El ojo te ve ¿Hacia un totalitarismo digital?

Por: María de Menos Lobos, Ekintza Zuzena. 03/05/2025

Unión Europea-1, Privacidad-0

El pasado 8 de noviembre de 2023 el Parlamento Europeo, el Consejo de la UE y la Comisión aprobaban el borrador del Reglamento de Identidad Digital Europea (eIDAS2)[2], una *app* de identificación que estará reconocida por el conjunto de Estados de la UE. Esta contendrá los datos personales de cada ciudadano: carnet de identidad, pasaporte, carnet de conducir, títulos académicos, datos bancarios, historial médico, etc. El sistema se nos vende como un gran avance, pues sólo con un teléfono móvil, podremos hacer todo tipo de trámites administrativos o privados en cualquiera de los países miembros.

Sin embargo, la filtración del documento final ha disparado las alarmas entre las asociaciones de defensa de la ciberseguridad: el reglamento permite que los Estados puedan imponer a los navegadores autoridades de certificación, aunque estas no cumplan los estándares de seguridad. Además de introducir una falla muy peligrosa en internet, esto proporciona una herramienta sin precedentes para la cibervigilancia. Basta con que un Estado designe una autoridad de certificación que lo autorice, para que pueda acceder al tráfico web cifrado de toda la ciudadanía de la UE. La Identidad Digital, además, centraliza convenientemente los datos de cada individuo, de manera que, cruzándolos, será muy sencillo reconstruir su vida entera.

Pese a su potencial peligro, esta no es la peor noticia que ha recibido nuestra privacidad últimamente. El 9 de febrero, el Parlamento Europeo aprobaba por amplísima mayoría el reglamento marco Prüm II[3], de obligado cumplimiento para todos los Estados de la UE. Este actualiza y amplía diversas normativas sobre el intercambio de datos policiales. Además de compartir los perfiles de ADN, impresiones dactilares y datos de matriculación de vehículos, Prüm II incluirá las imágenes faciales, impulsando la tecnología de reconocimiento facial entre los países de la UE que eran reacios a incorporarla. También crea un sistema unificado de búsqueda entre las bases de datos de antecedentes policiales (EPRIS), similar al que ya existía para los antecedentes penales (ECRIS) e interconectado con este. Para tener antecedentes policiales, no es necesaria una condena penal. Basta con

que la persona haya sido detenida, vigilada, identificada, o considerada «sospechosa» por la policía… así que EPRIS puede parecerse bastante a una lista negra a nivel europeo. Además, el intercambio de datos será obligatorio y el sistema de búsqueda estará automatizado, por lo que un país no podrá poner filtros, por ejemplo de derechos humanos, antes de dar acceso a sus datos.

Lo más preocupante es que la búsqueda automatizada en estas enormes bases de datos ya no estará limitada, como ocurría con el ECRIS, a las investigaciones penales y otras cuestiones como la desaparición de personas o la identificación de restos humanos. Ahora, también se vuelve prospectiva, puesto que estará encaminada a la «prevención de delitos». La policía podría utilizar este sistema para identificar a quienes grabe por la calle como participantes en una manifestación, o para reconstruir la red de conocidos y amigos de una persona a partir de las fotos de sus redes sociales… Bajo el Prüm II, todos somos sospechosos, y nuestra presunción de inocencia se diluye.
Podrá decirse que esto no es nada nuevo, y que la principal función de la policía siempre ha sido el mantenimiento del «orden», no la investigación de delitos. Y esta es una tarea preventiva, de vigilancia de la población. Debajo de cualquier democracia liberal hay un Estado policial que trabaja para mantener el statu quo.

Pero aunque en este sentido, estos reglamentos no sean novedosos, sí que son exponentes de una tendencia: la apuesta por las nuevas tecnologías y la inteligencia artificial, para lograr un Estado de hipervigilancia. Un «super-Estado policial», en el que idealmente sea posible saber quién está dónde y haciendo qué en todo momento, y lo que es peor: predecir qué va a hacer quién en cada momento. Teniendo en cuenta la potencialidad de muchas de las tecnologías de las que vamos a hablar aquí, nos encontramos ante un horizonte bastante distópico y orwelliano…

Por supuesto, las herramientas tecnológicas para el espionaje masivo de la población no comienzan hoy su andadura. Y aunque no dejan de crecer, ya están muy avanzadas…

Echelon, el ojo del imperio

Es el caso de Echelon, el mayor sistema mundial de espionaje de las comunicaciones conocido, que depende de la NSA o Agencia Nacional de Seguridad de EEUU.[4]
Echelon se crea durante la guerra fría con la firma del tratado UKUSA entre EEUU,

Reino Unido, Australia, Nueva Zelanda y Canadá. Aunque las primeras filtraciones sobre su existencia datan de los años 70, y en 2001 un comité de investigación del Parlamento Europeo concluyó que Echelon estaba espiando en diversos países de la UE, su existencia se hace más conocida en 2013, cuando el ex-agente de la CIA y la NSA Edward Snowden, filtra cantidades enormes de información clasificada a la prensa.

Gracias a Snowden, sabemos que Echelon es una red que intercepta las comunicaciones de voz, texto, imágenes y vídeo que se transmiten por radio, fax, satélite, microondas, fibra óptica y teléfono en el mundo entero. También recoge los metadatos relacionados con estas comunicaciones, como la hora, el lugar, la periodicidad, la dirección IP del ordenador o la tarjeta del teléfono. Y puede, entre otras muchas cosas, monitorizar el uso de diversas redes sociales en tiempo real, y recoger datos de las tarjetas de crédito y transacciones bancarias.

La capacidad de esta red es inmensa, centenares de miles de personas trabajan para ella, e incluso posee satélites propios, lo que le permite interceptar más de 3.000 millones de comunicaciones al día. También recibe ayuda: EEUU ha firmado tratados bilaterales de inteligencia para ayudar a otros gobiernos a espiar a su propia población, a cambio de que compartan la información obtenida. Entre estos, se encuentran Alemania, Francia, Italia, Países Bajos, Suiza, Suecia, Finlandia, Noruega, y por supuesto, España. Por otro lado, tiene acceso a los contenidos e historiales completos de nueve grandes empresas de servicios de internet, entre ellas Google, Facebook, Apple, Microsoft, Yahoo y Dropbox. Empresas de telecomunicaciones, como Vodafone, también colaboran con Echelon mediante la cesión masiva de datos de su clientela.

La información que recoge es en su mayor parte aleatoria, aunque también puede centrarse en un individuo. Por ejemplo, en 2015, se destapó que había espiado durante una década a la canciller Angela Merkel y otros miembros del Gobierno alemán. Los datos van a parar a unos superordenadores donde se procesan mediante diversos programas, que extraen información de todo tipo: desde un perfil de usuario concreto, hasta patrones generales de comportamiento de la población.

SITEL, nuestro Echelon local

Hemos mencionado que el Estado español colabora con Echelon cediendo datos a la NSA. Para ello, cuenta con su Echelon particular, un software espía llamado

Sistema Integrado de Interceptación Telefónica, o SITEL. SITEL fue encargado por el Ministerio del Interior del Gobierno de Aznar en 2001, y funciona desde 2004. Al igual que su hermano mayor, puede interceptar cualquier tipo de comunicación telefónica o telemática y sus metadatos. También utilizar los teléfonos móviles como micrófonos ambientales, que graban todo lo que tienen a su alrededor desde el momento en el que suena el tono, aunque no se descuelgue. Los datos captados por SITEL se almacenan en centros de monitoreo de la Policía Nacional, la Guardia Civil y el CNI, donde se seleccionan, analizan y archivan, ya sea de modo artesanal, ya utilizando programas de inteligencia artificial.

Si el Estado de hipervigilancia es un desarrollo del Estado policial, no es de extrañar que comparta muchos rasgos con el hacer cotidiano de la policía. Uno de ellos es la relación ambigua con la legalidad. El Estado policial tiene la capacidad de hacerse trampas al solitario, bien ocultándose tras la ley de secretos oficiales «por motivos de seguridad nacional», bien legalizando a posteriori lo que va necesitando, utilizando trucos y atajos o directamente ignorando la normativa… Porque ¿quién vigila al vigilante?

SITEL constituye un buen ejemplo: los primeros años, su existencia no se conocía y funcionaba sin marco legal. Más tarde, se le dota de un reglamento, que tampoco es conforme a derecho, puesto que al afectar a derechos fundamentales, debería regularse por ley orgánica. Once años después, en 2015, se introduce en una ley orgánica, mediante una reforma del artículo 588 de la LECRIM. Este parece bastante garantista: establece que sólo puede activarse SITEL de forma excepcional cuando no exista otro procedimiento, con una orden judicial, y dentro de una investigación sobre unos delitos específicos, prohibiendo el espionaje aleatorio o con fines preventivos.

Sin embargo, esta regulación contiene muchas trampas. Llama la atención que entre los delitos enumerados encontremos los *«cometidos por medios informáticos o de cualquier otra tecnología de la información y la comunicación»*. Esto es tautológico: SITEL podrá espiar todos los delitos que sea capaz de espiar, puesto que se trata de un sistema para pinchar este tipo de tecnologías. Otros delitos «espiables» son los de terrorismo, verdadero comodín para la represión: desde la reforma del 2015, se puede entrar en esta categoría sin pertenecer a un grupo armado, ni a un grupo organizado, ni cometer ninguna acción violenta contra las personas, ni provocar daños materiales, ni planear hacerlo siquiera. Ya hemos visto cómo en su memoria, la Fiscalía de la Audiencia Nacional clasifica año tras año como «amenazas

terroristas» a colectivos anarquistas, antifascistas, ecologistas y nacionalistas de izquierdas.

La regulación de SITEL sí que contiene una línea roja importante: prohíbe el espionaje de vigilancia, prospectivo. Sin embargo, no existe ninguna garantía de que esta norma se cumpla, pues no hay supervisión externa: los datos llegan a los centros de monitoreo del CNI, y sólo posteriormente son enviados (o no) a los juzgados. De hecho, la Asociación de Internautas denuncia que el mercadeo de datos y grabaciones extraídos con SITEL, filtrándolos a medios de comunicación a cambio de dinero, es constante. Por otro lado, el pinchado «legal» de comunicaciones está totalmente fuera del control, y se utiliza de manera fraudulenta por la policía: cuando esta solicita una orden para investigar a una persona dentro de un procedimiento penal, añade otros nombres que no tienen ninguna relación con la causa. Si la instrucción del procedimiento termina, los incluye en otra diferente, y así los mantiene bajo vigilancia. Se calcula que hay cerca de un millón de líneas pinchadas al año «legalmente» en el Estado español, lo cual es imposible de supervisar, pues supone una media de 597 intervenciones telefónicas al día por juez. Este número no guarda proporción ni con el de delitos investigados ni con el de condenas, y nos acerca mucho al escenario de la vigilancia masiva.

Además, la Policía Judicial y el Ministerio Fiscal también pueden, según la LECRIM, pedir metadatos sin orden judicial a las empresas de comunicaciones directamente, siempre que sea dentro de una investigación criminal, y estas estarán obligadas a proporcionarlos. En algunos casos, como la petición de la dirección IP de un ordenador o el código PIN de un teléfono, los agentes ordinarios también podrán hacerlo.

Un espía israelí luchando por la unidad de España

Aunque SITEL es el sistema de información mayor, o más conocido, que depende del Estado español, existen otros, tales como el sistema SIGO de la Guardia Civil, el proyecto OSEMINTI, del Ministerio de Defensa… y por supuesto, Pegasus. Este sistema de espionaje fue desarrollado por la empresa Israelí NSO Group, para su venta exclusiva a los gobiernos bajo la supervisión del Ministerio de Defensa de Israel. Opera como un virus que se introduce en el teléfono móvil aprovechando las vulnerabilidades de seguridad. Desde el momento en que lo infecta, puede acceder a todo el contenido del dispositivo, su localización, las comunicaciones que se llevan a cabo con él, o activar la cámara o el micro para espiar su entorno. Pegasus es una

tecnología muy costosa -cada licencia adquirida sirve para un sólo teléfono- pero cuya presencia es muy difícil de detectar, incluso en un análisis informático forense. El escándalo internacional sobre el uso masivo de este software espía estalla en 2021, gracias a las investigaciones de la red de periodistas contra la censura y por la libertad de prensa Forbidden Stories, Citizen Lab, un laboratorio de investigación sobre tecnología de la información y derechos humanos de la Universidad de Toronto, y Amnistía Internacional. Estas revelaron que al menos 50.000 teléfonos de más de cincuenta países se habían infectado con Pegasus.[5]

De nuevo, uno de estos países es España, donde el CNI lo compró ilegalmente con fondos reservados por seis millones de euros en 2014. Las primeras sospechas sobre el uso de este software por parte del Gobierno datan de 2020, cuando una investigación conjunta de *El País* y *The Guardian* revela que se utilizó entre abril y mayo de 2019 para espiar a Roger Torrent, entonces presidente del Parlament, Ernest Maragall, Anna Gabriel y otros políticos catalanes. Sin embargo, el Gobierno no admitió haber utilizado el programa espía, y la querella presentada por Torrent y Maragall contra el exdirector del Centro Nacional de Inteligencia Félix Roldán y la empresa israelí NSO Group, se archivó en 2022.

No obstante, en ese momento ya se había publicado un informe de Citizen Lab[6] que demostraba que Pegasus y en menor medida Candiru, otro software espía israelí, se había utilizado para espiar a 65 políticos y activistas relacionados con el independentismo catalán, desde 2017 hasta al menos 2020. Esto fue corroborado un año después por una comisión de investigación del Parlamento Europeo[7]. La misma directora del CNI, Paz Esteban, llegó a admitir que se había espiado con autorización judicial a 18 personas, lo cual suscita más dudas de las que resuelve sobre las 47 restantes… Para añadir confusión, poco después de conocerse estos datos, se revela que los teléfonos del presidente Pedro Sánchez y otros miembros de su Gobierno, también habían sido infectados.

Desde entonces, no han dejado de surgir escándalos sobre el espionaje a personalidades políticas, del mundo del periodismo, de la abogacía o del activismo, vinculadas con el independentismo catalán[8]. Además de las diversas noticias acerca de seguimientos, balizas en vehículos e infiltraciones policiales, en octubre de 2022 la Directa hace público que 38 personas relacionadas con los CDRs han sido espiadas mediante SITEL, y otro software similar a Pegasus. En 2023, se revela que la Audiencia Nacional autorizó el espionaje por la Guardia Civil de una cuarentena de personas, también utilizando un programa espía cuyo nombre y características

no han salido a la luz, dentro de la investigación por terrorismo contra Tsunami Democratic.

Por el momento, la única consecuencia del caso Pegasus ha sido la destitución de Paz Esteban, aunque se ha aprobado una comisión de investigación en el Congreso. Las personas afectadas han interpuesto 20 querellas contra el CNI, su ex-directora, y NSO Group. De estas, la única que está avanzando es la de Pere Aragonés, espiado entre julio de 2018 y marzo de 2020, cuando era vicepresidente de la Generalitat.

Aunque durante ese tiempo el PSOE ya había llegado al ejecutivo, este ha tratado de distanciarse achacándole toda la responsabilidad al gobierno de Mariano Rajoy, como si el CNI hubiese actuado por su propia cuenta. Esta posibilidad es un tanto alarmante, pero desde luego no imposible. La opacidad del Estado policial, protegido por una ley de secretos oficiales aprobada durante la dictadura y financiado por millones de euros en fondos reservados, y la falta de mecanismos de investigación y rendición de cuentas independientes, le dan un poder y una discrecionalidad enormes. Ya hemos visto cómo se van sucediendo los escándalos que relacionan a policías, expolicías, militares y servicios secretos, con trabajos ilícitos en los que están implicados empresarios, banqueros, medios de comunicación, jueces, políticos, e incluso la casa real… Trabajos que unas veces forman parte de una guerra sucia del Gobierno, o de la oposición, y otras obedecen a negocios mafiosos privados, pero que en todo caso se producen con una impunidad notable y están al servicio de unas «élites» que proceden directamente del franquismo… es el Estado profundo, fruto de la continuidad con la dictadura.

No obstante, el PSOE no es precisamente un partido bisoño en cuestiones de guerra sucia, y varias de sus actuaciones en torno a Pegasus resultan bastante sospechosas: el hecho de que no haya desclasificado toda la información solicitada por el juez de instrucción, su primera negativa a abrir una comisión de investigación en el Congreso, la insistencia de la Fiscalía para que se cerrasen todas las querellas contra el CNI, y sobre todo, las declaraciones de la ministra de Defensa Margarita Robles, a favor del espionaje:

«¿Qué tiene que hacer un Estado, qué tiene que hacer un Gobierno, cuando alguien vulnera la constitución, cuando alguien declara la independencia, cuando alguien corta las vías públicas, realiza desórdenes públicos…?»[9]

La política «del enemigo»: una lógica de guerra

¿Qué tiene que hacer? La señora Robles da a entender que está justificado que «un Estado, un Gobierno», se salte sus propias normas y vulnere los derechos fundamentales de un grupo de personas elegidas por su forma de pensar, porque es un caso de «defensa propia». Se trata del discurso legitimador por excelencia del Estado policial y sus abusos: el de la política del enemigo o de excepción. Este marco introduce una lógica de guerra: los derechos y garantías democráticos son para la ciudadanía, pero no se aplican cuando hay que lidiar con «enemigos» internos. En este caso excepcional, todo esfuerzo para destruir la amenaza estará justificado, pues de ello dependerá la supervivencia de la sociedad.

Obviamente se trata de una falacia: las prácticas de excepción vacían la democracia desde dentro, hasta convertirla en la fachada hueca de algo bien distinto… y una vez que se introducen, tienden a normalizarse y dejar de ser excepcionales, porque ¿qué Estado va a limitarse a sí mismo si puede evitarlo? Obviamente, esto no es nada nuevo, pero sí que es una tendencia que se acelera cada vez más. Y conforme va avanzando, se va asimilando esta lógica bélica, del «conmigo o contra mí», que sustituye a la democracia y los derechos humanos como marco de referencia… no es de extrañar que la extrema derecha esté en ascenso en todo occidente, cuando ya ha ganado el «sentido común».

Esta política necesita crisis, situaciones excepcionales, para avanzar. En el Estado español, la «lucha contra el terrorismo» ha sido su vehículo por excelencia durante décadas. Hay que tener en cuenta que tras cuarenta años de dictadura fascista, tampoco partíamos de cero precisamente, vista la continuidad con las instituciones policiales, militares, judiciales, fiscales y de inteligencia del franquismo. Sin embargo, aunque quizá estemos más «adelantados» en este proceso, la degradación democrática en favor del Estado policial es común a todo occidente. El siglo XXI se inaugura bajo este signo, con «la guerra contra el terror» de George Bush.[10]

Por citar ejemplos recientes, con ocasión de la guerra de la OTAN contra Rusia en Ucrania, las autoridades europeas han censurado los medios rusos en todos los Estados miembros de la UE, un atentado a la libertad de información y de prensa sin precedentes. En cuanto a la epidemia de COVID-19, nos ha familiarizado con un sinfín de tecnología de vigilancia invasiva y con la idea de que esta servía para

protegernos. Un ejemplo muy notable, los drones: su adquisición y uso por las distintas administraciones aumentó exponencialmente durante la pandemia, y desde entonces hemos normalizado su presencia. Los drones son aparatos muy silenciosos y menudos, difíciles de localizar desde el suelo. Pueden grabar en tiempo real espacios públicos o privados, no llevan distintivos policiales reconocibles ni es posible saber cuándo tienen las cámaras activadas. Se trata de una tecnología capaz de incorporar cámaras muy potentes, y otros dispositivos como infrarrojos, sensores de movimiento, geolocalización y tecnología de reconocimiento facial. Y la policía ni siquiera necesita autorización judicial para su utilización. Suponen, por lo tanto, una amenaza bastante grande a nuestra privacidad. Sin embargo, se adoptaron durante la pandemia sin ningún debate público. ¿Por qué? Probablemente, por miedo a la enfermedad.

Securitarismo y miedo

Y es que el miedo es un elemento fundamental para las políticas de excepción: estas requieren que la población se sienta vulnerable. Que por miedo, cambie derechos y libertades, por seguridad. De nuevo, esto es una falacia, pues no hay nada más peligroso y temible que un Estado sin líneas rojas. Pero en todo caso, parece funcionar. Tanto es así que, cuando no hay un enemigo, se inventa, mediante campañas de terror amplificadas alegremente por los medios de comunicación.

Esta política «del enemigo» tiene además la gran ventaja de distraer la atención del origen estructural de los problemas y conflictos sociales. Estos se muestran como las acciones de individuos o grupos inadaptados, o directamente malvados, enemigos de la sociedad que es preciso reprimir. El Estado policial, única faceta de lo público que la agenda neoliberal no tiene previsto desmontar o privatizar, acude entonces al rescate. Bajo este prisma securitario, no hay transformación social, porque no existe ningún problema con causas sociales y políticas. Sólo hay gestión del orden dentro de un marco que no se cuestiona. Por supuesto, quienes sí que lo hacen son candidatos ideales para ser enemigos, como muestra la memoria de la Fiscalía de la Audiencia Nacional. Pero además, y esto es especialmente ruin, también son señalados y criminalizados los grupos sociales más vulnerables, que resultan así no sólo víctimas, sino también chivos expiatorios.[11]

La hipervigilancia forma parte de toda esta lógica. Si la Policía no se enfrenta a unas personas con derechos como la presunción de inocencia, que han infringido una ley

en concreto, sino a «enemigos de la sociedad», si no importa lo que han hecho sino cómo piensan, o a qué grupo social pertenecen, entonces tiene todo el sentido controlarlos a priori y vigilarlos continuamente. La acción policial se vuelve preventiva, proactiva. A las pruebas concretas les sustituyen las suposiciones, hipótesis y prejuicios del relato policial. Y en este proceso, toda la población termina siendo un objetivo sospechoso bajo su mirada.

Policía del futuro con prejuicios del pasado

Una mirada policial «cibernética», ampliada tecnológicamente. Un ejemplo, las cámaras de seguridad. Estas ya han invadido por completo el espacio público, siendo España el sexto país europeo con mayor número grabando en las calles.12 Y es muy posible que hagan algo más que grabar… Un proyecto del Ministerio del Interior financiado por la UE con casi diez millones de euros, ha desarrollado un ABIS (Sistema Automático de Identificación Biométrica), del que van a disponer la Policía Nacional y la Guardia Civil13, diseñado para ser interoperable con el resto de bases de datos europeas en el marco Prüm II. Este buscará de forma automatizada coincidencias en una base de datos biométricos de individuos condenados y sospechosos, donde hay huellas dactilares y de las manos, e imágenes faciales. Y aunque de momento, no está autorizado utilizarlo para identificar a personas en vivo, probablemente pronto cambie la ley para adecuarse al marco europeo… Por el momento, la policía puede utilizar esta tecnología sin supervisión de ningún tipo, para labores de *«protección y prevención frente a las amenazas contra la seguridad pública»*14.

De hecho, están proliferando en el Estado español cámaras de seguridad «inteligentes» que nos graban cuando pasamos por la calle, instaladas en nombre de la «lucha contra el crimen». El año pasado, el Ayuntamiento de Barcelona abrió una licitación para colocar 17 en el paseo de Gracia. Estos aparatos cuentan con un sistema de reconocimiento facial y biométrico incorporado, pueden grabar matrículas, distinguir sonidos, equipajes, formas de vestir, y alertar de cualquier comportamiento sospechoso15. ¿Y qué es un comportamiento sospechoso? ¿Quién lo decide? Aquí nos adentramos en las oscuras aguas de la creación automática de perfiles de riesgo…

Uno de los grandes peligros de este tipo de tecnología es que, bajo su aspecto aséptico y objetivo, reproduce los mismos sesgos y prejuicios de la sociedad que la ha creado. Las IAs fallan. Pero además, fallan de un modo discriminatorio, que hace

que los grupos vulnerables lo sean aun más. Un ejemplo es la tecnología Palantir-Gotham, un software de vigilancia con inteligencia artificial utilizado por las policías locales de grandes ciudades de EEUU como Los Angeles, Chicago o Nueva Orleans. Este es capaz de cruzar cantidades inmensas de datos sobre una persona, que extrae de archivos públicos de todo tipo, redes sociales, tiendas online, etc., para establecer su grado de peligrosidad. El sistema ha recibido multitud de denuncias, ya que su IA ha demostrado ser tan racista y clasista como el agente de policía medio… De nuevo, vemos cómo la hipervigilancia tecnológica reproduce todos los vicios del Estado policial. Para colmo, cada vez que se realiza una detención guiada por este sistema, la persona detenida pasa a engrosar las bases de datos de la IA, reforzando su sesgo. La política del enemigo se convierte en una profecía autocumplida, que el prestigio de lo tecnológico hace más difícil cuestionar.

Europa en guerra contra los inmigrantes… y contra todos los demás

Volviendo al ámbito europeo, si hay un tema clave para el desarrollo del Estado de hipervigilancia es el del control de fronteras. De nuevo, viene de la mano de una lógica de guerra. La inmigración no se entiende como un derecho de las personas, ni siquiera como una cuestión humanitaria: se trata de una amenaza, ante la cual se busca de manera obsesiva blindar el espacio Schengen. Prueba de ello es el aumento constante de financiación y competencias de la Agencia Europea de Fronteras y Costas, Frontex[16]. Está previsto que Frontex, que cuando nació en 2004 contaba con 50 empleados, comande para 2027 una guardia de 10.000 agentes de fronteras armados, que podrán actuar en la totalidad del espacio Schengen, sin el consentimiento del país en el que se encuentren. Su presupuesto tampoco ha dejado de crecer, y para 2027 alcanzará los 900 millones de euros al año.

Frontex tiene diversas funciones: cogestión de los *hotspots*[17], organización de los vuelos de deportación[18], creación de una red para la externalización de fronteras… pero su principal labor es de vigilancia. La fundación Por Causa ha denunciado que está apostando por la compra de drones y otros aparatos de control remoto, para patrullar las fronteras marítimas sin tener que rescatar a las personas que naufragan. Los drones están equipados con cámaras, cámaras térmicas y de visión nocturna, sensores de movimiento, un programa de reconocimiento de vehículos, intercepción de señales y comunicaciones, radar marítimo, etc. Este tipo de dispositivos también están presentes en muchos puntos de las fronteras terrestres, bordeadas además por kilómetros de muros. Toda la información que captan se comparte en tiempo real con los puestos de control de Frontex a través del sistema

Eurosur.[19]

Frontex también se ocupa de la vigilancia en las entradas habilitadas, como son, por ejemplo, los aeropuertos. En ellas se toman los datos biográficos y biométricos (huellas dactilares, reconocimiento facial, reconocimiento del iris, etc.), de las personas mayores de 6 años que quieren entrar en la UE, o que solicitan asilo o visado, sean admitidas o no. La información va a parar a diversas bases de datos interconectadas, que cuentan con sistemas de filtrado y creación de perfiles por inteligencia artificial: el SIS o sistema de información Schengen, de Europol, con descripciones de personas desaparecidas o en busca y captura. El VIS o sistema de información de visados, para realizar comprobaciones de identidad a quienes solicitan visados y permisos de residencia. Y el Eurodac, recientemente ampliado, con las huellas dactilares, imágenes faciales y otros datos de personas que han solicitado asilo o han tratado de entrar en la UE de forma irregular.

Además, hay dos nuevos sistemas en fase de desarrollo: El SES, o Sistema de Entrada y Salida, por el que fronteras automatizadas registran y almacenan los datos biográficos, biométricos y relativos a las entradas y salidas de quienes las atraviesan, y pueden calcular la duración de cada estancia y cuándo ha caducado. Y el SEIAV, o Sistema Europeo de Información y Autorización de Viajes, especialmente problemático, pues inspecciona a quien no necesita visado y determina de manera automática si constituye «un riesgo» y no puede viajar.

A toda esta inmensa cantidad de información, hay que añadirle, gracias al nuevo marco Prüm II, las bases de datos ECRIS y EPRIS, con las personas que tienen antecedentes penales y policiales, ya sean de la UE o de terceros países. Todas estas bases de datos estarán interconectadas en el sistema de búsqueda, para lo cual pasarán por un sistema central que tendrá acceso a toda la información, el «Registro Común de Datos de Identidad». Esto supone, en palabras de Ella Jakubowska, abogada de la organización EDRi[20], *«la infraestructura de vigilancia biométrica más grande que creo que jamás hayamos visto en el mundo»*. Se calcula que el Registro Común de Datos de Identidad ya acumula datos biométricos de más de 350 millones de personas, migrantes y no migrantes, a los que tienen acceso inmediato las agencias de migración y de control de fronteras, los cuerpos y fuerzas de seguridad y la Interpol. No nos cabe duda de que este número seguirá aumentando, hasta contener a la totalidad de habitantes de la UE, y que almacenará datos cada vez más minuciosos. Se trata de un triste ejemplo de cómo las políticas de excepción, creadas so pretexto de combatir un «enemigo», terminan

extendiéndose a toda la población…

Esta lógica expansiva, cuando hablamos de bases de datos y de inteligencia artificial, es además exponencial. Puede que un solo dato no signifique mucho, pero cuando de la vigilancia masiva se extraen y acumulan miles de millones de datos, y se tiene la capacidad de cruzarlos y compararlos entre sí, se obtiene muchísima información. La cual se puede utilizar, a su vez, para afinar las herramientas de vigilancia y de control social. Esto incluye, como en el caso del SEIAV, la seguridad predictiva y creación de perfiles de riesgo… y todo ocurre de una manera invisible, que se sustrae al debate público.

El gran negocio de la vigilancia

La política migratoria de la UE también ejemplifica el papel determinante de la industria en el ascenso securitario. Frontex tiene la capacidad de firmar contratos, y además, de obligar a los países miembros a adquirir tecnología, a través de las recomendaciones de sus informes de vulnerabilidad de fronteras, que son vinculantes. Es, pues, un cliente suculento para los lobbies de la industria militar, de seguridad y vigilancia, y también del análisis de big-data y la inteligencia artificial, a los que transfiere cientos de millones de dinero público. De hecho, tiene una relación fluida y regular con ellos, y actúa como facilitador e intermediario de sus intereses ante la UE. Las políticas migratorias europeas, además de producir miles de muertes atroces e innumerables sufrimientos, dan muchísimo dinero.

Pero esto va más allá, pues la agencia también tiene bastante protagonismo en la elección de los proyectos de I+D+I que serán financiados por la UE. No por casualidad, el anterior programa marco Horizonte 2020, dedicó 118 millones de euros al área de «Seguridad exterior y fronteriza». Frontex incluso colabora probando los nuevos inventos en las fronteras, utilizando a inmigrantes reales como involuntarios conejillos de Indias. Esta capacidad de decisión sobre qué se investiga implica tener influencia sobre el futuro, por lo que cabe preguntarse, ¿quién lo está modelando realmente? En palabras de la fundación Por Causa:

«Un Frontex impávido, sin mecanismos reales de transparencia o rendición de cuentas, deja sus puertas abiertas a una industria que endurece el blindaje fronterizo vendiendo soluciones cada vez más intrusivas, letales e irrespetuosas con los derechos humanos. No se trata de una relación inocua o estrictamente comercial sino de un verdadero rearme político e ideológico en pos de la militarización de las fronteras y la antimigración.»

Batidora 007

El ámbito de la vigilancia policial no es el único en el que espiarnos y robar nuestros datos es un floreciente negocio. Un síntoma del interés creciente que suscitan nuestras vidas son los escándalos sobre objetos cotidianos espía que se suceden desde hace unos años: los asistentes virtuales Alexa y Siri, Cayla, una muñeca con micrófono y conexión a *bluetooth*… El «internet de las cosas», de electrodomésticos *«smart»* conectados a internet, constituye un vehículo perfecto. A menudo consentimos inadvertidamente este espionaje al firmar un montón de letra pequeña, por ejemplo con los televisores LG, pero se han llegado a encontrar micrófonos ocultos de forma ilícita en lugares tan inesperados como los robots de cocina de Lidl. Otros instrumentos privilegiados para el robo de datos son las redes sociales y numerosas *apps*: en este caso, nosotros mismos colaboramos entregando voluntariamente cantidades ingentes de información sobre nuestra vida, condiciones físicas, hobbies, ideología, creencias, hábitos de consumo… de nuevo, cada uno de estos datos por sí solo, no vale nada. Pero ¿qué pasa cuando son miles de millones?

Aquí entra de nuevo en funcionamiento la minería de datos: estos se venden por paquetes a empresas que los procesan mediante algoritmos, para extraer perfiles sociales. Un conocimiento muy cotizado, ya que proporciona, por ejemplo, tipos de consumidor para enviar publicidad personalizada, orientación sobre qué nuevos productos introducir en el mercado, o incluso perfiles electorales para manipular la intención de voto… Es muy conocido el caso de Cambridge Analítica, que una investigación periodística sacó a la luz en 2018. Con el consentimiento de Facebook, esta empresa explotó la información personal de más de 87 millones de usuarios. Valiéndose de un engaño, accedía al perfil de una persona y de todos sus contactos en la red social. A partir de sus datos, creaba perfiles psicológicos e ideológicos que le permitían diseñar publicidad electoral encubierta y personalizada, mediante el envío de noticias (a veces falsas) y contenidos seleccionados, a través de las redes sociales. Según su propia página web, la empresa habría trabajado en

aproximadamente cien campañas electorales alrededor del mundo, incluyendo la de Donald Trump.

En realidad, en esta dinámica, más que «usuarios de servicios» somos la materia prima de una industria… es otra vuelta de tuerca de un sistema capitalista que necesita conquistar, colonizar y convertir en objeto de negocio y de lucro privado cada vez más espacios a todas las escalas: los parques y plazas de las ciudades, el código genético de las plantas, el vientre y la fertilidad de las mujeres, la salud, el agua, y nuestra privacidad. Es por ello que las tecnologías de espionaje que buscan extraer cada vez más datos, y las de inteligencia artificial y minería de datos que buscan convertirlos en información utilizable, son objeto de un inmenso esfuerzo de investigación pública y privada a nivel mundial, que produce constantes innovaciones. Y cuanto más avanza, más retroceden nuestros derechos.

Determinismo tecnológico: amor por lo nuevo

Cabe preguntarse por qué la sociedad colabora tan alegremente con este robo masivo de datos para su propia manipulación y control. Y aquí entra en funcionamiento un segundo discurso legitimador: el del progreso y el desarrollo tecnológico. Es ciertamente descorazonador que, a las puertas de un colapso climático y energético que puede llevarnos a la extinción, esta ideología decimonónica siga vigente. Sin embargo, si un electrodoméstico puede conectarse a internet, aunque esto sea del todo inútil y lo haga más caro, más difícil de reparar, y susceptible de espiarnos, se considerará mejor que uno que no lo hace. La innovación tecnológica es buena «per se». Es más, no sólo buena, sino también inevitable: como sociedad, no nos planteamos que el desarrollo tecnológico sea «opcional», que podamos reflexionar sobre su rumbo, sus consecuencias, o nuestras necesidades, y tomar decisiones. Ni mucho menos que tenga sesgos, que falle o que obedezca a intereses que pueden perjudicarnos…

El determinismo tecnológico también está presente en las políticas públicas, (no por casualidad tenemos un «Ministerio *para* la Transformación Digital») que asumen que «la digitalización» es un fin en sí mismo. En realidad, hoy por hoy este proceso es una forma encubierta de privatización, ya que supone que el Estado transfiera cantidades ingentes de dinero público y se vuelva crecientemente dependiente de empresas tecnológicas privadas. Además, saca del debate público y despolitiza cuestiones que no son sólo técnicas, quitándonos soberanía y obligándonos de facto, a comprar tecnología, también privada. Si finalmente se aprueba el

Reglamento de Identidad Digital Europea, ¿cuánto tiempo tardará en ser obligatorio llevar la identificación en el teléfono?21

Poli bueno, poli malo

Un efecto secundario es que la privacidad está dejando de ser un derecho. No sólo porque el espacio del que dispone se reduce cada día, tanto *de facto* como *de iure*, sino porque ya no se percibe como tal. Esto abre la puerta a su criminalización. Aunque parece una afirmación exagerada, el juez de la Audiencia Nacional, Javier Gómez Bermúdez, ya interpretó en 2014 como un indicio de terrorismo el tener un correo seguro de Riseup… lo cual le llevó a enviar a siete personas a prisión preventiva tras la Operación Pandora, vergonzoso montaje policial contra el «terrorismo anarquista», que finalmente fue archivado.22 Más recientemente, en Francia otros siete militantes de izquierda han sido condenados por terrorismo, en el llamado «Caso 8 de diciembre». Estas personas no habían participado en ninguna acción terrorista, ni planeaban hacerlo, ni pertenecían a ningún grupo armado… Eso sí, utilizaban aplicaciones cifradas como Signal para comunicarse, y se interesaban por la seguridad en la red, cosa que, para la Dirección General de la Seguridad Interior francesa, era un indicio de «comportamiento clandestino» y ha sido la principal «prueba» de la acusación.23

Un montaje policial ejemplarizante, para reprimir al activismo de izquierdas. Hasta aquí, ninguna novedad. Pero esta sentencia también está castigando la falta de fe en la tecnología. Como si el quedar fuera de ese credo te convirtiese directamente en alguien sospechoso, en enemigo de la sociedad. El buen ciudadano hace horas de cola para comprar el último *gadget* que grabará su intimidad y venderá sus datos. Porque el último *gadget* es «lo que todo el mundo quiere». Y si tú no lo quieres, ya se ocupa de ti el Estado policial.

El discurso securitario, de la guerra contra un enemigo, y el del progreso y el determinismo tecnológico, son dos caras de la misma moneda. Uno opera a través del miedo y la coacción; el otro, a través del deseo y la persuasión. Pero en ninguno de los dos somos sujetos políticos, ni hay lugar para la duda, el debate o la toma de decisiones colectiva. Y ambos legitiman el proceso por el que el flujo de datos que se extrae de la población es convertido en cantidades ingentes de dinero y en control social. Por las buenas, mediante la manipulación del comportamiento de las empresas especializadas en *microtargeting*, o por las malas, mediante el uso de herramientas cada vez más intrusivas del Estado policial. Así, mercado y vigilancia

avanzan juntos, y cada vez quedan menos espacios que puedan sustraerse a su colonización.

En palabras del colectivo Solenopsis:
«Hoy estamos enfrentando el inicio de una era de totalitarismo digital a través de una alianza capital-estado como un mismo ente complejo de vigilancia y control social.»[24]

Los Estados, vaciados progresivamente de cualquier función que no sea policial, garantizan el orden necesario para los negocios de unos conglomerados de empresas militares, de la comunicación, y de inteligencia artificial y minería de datos, que marcan el rumbo. Y ese rumbo es el de la guerra, interna y externa.

¿Salvados por el colapso?

Se trata, ciertamente, de un panorama muy oscuro. Y por desgracia la UE tiene dónde inspirarse, pues esta tendencia es global. China es, por el momento, el país que más ha desarrollado el uso de tecnologías para la vigilancia masiva: cuenta con un sistema central de vigilancia que combina las imágenes captadas por cámaras con reconocimiento facial, con la geolocalización por GPS de los teléfonos, las comunicaciones telemáticas y telefónicas, y el rastreo de datos de todo tipo por internet tales como viajes, transacciones bancarias, etc., de cada habitante. Toda la información es evaluada por una IA que concede una puntuación, el llamado «crédito social», conforme a la cual las personas podrán optar a más o menos servicios públicos, en un sistema de premio/castigo. La IA también hace una clasificación por perfiles de riesgo, y los dispositivos de vigilancia automatizados avisan a la policía a través de una app si alguién clasificado como sospechoso tiene un comportamiento inusual.[25]

Todo parece horriblemente eficaz, pero sin embargo, se nos plantea una duda: ¿puede este sistema crecer indefinidamente, en un mundo que es finito? Las nuevas tecnologías no son limpias. Su fabricación emite tanto CO2 como todo el tráfico aéreo mundial. La empresa Google consume tanta agua como una ciudad de 320.000 habitantes para refrigerar los servidores donde almacena los datos. Para compensar las emisiones de gases efecto invernadero de la producción de ordenadores, tabletas y *smartphones*, tendríamos que utilizar cada dispositivo entre 33 y 89 años. En las baterías se utilizan metales que ya empiezan a escasear, como el litio y el cobalto…

Si, como afirma la comunidad científica, nos encontramos ante las puertas de un colapso climático y energético, ¿qué proyección en el tiempo tiene este sistema de capitalismo de hipervigilancia? Parece que, cegado por la ilusión de su propia omnipotencia, ha olvidado que tiene los pies de barro, y que depende de un planeta que no puede sostenerlo. Es muy posible que estemos yendo hacia la extinción, y que la humanidad no tenga futuro. Pero si lo tiene, no es el Gran Hermano.

Post Data: la nueva Ley Europea de Inteligencia Artificial

El 13 de marzo, cuando este artículo ya estaba redactado, el Parlamento Europeo aprobó la Ley Europea de Inteligencia Artificial, que regula y también limita, algunos usos de la IA. Por supuesto, con la normativa recién aprobada no podemos hacer un análisis exhaustivo del texto, ni tampoco saber cómo se va a aplicar en el futuro. Pero ya contamos con algunas valoraciones que nos permiten, al menos, hacernos una idea general en lo que afecta al contenido de este artículo: las herramientas de espionaje masivo para el control social.

Esta ley clasifica los usos de la IA en distintos niveles de riesgo y prevé unas medidas de seguridad para cada uno de ellos. Los niveles son cuatro: el máximo, de prácticas que están prohibidas, alto riesgo, riesgo limitado, y riesgo mínimo o nulo.

Entre las prácticas que en principio están prohibidas, están la manipulación de las opiniones (como por ejemplo en el caso de Cambridge Analytica que comentamos), los sistemas de identificación de emociones en centros laborales y docentes, los sistemas de puntuación ciudadana (como el que ya se está utilizando en China), la evaluación de perfiles de riesgo de cometer un delito, aplicada de forma totalmente automatizada y a priori, los sistemas que extraen de forma masiva imágenes de

circuitos cerrados de televisión o de internet para crear bases de datos de reconocimiento facial, y algunos usos de la identificación biométrica, como la que busca «*inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona física*», y los dispositivos de identificación biométrica remota en tiempo real en lugares de acceso público.

Por otro lado, son considerados de alto riesgo otros sistemas de identificación biométrica remota en diferido, sistemas para el reconocimiento de emociones, sistemas para vigilar a los estudiantes o trabajadores en sus centros docentes o laborales, el uso policial o judicial de polígrafos, sistemas para la evaluación de pruebas durante una investigación judicial, sistemas de apoyo policial para valorar la probabilidad de que una persona cometa una infracción o reincida, y otros similares.

Parece que la práctica totalidad de los sistemas que nos preocupaban en este artículo están contenidos en esta regulación, y que por lo tanto todo lo que hemos escrito hasta ahora ha quedado obsoleto y ya no hay nada de qué preocuparse… De hecho, esta ha sido la versión que han dado los medios, un corta-pega de la nota de prensa del Parlamento Europeo: la UE, pionera mundial en regular el desarrollo de una IA centrada en el ser humano y respetuosa con los derechos de las personas. [26]

Sin embargo, ya se han hecho públicas diversas declaraciones de organizaciones de defensa de los derechos humanos, que cuestionan esta descripción, y denuncian que esta ley no es lo que parece:

Por un lado, todas las vulneraciones propias de la Europa fortaleza que denunciábamos en el artículo, siguen en pie. Según explica EDRi[27], mediante excepciones, la ley ha creado un marco legal paralelo para el control de fronteras, por el que sistemas que se prohíben o están sometidos a un mayor control, como los sistemas automatizados de análisis predictivo y evaluación de riesgos, o el reconocimiento de emociones para los detectores de mentiras, están permitidos en este contexto.

Además, las enormes bases de datos sobre migraciones, como Eurodac, ETIAS, o el Sistema de Información Schengen, no tendrán que aplicar la normativa hasta 2030.

Algo similar ocurre con el uso policial de la IA. Por ejemplo, los sistemas de reconocimiento biométrico en tiempo real en espacios públicos están prohibidos, excepto para uso policial, y en determinadas circunstancias… Dentro de estas, está la búsqueda de sospechosos de cometer una serie de delitos, descritos según el código penal de cada país, y castigados con un máximo de, como mínimo, cuatro años de prisión. Por supuesto, en este listado aparecen los delitos de terrorismo, que como ya hemos comentado, están definidos de una manera tan imprecisa en nuestro Código Penal que son idóneos para la persecución política…

Es cierto que, sin conocer todavía qué encaje va a tener esta ley con el marco Prüm II, parece que limita su enfoque prospectivo y de vigilancia, pues restringe el uso policial de esta tecnología a investigaciones concretas. El problema es que la introducción de estas excepciones a su prohibición implica que sí va a haber sistemas de reconocimiento facial en tiempo real en el espacio público, que obren en poder de la policía… ¿qué nos garantiza que no va a utilizarlos de forma ilícita? Esto es extensivo a otros sistemas calificados «de alto riesgo», como por ejemplo, los de identificación biométrica en diferido, los de evaluación predictiva sobre posibilidades de reincidencia, los detectores de mentiras, etc. El riesgo de abuso es enorme.

Máxime cuando en los campos de control de fronteras y policial, que se prestan especialmente a las vulneraciones de derechos humanos, esta normativa no endurece las condiciones, sino que las hace más laxas… por ejemplo, la ley obliga a las autoridades que utilizan sistemas de alto riesgo a registrarlos en una base de datos que es de consulta pública. Sin embargo, existe una exención para el uso policial y de control de fronteras, por lo que será imposible saber cuándo se están utilizando en este contexto, y consecuentemente, defenderse de posibles abusos. Otra garantía que deja de aplicarse, es el requisito de que dos personas físicas confirmen por separado la identificación biométrica hecha por la IA, antes de tomar una decisión. Si la decisión es, por ejemplo, llevarse a una persona detenida, o denegarle su visado, entonces ya no será obligatorio y serán las autoridades las que decidan si se aplica la doble comprobación humana o si es una precaución «desproporcionada».

Además de todas estas excepciones, existe un «comodín» que puede ser utilizado por cualquier Estado de la UE de la forma que quiera. Y es que los temas relativos a la defensa y la seguridad nacional quedan fuera de la regulación. Teniendo en cuenta que cada país puede decidir qué cuestiones son relativas a su seguridad

nacional, esto supone ya desde el principio una forma de escapar a la norma cuando sea preciso, y entrar directamente en las políticas de excepción.

No sólo los Estados tienen su «comodín», sino también las empresas desarrolladoras o proveedoras de las IAs… para que un sistema sea de alto riesgo, además de aparecer explícitamente en la ley, estas tienen que considerar que supone un riesgo significativo para los derechos humanos… ¿Por qué ninguna empresa se sometería a más controles, más gastos y más problemas, metiendo su producto o servicio voluntariamente en esta categoría?

Por otro lado, parece que está previsto que sean los Estados miembros quienes desarrollen su propia estructura de supervisión para garantizar el cumplimiento de la normativa. Conociendo el historial de impunidad del Estado español, y la clamorosa ausencia de mecanismos independientes de fiscalización y rendición de cuentas en todos los ámbitos donde puede vulnerar los derechos humanos, tenemos serias dudas de que esta estructura vaya ser algo más que decorativa.

Por último, la regulación no afecta a las exportaciones fuera de la UE, desentendiéndose de las violaciones de derechos humanos que puedan producirse en terceros países utilizando tecnología europea.

Esta ley todavía no se ha desarrollado. Tienen que crearse regulaciones en los diversos países miembros, y en general, está aun por ver cómo se llevará a la práctica. Por supuesto, este comentario es muy somero y puede que no le esté haciendo justicia, pero nuestra primera impresión es que la ley es más que nada una pantalla para tranquilizar a la población, y dar legitimidad al proceso de expansión conjunta del negocio de los datos y el control social. En palabras del asesor de Amnistía Internacional, Mher Hakobyan:

*«Resulta decepcionante que la UE y sus 27 Estados miembros hayan decidido dar prioridad al interés de la industria y de los organismos encargados de hacer cumplir la ley por encima de proteger a las personas y sus derechos humanos.»*28

1. Menos Lobos es un podcast antirrepresivo para las radios libres y comunitarias de todo el Estado. Puedes escucharnos aquí: www.menoslobos.net o ponerte en contacto con nosotras en menoslobos@riseup.net ??
2. G. Bejerano, Pablo. (19/11/2023). La UE tiene lista su identidad digital para todos los europeos. Y preocupa mucho a los expertos en ciberseguridad. *Xataka*

. https://www.xataka.com/seguridad/ue-tiene-lista-su-identidad-digital-para-todos-europeos-preocupa-mucho-a-expertos-ciberseguridad ??
3. EDRi. (6/02/2024). Automated data exchange in Prüm II: The EU's securitisation mindset keeps encroaching on our fundamental rights. https://edri.org/our-work/automated-data-exchange-in-prum-ii-eu-securitisation-mindset-encroaching-on-fundamental-rights/ ??
4. El grueso de la bibliografía utilizada para escribir este artículo, puede consultarse en: Menos Lobos. (19/05/2020) Espionaje Masivo y Coronavirus. https://www.menoslobos.net/2020/05/espionaje-masivo-y-coronavirus/ ??
5. En la web de Forbidden Stories puede leerse acerca de las diferentes investigaciones: https:// forbiddenstories.org/pegasus-project-articles/ ??
6. Scott-Railton J., Campo E., Marczak B., Razzak B.A., Anstis S., Böcü G., Solimano S.,Deibert R. (2022). CatalanGate: extensive mercenary spyware operation against catalans using Pegasus and Candiru. Citizen Lab, Informe N.155. Universidad de Toronto. https://catalonia.citizenlab.ca/es/ ??
7. Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware. (2022). Draft Report of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. Parlamento Europeo. https://www.europarl.europa.eu/doceo/document/PEGA-PR-738492_EN.pdf ??
8. Vigara S., y Bonilla T., Carbonell C. (2024). Vulneraciones de derechos en el Estado español 2022-2023. Defender a quien Defiende. https://defenderaquiendefiende.org/defender-a-quien-defiende-denuncia-mas-de-mil-vulneraciones-de-derechos-en-contexto-de-protesta-en-los-ultimos-dos-anos/ ??
9. Declaraciones del 28 de abril de 2022 en la sesión de control al Gobierno en el Congreso de los Diputados. ??
10. A día de hoy, sigue habiendo cuarenta prisioneros en Guantánamo. No tienen fecha de salida, ni cargos, ni han sido o van a ser juzgados ??
11. «La amenaza okupa» es un ejemplo paradigmático de cómo se desvía la atención de la especulación urbanística culpando a quienes la sufren, con una campaña mediática de terror y criminalización. ??
12. G. De Rivera, Laura. (23/07/2023). España es el sexto país europeo con más cámaras públicas de videovigilancia. Público. https://www.publico.es/ciencias/espana-sexto-pais-europeo-camaras-publicas-videovigilancia.html ??

13. https://fondoseuropeosparaseguridad.interior.gob.es/es/detalle/proyecto/SISTEMA-AUTOMATICO-DE-IDENTIFICACION-DACTILAR-SAID-ABIS/ ??
14. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. A.1. ??
15. Benvenuty, Luis. (08/04/2023). Barcelona instalará 17 cámaras inteligentes en el paseo de Gràcia. La Vanguardia. https://www.lavanguardia.com/local/barcelona/20230408/8881993/barcelona-instalara-17-camaras-inteligentes-paseo-gracia.html
    Los ayuntamientos y comunidades autónomas también están experimentando con las tecnologías de vigilancia. Al ser a una escala menor, suelen llamar menos la atención de los medios y suscitar menos polémica. Sin embargo, es un paso muy importante para la normalización y extensión de estas tecnologías. Otros ejemplos:
    Riu, Manel. (22/04/2022). Vigilancia masiva y tecnologías de control: cuatro ejemplos más allá del 'Catalangate'. *La Marea*. https://www.lamarea.com/2022/04/22/vigilancia-masiva-catalangate
    Zelaieta, Ahoztar. (22/02/2024). El armamento de videovigilancia que utiliza la Ertzaintza: 2.037 cámaras fijas, 1.435 bodycams y 13 drones. *El Salto Diario*. https://www.elsaltodiario.com/policia/armamento-videovigilancia-ertzaintza-2037-camaras-fijas-1435-bodycams-13-drones ??
16. Para escribir este apartado nos hemos basado en este informe, muy recomendable: Fundación Por Causa. (2021). Frontex, el guardián descontrolado. Autor. https://porcausa.org/wpcontent/up loads/2021/06/dos-Frontex-informe-porCausa.pdf ??
17. Se trata de campos de concentración donde se hacinan durante años los solicitantes de asilo ante la UE. Este es un informe sobre los *hotspots* en Italia: Amnistía Internacional. (2016). Hotspot Italy: How EU's flagship approach leads to violations of refugee and migrant rights. EUR 30/ 5004/2016. Autor. https://www.amnesty.org/en/documents/eur30/5004/2016/en/ ??
18. Sobre las vulneraciones de derechos humanos asociadas a estos vuelos: G. Berrio A., Calderó C., Cardona D., Daza F., Lo Coco D., Rocabert A. (2020). Vulneraciones de derechos humanos en las deportaciones. Iridia, Novact. https://iridia.cat/es/informe-vulneraciones-de-derechos-humanos-en-las-deportaciones-2/ ??
19. Aunque Ceuta y Melilla no están en el espacio Schengen, sus vallas también están equipadas con todo tipo de tecnología de vigilancia. De hecho, su sistema

de monitoreo ha servido de modelo para otras fronteras europeas: Amnistía Internacional. (2015). Miedo y Vallas. Los planteamientos de Europa para contener a las personas refugiadas. EUR 03/2544/2015. Autor. https://www.amnesty.org/en/documents/eur03/2544/2015/en/ ??

20. Se trata de una plataforma de asociaciones, académicos y expertos en ciberseguridad de toda Europa que trabaja para defender los derechos digitales y denunciar abusos de Estados y corporaciones. ??
21. Esta obligatoriedad de facto de la tecnología, está causando además graves problemas de discriminación entre la población, en especial para las personas de edad avanzada. ??
22. *Todo Por Hacer*. (02/2015). Efecto Pandora: represión contra las ideas. https: //www.todoporhacer.org/wp-content/uploads/2015/01/febreroWEB.pdf ??
23. Diario Octubre. (23/07/2023). La policía francesa considera el cifrado de las comunicaciones como 'terrorismo'. Diario Octubre. https://diario-octubre.com/2023/07/23/la-policia-francesa-considera-el-cifrado-de-las-comunicaciones-como-terrorismo/
    Sweeny, Nadia. (22/12/2023). «Affaire du 8 décembre»: l'inquiétante condamnation de militants comme terroristes. Politis. https://www.politis.fr/articles/2023/12/affaire-du-8-decembre-linquietante-condamnation-de-militants-comme-terroristes/ ??
24. Grupo Solenopsis. (2021). Vigilancia Masiva, Tecnocapitalismo y Estado policial. https://www.federacionanarquista.net/grupo-solenopsis-vigilancia-masiva-tecnocapitalismo-y-estado-policial-analisis-critico-y-estrategias-de-autodefensa-digital/ ??
25. El estudio del grupo Solenopsis antes citado analiza el sistema de vigilancia chino. ??
26. Ver, por ejemplo, Lacort, Javier. (13/03/ 2024). El Parlamento Europeo aprueba la Ley de IA: manipulación y vigilancia masiva quedan prohibidas por un texto pionero a nivel mundial. Xataka. https://www.xataka.com/legislacion-y-derechos/parlamento-europeo-aprueba-ley-ia-manipulacion-vigilancia-masiva-quedan-prohibidas-texto-pionero-a-nivel-mundial ??
27. EDRi, (13/03/2024). #ProtectNotSurveil: The EU AI Act fails migrants and people on the move. https://edri.org/our-work/protect-not-surveil-eu-ai-act-fails-migrants-people-on-the-move/ ??
28. Amnistía Internacional, (13/03/2024), UE: La legislación sobre inteligencia artificial no impide la proliferación de tecnologías abusivas, https://www. amnesty.org/es/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/

??

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Redes libertarias

Fecha de creación
2025/05/03