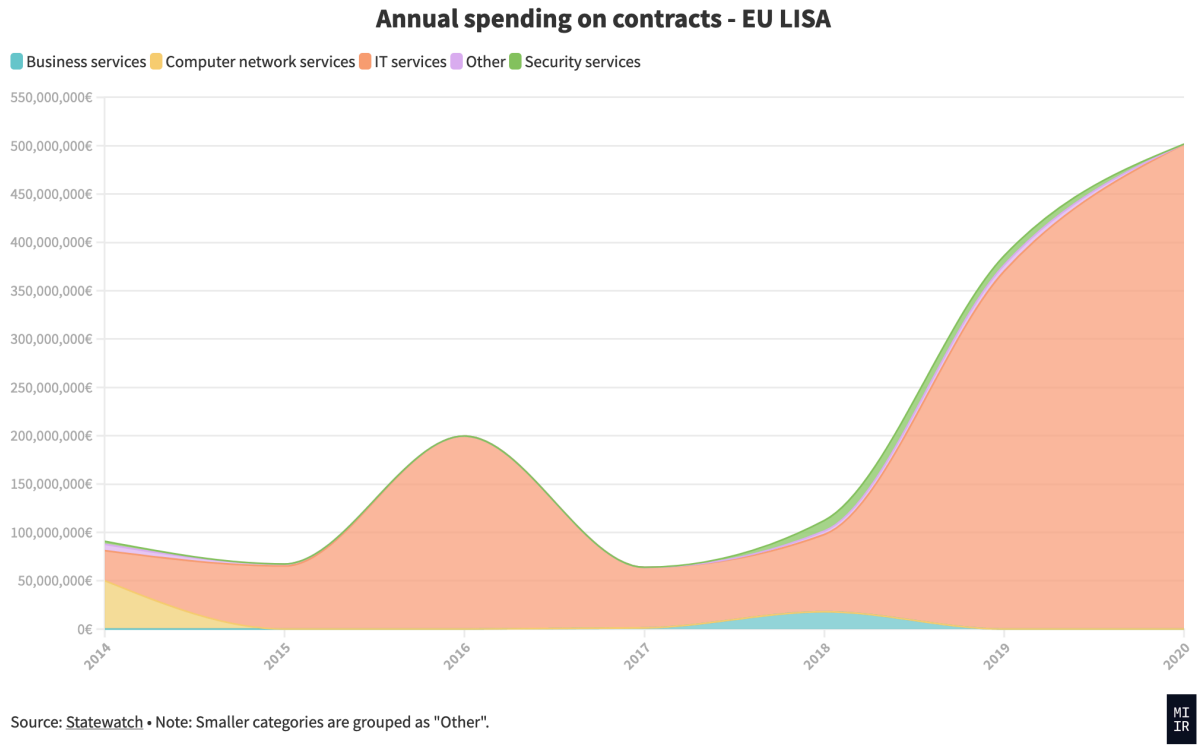
Del mismo modo, en un estudio de prueba del software Rekognition de Amazon, el programa identificó incorrectamente a 28 miembros del Congreso (!) como personas que habían sido arrestadas previamente por un delito. Las identificaciones erróneas afectaban en su gran mayoría a negros y latinos. Pero no hay que suponer que esto sólo ocurre en Estados Unidos.

Como se ha comentado en las dos partes anteriores de la investigación del MIIR sobre "Las murallas digitales de Europa", la UE, como parte de una nueva arquitectura de vigilancia de fronteras y control de la movilidad, ha introducido en los últimos años una serie de sistemas para registrar y controlar a los ciudadanos que se desplazan por el espacio europeo. La UE está utilizando diferentes mecanismos de financiación para la investigación y el desarrollo, con un énfasis creciente en las tecnologías de inteligencia artificial (IA), que también pueden utilizar datos biométricos. Entre 2007 y 2013 (pero con proyectos en marcha hasta 2020) el más relevante fue el Séptimo Programa Marco (PM7), seguido de Horizonte 2020. Estos dos programas han financiado proyectos de seguridad de la UE por valor de más de 1.300 millones de euros. Para el actual periodo 2021-2027, Horizonte Europa cuenta con un presupuesto total de 95.500 millones de euros, con especial atención a las cuestiones de "seguridad". Tecnologías como la toma de decisiones automatizada, la biometría, las cámaras térmicas y los drones controlan cada vez más la migración y afectan a millones de personas que se desplazan. La gestión de fronteras se ha convertido en un rentable negocio de miles de millones de euros en la UE y otras partes del mundo. Según un análisis del TNI (Border War Series), se espera que el crecimiento anual del mercado de la seguridad fronteriza se sitúe entre el 7,2 % y el 8,6 %, alcanzando un total de 65.000 a 68.000 millones de dólares en 2025.

La mayor expansión se produce en los mercados mundiales de datos biométricos e inteligencia artificial (IA). Se prevé que el propio mercado de la biometría duplique su volumen de negocio, pasando de 33.000 millones de dólares en 2019 a 65.300 millones en 2024. Una parte importante de la financiación se dirige a mejorar las capacidades de EU-LISA (Agencia Europea para la Gestión Operativa de Sistemas Informáticos a Gran Escala en el Espacio de Libertad, Seguridad y Justicia), que se espera que desempeñe un papel clave en la gestión de la interoperabilidad de las bases de datos para la movilidad y el control de la seguridad. Las actividades de este superordenador están financiadas por:

- una subvención del presupuesto general de la UE.
- Una contribución de los Estados miembros relacionada con el funcionamiento del espacio Schengen y las medidas relacionadas con Eurodac.
- contribuciones financieras directas de los Estados miembros.

Chris Jones, director ejecutivo de la organización sin ánimo de lucro Statewatch, lleva varios años siguiendo el rastro del dinero que empieza en Bruselas. Explica que "los proyectos EU-LISA suelen estar a cargo de consorcios de empresas privadas, organismos públicos y universidades. Las empresas privadas reciben las mayores sumas, más que los organismos públicos". Un reciente estudio de Statewatch (Funds for Fortress Europe: spending by Frontex and EU-LISA, enero de 2022) destaca que alrededor de 1.500 millones de euros se destinaron a contratistas privados para el desarrollo y refuerzo de EU-LISA en el periodo 2014-2020, y que el mayor incremento se produjo después de 2017 y del momento álgido de la crisis de los refugiados.



https://public.flourish.studio/visualisation/9014422/

El oligopolio de la vigilancia

Uno de los contratos más importantes firmados en 2020, por valor de 300 millones de euros, fue el de las empresas francesas Idemia y Sopra Steria para la implantación de un nuevo Sistema de Correspondencias Biométricas (BMS). Estas empresas suelen conseguir nuevos contratos ya que tienen acuerdos para el mantenimiento de los sistemas EES, EURODAC, SIS II y VIS. Otras empresas a las que se les han adjudicado contratos de alto valor para trabajos relacionados con EU-LISA son Atos, IBM y Leonardo -por 140 millones de euros- y el consorcio Atos, Accenture y Morpho (posteriormente Idemia), que en 2016 firmó un contrato por valor de 194 millones de euros. Los datos recogidos por Statewatch también muestran la cooperación -generalmente a través de empresas conjuntas- en la expansión del sistema EU-LISA con empresas de intereses griegos, como Unisystems SA (propiedad del Grupo Quest del ex presidente de la Asociación de Industriales Griegos Th. Fessa), que firmó un contrato de 45 millones de euros en 2019. Del mismo modo, European Dynamics SA (propiedad de Konstantinos Velentzas) participó en un contrato de 187 millones de euros adjudicado en 2020, y la empresa luxemburguesa Intrasoft International SA (anteriormente propiedad de los intereses de Kokkalis) participa con otras cinco empresas en un proyecto de 187 millones de euros en 2020.

Contracted companies (by contract size) - EULISA

Search...

Company name	Sum of all contracts	Number of contracts	Address
Sopra Steria Benelux SA/NV	604,954,007 €	6	15/23 Avenue Arnaud Fraiteur, Brussels, Belgium
Atos Belgium NV	573,501,690 €	4	DA Vincilaan 5, Zaventem, Belgium
Idemia Identity & Security SAS	302,550,000 €	1	2, place Samuel de Champlain, Courbevoie, France
Accenture NV/SA	271,786,039 €	8	boulevard de Waterloo 16, Brussels, Belgium
Morpho SAS	194,450,000 €	1	11 boulevard Gallieni, Issy-les-Moulineaux, France
ARHS Developments SA	187,000,000 €	1	13 Boulevard du Jazz, Belvaux, Luxembourg
European Dynamics Belgium SA	187,000,000 €	1	15, rue Belliard, Brussels, Belgium
European Dynamics Luxembourg SA	187,000,000 €	1	12, rue Jean Engling, Luxembourg, Luxembourg
European Dynamics SA	187,000,000 €	1	209, Kifissias Ave. & Arkadiou Str, Athens, Greece
Everis Belgique SPRL	187,000,000 €	1	rue de SPA 8, Brussels, Belgium

1 / 5

Source: Statewatch

MI IR

https://public.flourish.studio/visualisation/9468645/

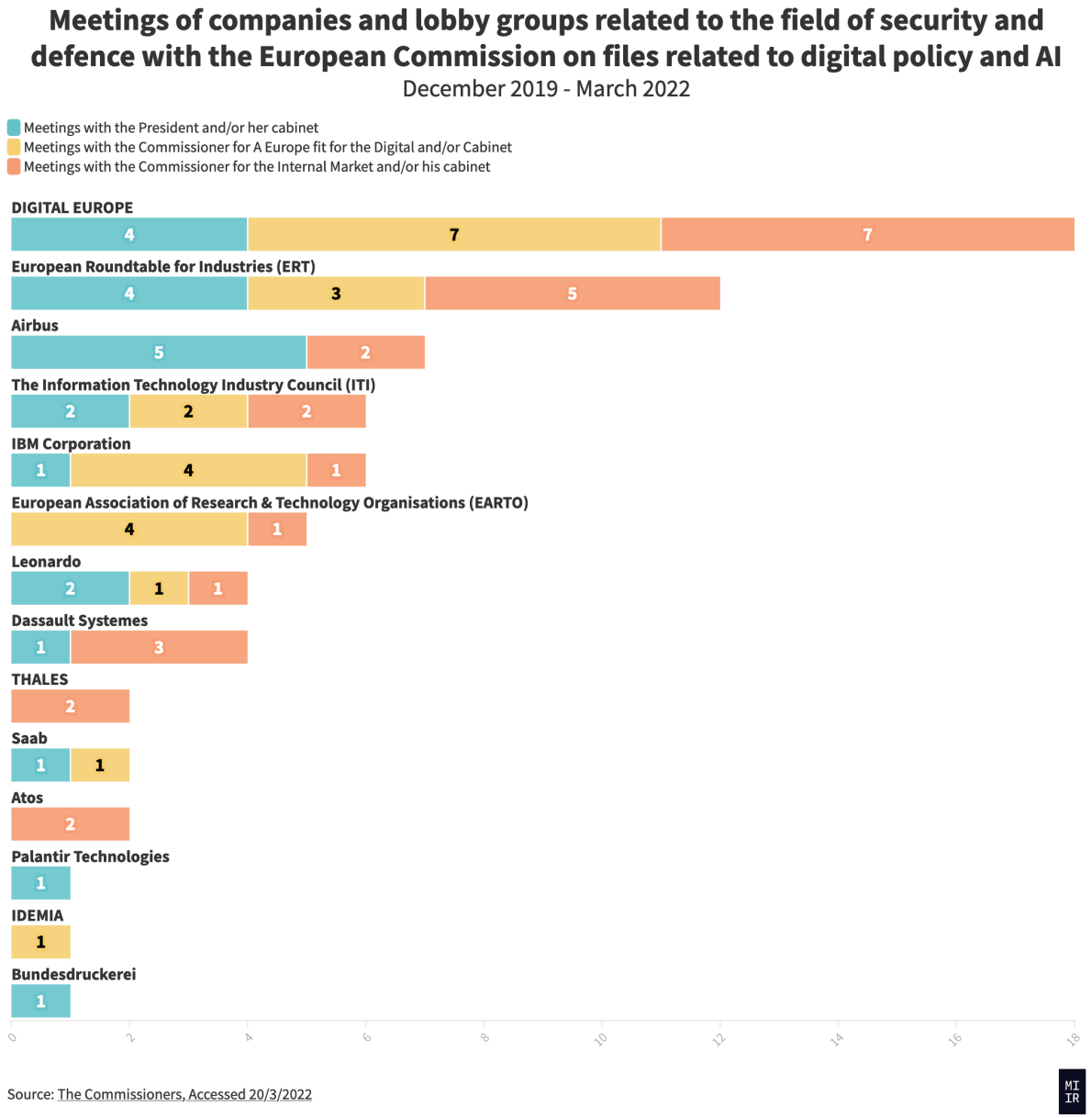
La relación de EU-LISA con la industria también se ilustra con la celebración frecuente de eventos conjuntos, como la "mesa redonda con la industria" que se celebrará el 16 de junio de 2022 en Estrasburgo. Será la decimoquinta reunión consecutiva de este tipo y reunirá a organismos de la UE, representantes de sistemas de gestión de la movilidad y particulares. "Hay negociaciones extensas, largas y muy secretas entre los Estados miembros y los eurodiputados cada vez que quieren cambiar algo en las bases de datos. Pero no sabemos cuál es la influencia real de las empresas que gestionan estos sistemas, si ayudan en lo que es técnicamente factible y cómo interactúa todo esto con el proceso político", afirma Chris Jones, de Statewatch. También se desconoce el contenido de los contratos firmados entre los consorcios y EU-LISA, ya que no se publican.

La nueva frontera de la IA y las presiones sobre la UE

En abril de 2021, la Comisión Europea publicó su esperado proyecto de reglamento sobre inteligencia artificial (AI ACT). Se espera que el proceso de consulta dure algún tiempo. Esta importante pieza legislativa supera las 200 páginas y que será -entre otras cosas- un perfeccionamiento de la legislación sobre protección de datos (Directiva 680/2016). Se espera que las empresas y los operadores del sector ejerzan una presión considerable hasta que el proyecto de ley se presente en su forma definitiva al Parlamento Europeo.

El MIIR ha investigado los registros de las reuniones oficiales sobre cuestiones de política digital y de IA entre la presidenta de la Comisión Europea, Ursula von der Leyen, la comisaria Margrethe Vestager ("Una Europa preparada para la era digital"), el comisario Thierry Breton (Mercado Interior)

y su personal entre diciembre de 2019 y marzo de 2022. Se desprende que al menos 14 agencias, gigantes del sector privado y consorcios de empresas relacionadas con el sector de la seguridad y la defensa se reunieron con los principales representantes de la Comisión Europea 71 veces en 28 meses para tratar temas relacionados con la política digital y la IA. La mayoría de las reuniones con los comisarios fueron celebradas por DIGITALEUROPE, una organización que representa a 78 miembros corporativos, entre los que se encuentran importantes empresas de defensa y seguridad como Accenture, Airbus y Atos. También se identificaron otros consorcios que ejercen una fuerte presión, como la Mesa Redonda Europea de Industrias (ERT), que representa a varias empresas de defensa y seguridad como Leonardo, Rolls-Royce y Airbus.



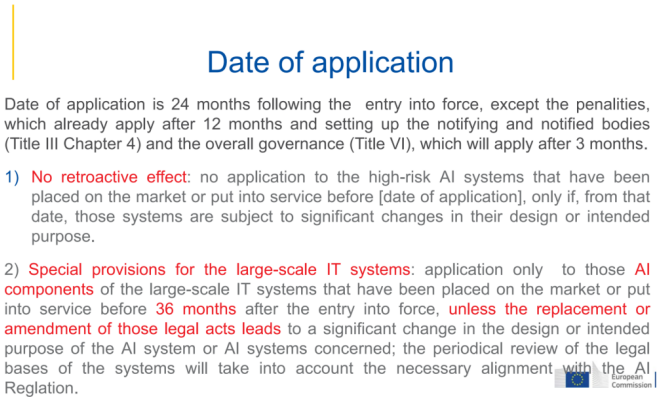
https://public.flourish.studio/visualisation/9083043/

Sistemas de alto riesgo

La propuesta de reglamento europeo (COM/2021/206 final), adoptada en abril de 2021, ofrece una buena visión de los sistemas y aplicaciones de IA que se prevé regular, así como de los riesgos de su funcionamiento no regulado en los puntos de entrada a Europa. Como se indica: "[...] conviene clasificar como de alto riesgo los sistemas de IA destinados a ser utilizados por las autoridades públicas competentes responsables de las tareas en los ámbitos de la gestión de la inmigración, el asilo y el control de fronteras como polígrafos y herramientas similares o para detectar el estado emocional de una persona; para evaluar determinados riesgos que presentan las personas físicas que entran en el territorio de un Estado miembro o solicitan un visado; para evaluar determinados riesgos que presentan las personas físicas que entran en el territorio de un Estado miembro o solicitan un visado; para evaluar el riesgo de los datos personales de una persona [...]"

El parámetro crítico

El ámbito en el que pueden aplicarse los sistemas de IA de "alto riesgo" parece amplio. A pesar de las esperanzas de que una nueva directiva regule su funcionamiento, hay un parámetro que puede eliminar esta posibilidad. Según se desprende de una presentación interna de la revisión interna de la Comisión Europea que tuvo lugar en mayo y que fue sacada a la luz por Statewatch, el nuevo reglamento, si se aprueba, entrará en vigor 24 meses después de su firma y no se aplicará a todos los sistemas, ya que no se prevé que sea retroactivo para los que estén en el mercado antes de la fecha de entrada en vigor.



"Es como si dijera claramente: 'sí, debemos controlar el uso de la inteligencia artificial y el aprendizaje automático de forma responsable. Pero no lo haremos para los sistemas que ya estamos construyendo porque... tenemos otras ideas para ellos...'", comenta Chris Jones. La cuestión también se aborda en la declaración conjunta emitida bajo los auspicios de la red de derechos digitales EDRI en noviembre por 114 organizaciones de la sociedad civil, en la que se destaca que "no se incluye en el proyecto de ley ni se proporciona ninguna justificación razonable para esta exención del reglamento sobre IA". En la comunicación, piden al Consejo de Europa, al Parlamento Europeo y a los gobiernos

de los Estados miembros que incluyan en el proyecto de ley definitivo salvaguardias para la rendición de cuentas que garanticen un marco seguro para la aplicación de los sistemas de IA y, sobre todo, la protección de los derechos fundamentales de los ciudadanos europeos.

Robo-perros en acción: Algoritmos y proyectos de investigación de pesadilla

"Hay un gran esfuerzo por parte de las instituciones de la UE y de los Estados miembros para aumentar el número de deportaciones. La UE ha invertido dinero y recursos y estas bases de datos para decir esencialmente 'queremos ayudar a sacar a estas personas de suelo europeo'", señala Chris Jones, de Statewatch. De hecho, la automatización y el uso de herramientas algorítmicas impulsadas por la industria ya están desempeñando un papel importante en los puntos de entrada a Europa, lo que plantea muchos interrogantes sobre la salvaguarda de los derechos de los refugiados y los inmigrantes. No es sólo la elaboración de perfiles lo que preocupa a quienes critican estos proyectos de la UE, sino también la calidad de los datos en los que se basa este proceso. "Parece una 'caja negra', en la que no sabemos exactamente lo que hay dentro", afirma la especialista en derecho de los refugiados y antropóloga Petra Molnar, que se centra en el riesgo de la automatización sin factor humano en la toma de decisiones cuando determina vidas humanas.

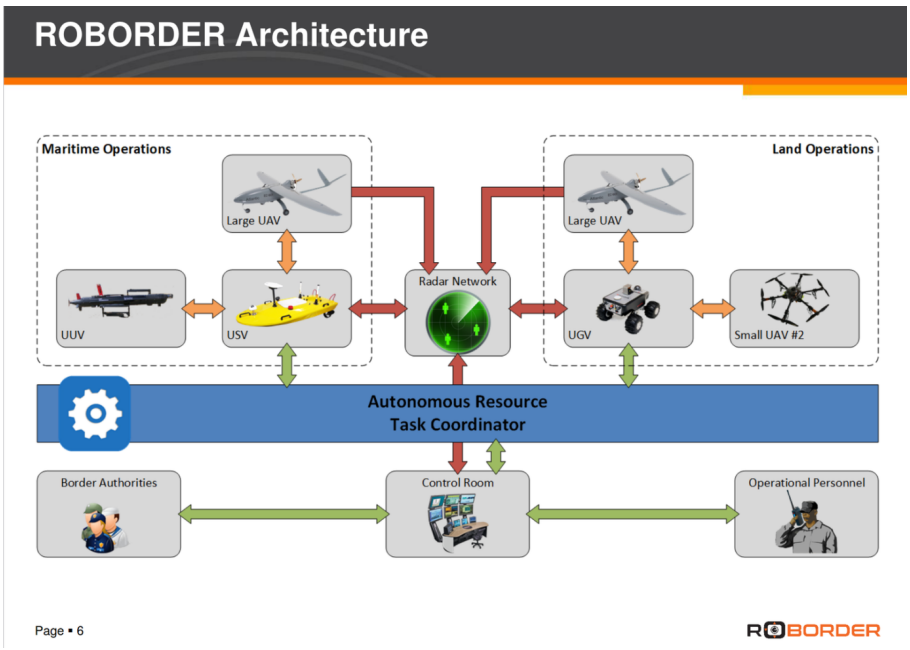
Algunos de los principales sistemas piloto financiados en los últimos años son los siguientes

iBorderCtrl - Detectores de mentiras "inteligentes": Combina herramientas de cotejo facial y autentificación de documentos con tecnologías de IA. Se trata de un "detector de mentiras", probado en Hungría, Grecia y Letonia, que implica el uso de un "guardia fronterizo virtual", personalizado en función del sexo, la nacionalidad y el idioma del viajero: un guardia que hace preguntas a través de una cámara digital. El proyecto se financió con 4,5 millones de euros del programa Horizonte 2020 de la Unión Europea, y ha sido muy criticado por considerarlo peligroso y pseudocientífico ("Sci-fi surveillance: Europe's secretive push into biometric technology", The Guardian, 10 de diciembre de 2020; "We Tested Europe's New Lie Detector for Travelers - and Immediately Triggered a False Positive", The Intercept, 26 de julio de 2019).

Se probó en condiciones simuladas a principios de julio de 2019 en las instalaciones de TRAINOSE, en una zona especialmente diseñada del Centro de Estudios de Seguridad de Atenas. Antes de la salida, el viajero tenía que subir una foto de un documento de identidad o pasaporte a una aplicación especial. A continuación, respondieron a las preguntas formuladas por un guardia de fronteras virtual. Un software especial registraba sus palabras y movimientos faciales, que podrían haber escapado a la atención de un ojo ordinario, y al final el software calculaba -supuestamente- el grado de sinceridad del viajero.

El 2 de febrero de 2021, el Tribunal de Justicia de las Comunidades Europeas se pronunció sobre una demanda presentada por el eurodiputado y activista Patrick Breyer (Partido Pirata) contra la privacidad de este proyecto de investigación, que calificó de pseudocientífico y orwelliano.

Roborder (un enjambre autónomo de robots heterogéneos para la vigilancia de fronteras): Su objetivo es desarrollar un sistema autónomo de vigilancia de fronteras mediante robots no tripulados que incluyan vehículos aéreos, marítimos, submarinos y terrestres. El conjunto de la plataforma robótica integra sensores multimodales en una única red interoperable. Del 28 de junio al 1 de julio de 2021 tuvo lugar en Grecia la prueba piloto final del proyecto, en la que participa el Ministerio de Defensa Nacional griego.



Foldout: El proyecto de investigación Foldout, de 8,1 millones de euros, no oculta sus objetivos: "en los últimos años la migración irregular ha aumentado de forma espectacular y ya no es posible gestionarla con los sistemas existentes". La idea principal del proyecto, pilotado en Bulgaria y que se está extendiendo a Finlandia, Grecia y Guinea Francesa, es colocar sensores de movimiento en los tramos de tierra de la frontera donde el terreno o la vegetación dificultan la detección de un cruce irregular. Ante cualquier movimiento sospechoso, humano o de un vehículo, existirá la posibilidad de enviar un dron a ese punto o activar las cámaras de tierra para una vigilancia adicional. El consorcio que lo desarrolla está coordinado por el Instituto Austriaco de Tecnología (que ha recibido 25 millones de euros de 37 proyectos europeos).

Entre las organizaciones que presionan a favor de estos proyectos a nivel europeo, conocimos a EARTO, un consorcio de centros de investigación y beneficiarios de proyectos en diversos campos, entre ellos el de la seguridad. Entre ellos, KEMEA (Grecia), la Fraunhofer-Gesellschaft (140

proyectos de investigación financiados por la UE, entre ellos Roborder) y el Instituto Austriaco de Tecnología (Foldout).

Muchos de los proyectos de investigación de Horizonte 2020 (Roborder, iBorderCtrl, Foldout, Trespass, etc.) han sido descritos por sus propios autores como todavía "inmaduros" para su uso generalizado. Sin embargo, el cambio general en el enfoque de la Unión Europea sobre el uso de la IA para el control de la movilidad y la prevención de la delincuencia puede verse en la financiación cada vez mayor del Fondo Europeo de Seguridad. Uno de estos proyectos es el suministro por parte de la policía griega de miles de dispositivos móviles que permitirán identificar a los ciudadanos mediante programas de reconocimiento facial y huellas dactilares. El coste total del proyecto, realizado por Intracom Telecom, supera los 4 millones de euros y el 75% procede del Fondo Europeo de Seguridad.

El "experimento" de Samos

"Las fronteras y la inmigración son el laboratorio perfecto para los experimentos. Condiciones opacas y de alto riesgo con bajos niveles de responsabilidad. Las fronteras se están convirtiendo en el campo de pruebas perfecto para las nuevas tecnologías que luego pueden utilizarse más ampliamente en diferentes comunidades y poblaciones. Esto es exactamente lo que se ve en Grecia, ¿verdad? ", se pregunta la abogada Petra Molnar. La respuesta es afirmativa, tanto para el norte como para el sur del país.

En la isla de Samos, en la frontera sureste de Grecia con Turquía, en el nuevo campamento de migrantes que el gobierno griego está casi anunciando, se están poniendo en marcha dos sistemas piloto especiales llamados YPERION y KENTYROS.

YPERION es un sistema de gestión del asilo para todas las necesidades del Servicio de Acogida e Identificación. Trata los datos biométricos y biográficos de los solicitantes de asilo, así como de los miembros de las ONG que visitan las estructuras correspondientes y de los trabajadores de estas estructuras. Está previsto que sea la herramienta principal para el funcionamiento de los Centros de Acogida Cerrados (CRC), ya que se encargará del control de los accesos, del seguimiento de las prestaciones por solicitante de asilo mediante una tarjeta individual (alimentos, suministros de ropa, etc.) y de los desplazamientos entre los CRC y las instalaciones de alojamiento. El proyecto incluye la creación de una aplicación para teléfonos móviles que proporcionará información personalizada al usuario, para que actúe como su buzón electrónico en relación con su proceso de solicitud de asilo, con la posibilidad de proporcionar información personalizada.

KENTYROS es un sistema digital para la gestión de la seguridad electrónica y física alrededor y dentro de las instalaciones, utilizando cámaras y algoritmos de análisis de comportamiento de IA. Incluye la gestión centralizada desde el Ministerio de Gobernación Digital y servicios como : la señalización de alarmas de ruptura del perímetro mediante cámaras (con capacidad de termometría,

enfoque y rotación) y algoritmos de análisis de movimiento; la señalización de alarmas de comportamiento ilegal de personas o grupos de personas en zonas de reunión dentro de las instalaciones; y el uso de sistemas de aviones no tripulados para evaluar incidentes dentro de las instalaciones sin intervención humana.

"KENTYROS utiliza cámaras que tienen una gran capacidad para enfocar a individuos concretos, cámaras que también pueden tomar la temperatura de alguien. Lo más importante no es que KENTYROS utilice esta imagen por motivos de seguridad, sino que también se utilizarán algoritmos de análisis del comportamiento, sin explicar exactamente lo que significa", afirma el abogado y miembro de Homo Digitalis, Kostas Kakavoulis. Como señala, "un algoritmo aprende a llegar a determinadas conclusiones a partir de unos datos que le hemos dado. Un algoritmo de este tipo podrá distinguir que la persona X puede tener un comportamiento más agresivo y atacar a otros solicitantes de asilo o a los guardias, o querer escapar ilegalmente del centro de acogida". Otro uso de los algoritmos de análisis del comportamiento es el análisis de la mentira, que puede juzgar si nuestro comportamiento y nuestras palabras reflejan algo que es cierto o no. Esto se hace principalmente a través del análisis de datos biométricos, los datos que todos producimos a través de nuestro movimiento en el espacio, a través de nuestra presencia física, a través de nuestra apariencia física y también la forma en que movemos las manos, la forma en que parpadeamos, la forma en que caminamos, por ejemplo. Todo esto puede parecer insignificante, pero si alguien puede recogerlos durante un largo periodo de tiempo y puede correlacionarlos con los datos de muchas otras personas, puede llegar a conclusiones sobre nosotros, que pueden sorprendernos, sobre lo agresivo que puede ser nuestro comportamiento, la ansiedad que tenemos, el miedo que tenemos, si decimos la verdad o no". La legislación actual prohíbe el tratamiento de datos personales sin posibilidad de intervención humana.

La abogada Petra Molnar ha investigado recientemente los efectos de las aplicaciones de IA en el control de los flujos migratorios. Estuvo en Samos en la inauguración del nuevo centro de acogida cerrado. "Múltiples capas de alambre de espino, cámaras por todas partes, puestos de huellas dactilares en la puerta giratoria, puntos de entrada y salida. Los refugiados lo ven como un complejo carcelario. Nunca lo olvidaré. La víspera de la inauguración estuve en el antiguo campamento de Vathi, en Samos. Hablamos con una joven madre de Afganistán. Empujaba a su hija pequeña en un cochecito y escribió a toda prisa un mensaje en su teléfono que decía: "Si vamos allí, nos volveremos locos". Y cada vez que veo los campos con estos sistemas, me doy cuenta de que encarna ese miedo que tiene la gente cuando va a estar aislada, y las tecnologías de vigilancia se utilizan para controlar aún más sus movimientos".

Médicos Sin Fronteras calificó la nueva estructura de Samos de "pesadilla distópica". No fueron los únicos. "El sistema KENTYROS se enmarca en el uso de tecnologías altamente intrusivas para proteger la privacidad, los datos personales y otros derechos, como algoritmos de análisis de

comportamiento y movimiento, drones y cámaras de vigilancia de circuito cerrado. Existe una seria posibilidad de que la instalación de los sistemas YPERION y KENTYROS pueda violar la legislación de la Unión Europea sobre el tratamiento de datos personales y las disposiciones de la Ley 4624/2019", señala la ONG Homo Digitalis. La Asociación Helénica de Derechos Humanos, HIAS Grecia, Homo Digitalis y un profesor de la Universidad Queen Mary de Londres, el Dr. Niovi Vavoula, presentaron el 18 de febrero de 2022 una solicitud ante la Autoridad de Protección de Datos griega (DPA) para el ejercicio de las facultades de investigación y la emisión de un dictamen sobre el suministro y la instalación de los sistemas. El miércoles 2 de marzo de 2022, la Autoridad inició una investigación del Departamento de Inmigración y Asilo en relación con los dos sistemas en cuestión.

El fetiche de la automatización

"El problema es que las autoridades, y los políticos, están empezando a percibir los análisis de datos avanzados como factores de algún tipo de conocimiento objetivo e imparcial sobre cuestiones de seguridad, porque tienen esta aura de precisión matemática. Pero la inteligencia artificial y el aprendizaje automático pueden ser en realidad muy precisos a la hora de reproducir y magnificar los sesgos del pasado. Debemos recordar que los datos de mala calidad sólo conducirán a decisiones automatizadas y sesgadas", afirma el investigador George Glouftios.

---

[1] Se han resumido; las descripciones completas están disponibles en el documento del acuerdo de subvención.

[2] Al principio del proyecto, estos eran: (1) el consentimiento informado; (2) la comercialización de los datos; y (3) las cuestiones de seguridad/ciberseguridad.

[3] Disponible en: http://guidelines.panelfit.eu/understanding-data-protection/

[4] Publicación en Facebook: 159 personas alcanzadas; Primer tuit: 811 impresiones, 2 likes, 1 retweet; Segundo tweet: 1.841 impresiones, 6 likes, 7 retweets; Boletín de ECSA, julio de 2020: 438 aperturas (21,9% de suscriptores); Lista de correo de ECSA de más de 600 personas y organizaciones.

[5] La guía PANELFIT sobre investigación e innovación responsables ofrece más información para este grupo.

[6] Art. 21 de la Directiva 2013/33/UE (Directiva sobre las condiciones de acogida refundida). Véase: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/vulnerable-person_en

[7] Aunque esta guía se centra en Europa, muchos de los tipos de vulnerabilidad se dan en otros lugares. Al mismo tiempo, hay otras causas y tipos de vulnerabilidad que se encuentran fuera de Europa.

[8] Por ejemplo, los "refugiados" son un grupo vulnerable, pero "ser pobre" y "no tener hogar" son una descripción del estado de alguien en un momento dado y en un contexto determinado.

[9] Son las siglas de lesbiana, gay, bisexual, transexual, queer, intersexual y asexual.

[10] Véase: www.theguardian.com/world/2020/may/19/hungary-votes-to-end-legal-recognition-of-trans-people

[11] Los sami son el único pueblo europeo que figura en la lista de pueblos indígenas de la ONU.

[12] Véase: www.iwgia.org/en/sapmi.html

[13] Existen herramientas gratuitas en línea que realizan análisis de epilepsia fotosensible; véase, por ejemplo, www.w3.org/TR/WCAG20-TECHS/G15.html; el sitio web de Mozilla también tiene una sección sobre soluciones de accesibilidad para desarrolladores: https://developer.mozilla.org/en-US/docs/Web/Accessibility/Seizure_disorders