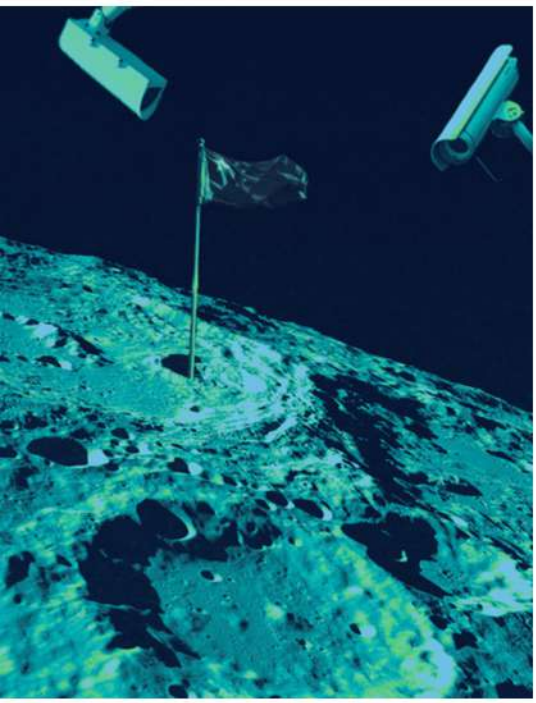
fundaciónHermes
derechos de ciudadanía digital

Geolocalización

Hoy, geolocalizados. Mañana, fichados de pies a cabeza

Se llama Skynet, sí, igual que la inteligencia artificial que lidera al ejército de las máquinas contra la humanidad en la saga de películas Terminator, pero de ficción no tiene nada. Es el nombre del gigantesco e inquietante sistema de vigilancia personal del Gobierno chino, capaz de analizar los rasgos de los **más de 1.300 millones de habitantes del país asiático** en apenas un segundo con una precisión del 99,8 %. Reconocer al resto de los 6.000 millones que viven fuera de China le tomaría apenas dos segundos. Es decir, que a Skynet no se le escapa nadie.

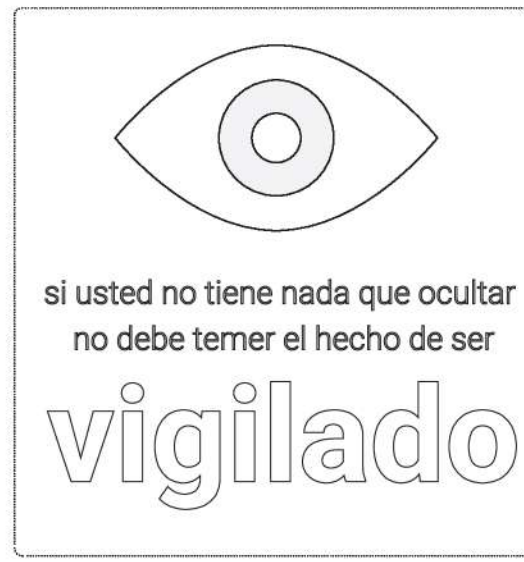
Lanzado a escala nacional en 2005, el programa de vigilancia es capaz de operar sin importar el ángulo de visión ni las condiciones de luminosidad.



Su esquema se basa en **una red que controla alrededor de 600 millones de cámaras en todo el país**. Eso equivale casi a una cámara por cada dos ciudadanos.

Aunque las autoridades utilizan el sistema principalmente para tareas de vigilancia comunes –como detectar infracciones, encontrar a criminales en busca y captura, personas desaparecidas y evitar crímenes– también pueden observar a disidentes políticos y evitar acciones contrarias al Gobierno. Este mismo sistema es el que China utilizará para vigilar su futura base espacial en la Luna, un recinto del tamaño de Disneylandia previsto para dentro de unos cinco años.

Pero volviendo a la Tierra, está claro que los sistemas Gran Hermano se están extendiendo por el mundo bajo la justificación de la seguridad ciudadana y potenciados por la inteligencia artificial. Desde el omnipresente **Skynet**, pasando por los sistemas de reconocimiento facial –ya empleados por muchos cuerpos policiales–, hasta la **geolocalización por parte de empresas y autoridades como la Agencia Tributaria**, la vigilancia sobre quiénes somos y dónde estamos en cada momento puede, como pasa con toda tecnología sin regulación, violar los derechos de intimidad y hasta de inocencia de las personas. "A veces se percibe que la vigilancia es incluso buena para el conjunto de la sociedad. Ello se debe a otros fines que son presentados como positivos, sobre todo en las dictaduras", analiza **José Luis Piñar, abogado y consultor experto en Derecho Administrativo y protección de datos**. "Se trata del famoso planteamiento autoritario: si usted no tiene nada que ocultar no debe temer el hecho de ser vigilado", concluye.



Piñar, también titular de la cátedra de Google sobre privacidad en la Universidad San Pablo CEU, destaca que un ataque a la propiedad o a la integridad física "se manifiesta físicamente y de inmediato"; a diferencia de un ataque a la privacidad, a la dignidad o al libre desarrollo de la personalidad –derechos digitales por los que aboga la Fundación Hermés– en los que la víctima no es consciente serlo.

La crisis sanitaria a raíz de la COVID supuso un punto de inflexión en el uso, por parte de los estados, de herramientas de geolocalización para controlar la pandemia. En China esto se convirtió en una obsesión y dio paso a la creación de diversos proyectos –además del de Skynet–, como Sharp Eyes, Golden Shield, Safe Cites y Police Clouds, entre otros.

Excepcional, necesario, normal

"La implantación de **técnicas de geolocalización o de videovigilancia** suele proponerse inicialmente como algo excepcional debido a situaciones extraordinarias", avisa Piñar. "A continuación se considera que el uso de esas tecnologías es necesario, y por último se asume que no son ni extraordinarias ni solo necesarias, sino normales en una sociedad compleja como la actual". Es decir, que lo que inicialmente es extraordinario pasa a ser necesario, para terminar siendo normal. No hay más que pensar en el caso de los controles y la creciente seguridad en los aeropuertos.

No estos sistemas exactos, pero sí sus objetivos, han sido exportados a todos los países del mundo con medios tecnológicos suficientes. Los programas de vigilancia implantados, aunque legales, no dejan de ser una amenaza latente para derechos fundamentales como la protección de datos y la privacidad.

Tasa Google

Ley del Impuesto sobre Determinados Servicios Digitales

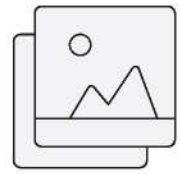
Por ejemplo, la utilización de la **geolocalización** por parte de la Agencia Tributaria en España **para perseguir el fraude fiscal** está respaldada por la Ley del Impuesto sobre Determinados Servicios Digitales (conocida como tasa Google). Esta ley fue aprobada en octubre de 2020 para determinar los impuestos que deben pagar las multinacionales tecnológicas, en función de los servicios que prestan en el país. La normativa se basa en la premisa de que conocer la localización exacta de las actividades digitales es imprescindible para calcular correctamente los impuestos adeudados.

> La geolocalización es empleada por la Agencia Tributaria en España para perseguir el fraude

"Cuando hablamos de geolocalización debemos ser conscientes de que estamos sometidos a una vigilancia constante. Una vigilancia que es posible gracias a unas tecnologías cada vez más sofisticadas, avanzadas y económicas que están generando lo que podemos denominar una suerte de panóptico digital. Una situación en la que –sabiendo que estamos vigilados– no identificamos al vigilante ni sabemos dónde se encuentra", reflexiona Piñar. "No debemos olvidar", añade, "que esa vigilancia pasa desapercibida. De modo que, al no ser conscientes de que nuestros derechos son violados (especialmente la privacidad), no somos capaces de dar la importancia que tiene al hecho de estar constantemente controlados".

Aunque la ley tiene como objetivo la persecución de un delito y eso es legítimo, las acciones al amparo de esta regulación pueden ser excesivas, por lo que muchas voces se han alzado en favor de establecer límites más estrictos sobre **cómo y cuándo se puede utilizar la geolocalización**. Entre las medidas propuestas por diferentes expertos del ámbito legal, se sugiere que se definan de forma muy precisa y sin lagunas los contextos, los límites temporales y el ámbito geográfico de aplicación. Además, se pide que se establezcan organismos de supervisión independientes para impedir el uso abusivo.

El caso Clearview

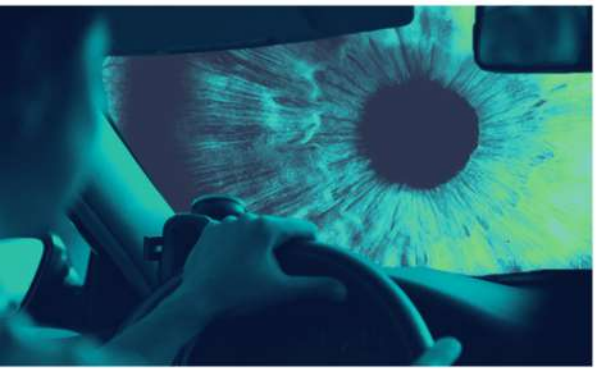


+30.000

millones de imágenes sin consentimiento

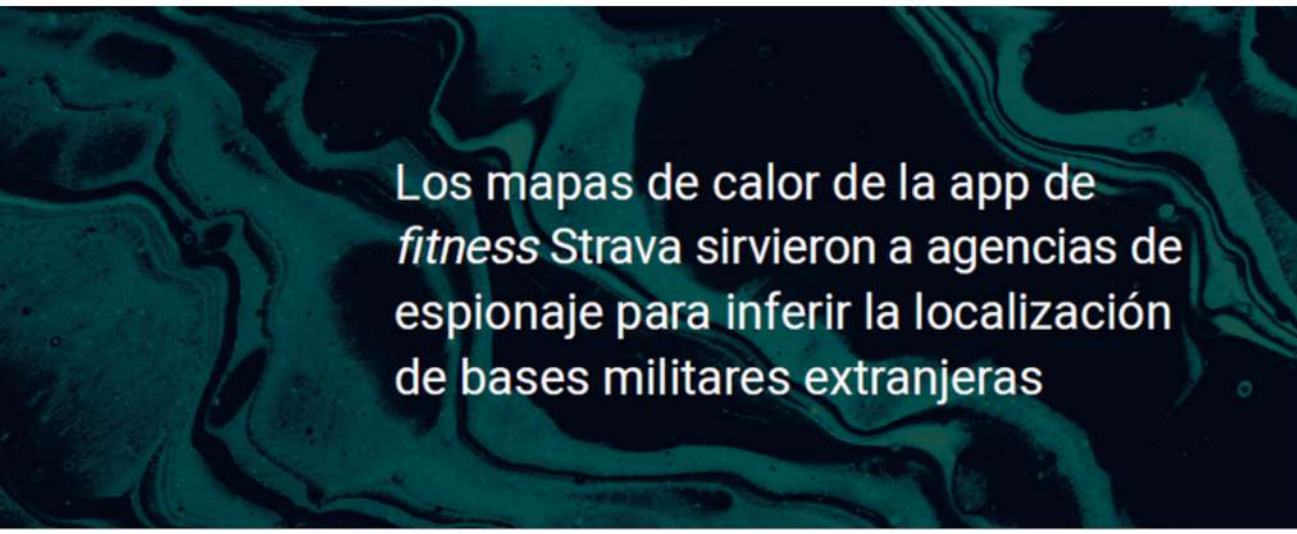
El debate sobre las prácticas legales de vigilancia, en todas sus formas, debería involucrar a legisladores, expertos en privacidad, defensores de los derechos digitales y a la sociedad en general; no son pocos los casos en los que se han visto comprometidas indebidamente la privacidad y la libertad de los individuos.

Especialmente sonado, entre esta clase de escándalos, fue el de caso **Clearview AI**, una empresa que desarrolló un sistema de reconocimiento facial utilizando, sin el consentimiento de los usuarios, imágenes y datos de redes sociales. La empresa llegó a extraer **más de 30.000 millones de imágenes de suscriptores de Facebook** y otras plataformas, que fueron empleadas por departamentos de policía de Estados Unidos y otros países. Y aunque el caso estuvo protagonizado por el reconocimiento facial, la compañía también tenía acceso a datos de geolocalización, lo que permitió rastrear a personas sin su conocimiento.



El caso Clearview ha sido el más reciente pero no el único, lo que demuestra el peligro que representan estas tecnologías cuando no tienen control. Ya en 2014 se conoció que una función interna de Uber –llamada "god view"– permitía a sus empleados **ver la ubicación en tiempo real de los conductores y pasajeros sin su consentimiento**.

Unos años más tarde saltó el caso Strava, una aplicación de fitness que publicaba mapas de calor globales mostrando los recorridos de sus miembros. Aunque estos mapas no revelaban directamente la identidad de estos, más de una agencia de espionaje infirió a través de esos movimientos la ubicación de bases militares secretas y los movimientos de personal militar en países conflictivos. Incluso Snapchat ha sido demandada por su función de Map Snap, que permitía a los usuarios compartir su posición en tiempo real con amigos. La preocupación se centraba en la posible exposición a ciertos peligros que esto suponía para menores de edad.



En paralelo a la utilización de la geolocalización no consentida se han producido hechos tan graves como la **venta de datos de ubicación** por parte de proveedores de servicios móviles como el que se destapó en 2019. Compañías como AT&T, T-Mobile y Sprint habían traspasado este tipo de información a agregadores de datos que luego los vendieron a terceros. También varias agencias gubernamentales de EE UU, incluyendo el Departamento de Seguridad Nacional, compraron durante 2020 registros de localización de teléfonos móviles de empresas privadas, todo ello sin autorización judicial.

RGPD

Reglamento General de Protección de Datos (Unión Europea)

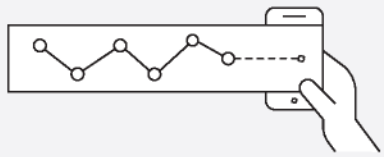
Para los ciudadanos es vital familiarizarse con las leyes y derechos relacionados con la privacidad y aprovechar herramientas legales como el **Reglamento General de Protección de Datos (RGPD) de la Unión Europea**, que establece estrictas normas sobre la recopilación y el procesamiento de datos personales, incluidos los de geolocalización. Las empresas deben obtener un consentimiento expreso y claro de los usuarios antes de recolectar sus datos de emplazamiento y deben proporcionar opciones para que estos gestionen su privacidad. Dentro de España, la **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)** se aplica a la recopilación y procesamiento de datos personales, incluidos los de ubicación.

Medidas personales de prevención

Ante la duda, no hay como cuidarse a uno mismo, por eso es importante tomar una serie de medidas de prevención y protección de la privacidad, que todos podemos tomar:

Desactivar la geolocalización en los ajustes del dispositivo cuando no sea necesaria

Revisar y limitar los permisos de posición otorgados a las aplicaciones



Neutralizar el historial de ubicaciones en las cuentas de Google, Apple u otros proveedores de servicios para evitar el seguimiento continuo.

Anular wi-fi y Bluetooth cuando no estén en uso para evitar el rastreo a través de estas conexiones.

Evitar conectarse a redes wi-fi públicas no seguras

Este listado es un mínimo, ya que si se quiere un extra de seguridad conviene utilizar una **VPN (Red Privada Virtual) para ocultar la dirección IP y la localización** real mientras se navega por internet; y echar mano de navegadores enfocados en la privacidad como Tor o Brave, que limitan el seguimiento online y protegen la ubicación, o utilizar aplicaciones que bloqueen rastreadores y protejan la información personal.

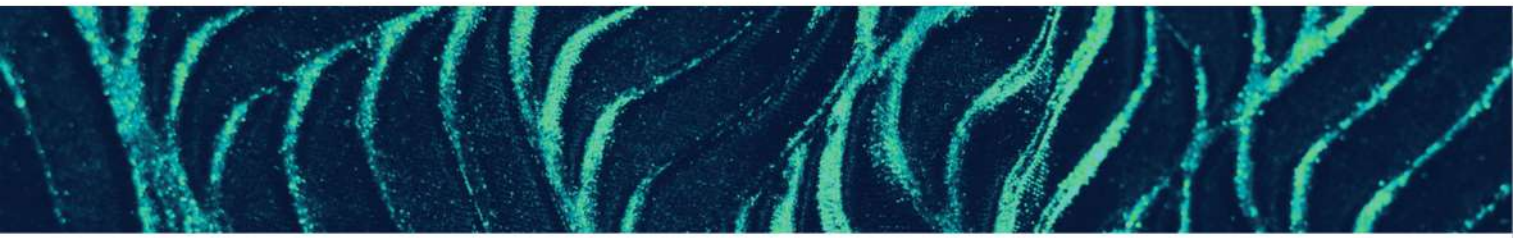
"Ante esta situación se impone una concienciación de los ciudadanos, pues debe por supuesto buscarse el equilibrio entre derechos fundamentales –como el derecho a la privacidad y el derecho a la seguridad– y los deberes de los ciudadanos; deberes que en no pocas ocasiones son olvidados y de cuyo cumplimiento depende el equilibrio y la supervivencia misma de la sociedad" destaca Piñar en un llamado a la conciencia.

"Los ciudadanos también deben ser capaces de reaccionar, de utilizar todos los medios que tienen a su alcance para contrarrestar la violación soterrada pero desgraciadamente imparable de ciertos derechos", opina PIñar. "Estos medios incluyen las vías de reclamación ante los organismos supervisores o ante los tribunales, que están demostrando que son capaces de enfrentarse a los retos de la innovación". En este aspecto, destaca el ejemplo de la Corte Suprema de Chile, con su sentencia de agosto de 2023 en el caso Emotiv, al **reconocer la existencia de los neuroderechos**.

Los casos de abusos subrayan la necesidad de regulaciones estrictas y claras sobre el uso de datos de geolocalización, reconocimiento biométrico y videovigilancia. Los programas de rastreo personal que puede utilizar la Agencia Tributaria española pueden parecer una nimiedad al lado del Skynet chino, pero son al fin y al cabo sistemas capaces de vulnerar el derecho a la intimidad, y todos requieren límites y controles. Es esencial que **las empresas y los gobiernos sean transparentes** sobre cómo recopilan, usan y comparten esta información, y que obtengan el consentimiento explícito de los usuarios. Además, deben implementarse salvaguardias robustas para proteger la privacidad y prevenir abusos. La tecnología de geolocalización tiene el potencial de mejorar nuestras vidas, piénsese en una emergencia sanitaria o en la ubicación de una persona perdida; pero es necesario equilibrar cuidadosamente su uso con la protección de los derechos fundamentales de privacidad.

> Es esencial que las empresas y los gobiernos sean transparentes sobre cómo recopilan, usan y comparten esta información

Piñar aclara que "no se trata de frenar el avance de la innovación ni de frenar el desarrollo y la transformación digital en nuestra sociedad. Se trata de impulsarla desde el respeto a los derechos fundamentales, para evitar situaciones que ya están dándose en otros entornos donde el valor de la libertad y de la privacidad es menos relevante. No olvidemos lo que advertía Strelnikov al doctor Zhivago, 'Ya no existe la vida privada en Rusia. La historia la ha matado. La vida privada ha muerto para un hombre que lo sea de verdad'".



Sponsors

accenture · aena · Agbar · Asterra Partners · ATRESMEDIA · Colegio Notarial de Madrid · ZF · Consorci barcelona ZONA FRANCA · MONDRAGON · coxenergy · Fundación "la Caixa" · Grupo HOTUSA · indra · Mobile WorldCapital Barcelona · PRISA · Prodigioso Volcán · Telefónica · Universidad de Navarra · urbaser

Colaboradores

Deloitte. · ECIJA · HENNEO · LLYC · taller de ideas