

Herta Security

Junio 2022 (Versión revisada)
Observatorio de Derechos Humanos y Empresas
En el Mediterráneo / Shock Monitor

recerca@odhe.cat

Una ficha de:



Con el apoyo económico de:



La información contenida en este informe es responsabilidad del Observatorio de Empresas en la Mediterránea – ODHE, una iniciativa de Suds y Novact. No se refleja necesariamente la posición de la Diputación de Barcelona.

FICHA DE EMPRESA

Nombre empresa	Herta Security S.L.
Grupo empresarial	Hasta 2021 la empresa formó parte del grupo Everis (actual NTT)
Año de creación y Sede Central	2009. Sede en Barcelona y oficinas en Madrid, Londres, Los Ángeles, Montevideo y Singapur.
CEO y otros altos cargos	Administrador único y director general: Javier Rodríguez Saeta Jose Rufino Torija Marti (consejero y secretario); Enrique López Pérez (Apoderado y socio de la empresa Belroal Consulting S.L.); Fernando Domínguez Criado (Consejero de la empresa)
Accionistas	Los principales accionistas y propietarios de la empresa Javier Rodríguez Saeta y Javier Herrando. Hasta el 2021 Everis, mantuvo el 25,83% de las acciones ¹ .
Tamaño empresa	Herta Security opera en más de 50 países y trabaja con más de 150 empresas. En 2018 su plantilla contaba con 35 trabajadores ² .
Sector industrial y servicios/productos	Soluciones de reconocimiento facial y visión por computador para servicios de seguridad (Biosurveillance y Biosurveillance Next), marketing (Biomarketing) , análisis forense (Biofinder), control de accesos (Bioaccess) y análisis de comportamiento humano (Biobserver) ³ . Durante la pandemia de la Covid-19, la empresa desarrolló nuevas aplicaciones para la gestión del distanciamiento social, control de aforo, e identificación de sujetos incluso con uso de mascarillas. Sus soluciones se aplican en espacios públicos y privados como infraestructuras de transporte público (aeropuertos, estaciones de autobús), casinos, acontecimientos multitudinarios (estadios, conciertos, etc) e infraestructuras críticas (gobierno, agentes de seguridad).
Impacto en la región Mediterránea	Herta integra sus tecnologías con otros productos de empresas que registran o están bajo investigación en casos de vulneraciones de derechos y actividades ilícitas en Asia Central y Oriental, incluyendo Oriente Próximo.
Complicidad Europa/Estado español	La tecnología de biometría facial es considerada de alto riesgo por su potencial impacto en derechos y libertades fundamentales. La empresa afirma no poder controlar el uso que sus clientes hacen de su tecnología. La empresa ha recibido subvenciones públicas a nivel estatal y europeo. Según la Universidad de Cardiff, Herta fue el principal proveedor de tecnología de reconocimiento facial en el proyecto IBorderCtrl que finalizó con el reconocimiento público del equipo coordinador del impacto negativo en libertades fundamentales. Herta se expande en proyectos de Smart Security y controles fronterizos; su último proyecto se localiza en el Puerto de Algeciras.
Otras informaciones relevantes	Web corporativa: hertasecurity.com/es/ <i>Amplios proyectos de Smart City en Phuket (Tailandia), Mumbai y Kākināda (India). En la India la empresa ha instalado su software en más 4.000 cámaras del sistema ferroviario del país.</i>

¹ Véase: https://es.nttdata.com/documents/esg-memorias/everis_memoria_2016_es.pdf

² Agustí, A. (2018). "Herta, seguretat per la cara". Port de Barcelona. Disponible (09/03/2022); https://www.viaempresa.cat/empresa/herta-seguretat-cara-mwc_52991_102.html

³ Véase: <https://hertasecurity.com/es/soluciones-de-reconocimiento-facial/>

Abstract

En tan solo 10 años Herta Security se ha convertido en una de las principales empresas del sector de ciberseguridad e inteligencia artificial del mundo⁴. La empresa ofrece Tecnologías de Reconocimiento Facial (TRF) y visión por computadora, especialmente en el sector de la seguridad. Sus soluciones tecnológicas se utilizan en estaciones de autobús, estadios, prisiones, casinos y proyectos de *Safe and Smart City*. Asimismo la TRF de Herta se integra con otras plataformas de gestión de vídeo, cámaras de videovigilancia, sensores y otros dispositivos de terceras empresas que registran vulneraciones de derechos humanos en contextos de alto riesgo.

La empresa nace en la Universidad Politécnica de Barcelona de la mano de Javier Rodríguez Saeta, actualmente administrador único y director general de la empresa. Según Javier Rodríguez: "Yo creía que en el futuro sería muy importante reconocer a personas que no quieren ser reconocidas, de forma automática y no colaborativa⁵". Con este leitmotiv, la empresa ha desarrollado tecnologías de alta precisión y procesamiento para identificar las caras de la población de forma masiva en tiempo real tanto en espacios público abiertos como control de accesos. En su [web](#) describe: "Cada día decenas de cámaras enfocan nuestras caras sin que ni siquiera nos demos cuenta". Sus principales clientes son gobiernos, Fuerzas y Cuerpos de Seguridad y otras empresas privadas.

La empresa opera a nivel global pero debido a las regulaciones europeas sobre protección de datos y privacidad, Herta ha intensificado sus operaciones en mercados de América Latina y Asia, incluyendo Colombia y Rusia. El CEO de la empresa considera que es imposible controlar lo que hacen sus clientes con la tecnología que ellos venden⁶.

El impacto de la TRF en los Derechos Humanos

La TRF identifica de forma masiva e indiscriminada las personas que transitan por espacios públicos y privados. En el entramado de las sofisticadas cámaras de videovigilancia que encontramos en las grandes urbes globales, es casi imposible para una persona poder mantenerse en el anonimato salvaguardando su derecho de privacidad. Según la Fundamental Rights Agency de la UE, la vigilancia permanente afecta a las libertades civiles y políticas como el derecho de libertad de expresión, asociación y protesta desalentando su ejercicio⁷.

Las vulneraciones son especialmente graves cuando son utilizadas por las fuerzas de seguridad de los Estados, ya que la tecnología TRF realiza un proceso automatizado para cotejar personas en el espacio público con perfiles registrados en casos criminales, pudiéndose provocar identificaciones erróneas. Además, estudios realizados por diversas universidades norteamericanas alertan de los altos índices de errores en la categorización por género de más de 20%, así como sesgos significativos que conducen a identificaciones erróneas de personas de ascendencia africana y asiática⁸.

⁴ Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace. Disponible (09/03/2022): https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf Pág.27-28

⁵ Agustí, A. (2018). Op. Cit.

⁶ Takahashi, D. (2015). "Nvidia highlights five startups that use cool graphics technology". Venture Beat. Disponible en: https://venturebeat.com/2015/03/18/nvidia-highlights-five-startups-using-cool-graphics-technology/?utm_source=dlvr.it&utm_medium=twitter (acceso: 09/03/2022).

⁷ EU Fundamental Rights Agency (2018). *Under watchful eyes: biometrics, EU IT systems and fundamental Rights*. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (Acceso: 09/03/2022)

⁸ INCLCLO (2021). *IN FOCUS. Facial Recognition Tech Stories and Rights Harms From Around the World*. Pág: 6-18. Disponible en <https://www.inclc.net/pdf/in-focus-facial-recognition-tech-stories.pdf> (Acceso: 09/03/2022)

Herta asegura que su tecnología de reconocimiento facial es conforme con el Reglamento de Protección de Datos (RGPD) a nivel europeo⁹. Sin embargo, expertos de varias universidades europeas, consideran que la RGPD no incluye mecanismos robustos de rendición de cuentas y transparencia de como los Estados realizan la revisión y autorización de los sistemas de vigilancia biométrica, así como las verificaciones de la "limitación del uso" de estas tecnologías¹⁰.

A nivel europeo, Herta Security participa en el [proyecto AI MARS](#) (Artificial Intelligence System for Monitoring, Alert and Response for Security in events) para proveer a los Cuerpos y Fuerzas de Seguridad del Estado de información sobre biométrica de la población en espacio públicos y privados como manifestaciones, centros comerciales o eventos deportivos¹¹.

A nivel internacional, la empresa Herta ha intensificado sus operaciones en otros mercados como América Latina. En ciudades como Medellín, Herta colabora con **Neural Labs** para identificar matrículas de vehículos y caras de la población¹². En Uruguay la empresa puso en marcha un sistema integrado por CDT Latam, incluyendo tecnología de **Wavestore, Axis Cameras y Huawei**, para identificar a *hooligans* en el estadio del centenario de Montevideo¹³.

El sistema de reconocimiento facial de Herta para acontecimientos deportivos también se implementó durante la **copa del mundo de fútbol en Rusia en 2018**¹⁴. Sin embargo, uno de los principales peligros de la TRF es que sean utilizados por gobiernos autoritarios que persiguen a ciudadanos por su orientación sexual o color de piel. Javier Rodríguez Saeta, CEO de Herta, asegura que **no puede controlar que hacen sus clientes con la tecnología proveída**: "Es un desafío para nosotros y una pregunta para el usuario final de la tecnología¹⁵".

Sin embargo, es importante destacar que la relación que se establece entre empresas de tecnologías de seguridad como Herta no solo se basa en una simple transferencia de tecnología, sino que requiere una amplia colaboración con el cliente para el diseño, adaptación e implementación de la tecnología, proceso que puede implicar el acceso de la empresa a datos personales en posesión del cliente. En el caso de agencias policiales y de seguridad estas bases de datos son muy sensibles por la implicaciones que pueden tener en la seguridad de las personas. En este sentido, Herta detalla como en la gala de los Globos de Oro de 2018 tuvieron **acceso a bases de datos policiales del FBI y la policía de Beverly Hills**¹⁶.

Colaboraciones de Herta y vulneraciones de derechos humanos.

En su web corporativa, Herta muestra los principales [partners](#) con los que desarrolla y ofrece su tecnología. Entre ellos destaca la empresa **Avigilion, parte de Motorola Solutions**, y que, de

⁹ Ver respuesta de Herta de abril 2022 a la primera versión de la ficha de su empresa en www.odhe.cat

¹⁰ Ragazzi, F., et al. (2021). *Biometric and Behavioural Mass Surveillance in EU Member States*. The Greens/EFA in the European Parliament. Disponible en: <https://www.greens-efa.eu/biometricsurveillance/> (Acceso: 09/03/2022)

¹¹ Véase: <https://itcl.es/proyectos-eia/aimars/>

¹² Pledge Times (2021). "Elías Valcárcel, CEO of Neural Labs: 'Smart cameras take very dangerous people off the street'" Disponible en <https://pledgetimes.com/elias-valcarcel-ceo-of-neural-labs-smart-cameras-take-very-dangerous-people-off-the-street/> (Acceso: 09/03/2022)

¹³ Mayhew, S. (2018). "Herta awarded for facial recognition system security Uruguay football stadiums". Biometric.Update.com. Disponible en: <https://www.biometricupdate.com/201808/herta-awarded-for-facial-recognition-system-securing-uruguay-football-stadiums> (Acceso: 09/03/2022)

¹⁴ Véase: <https://hertasecurity.com/es/news/reconocimiento-facial-para-identificar-a-los-malos/>

¹⁵ Takahashi, D. (2015). Op. Cit.

¹⁶ Véase: https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/herta_reconeixement_facial_mwc18

acuerdo Naciones Unidas, desarrolla **actividades ilícitas en los Territorios Ocupados Palestinos**¹⁷. Diomar Carrascal, *Country manager* de Herta, afirma que su TRF "se [integra](#) muy bien con la plataforma de Avigilion"¹⁸.

Herta ha establecido también alianzas con gigantes tecnológicos como [Nvidia e Intel](#). Actualmente ambas empresas fueron investigadas por Congreso de Estados Unidos por la venta de chips avanzados para **sistema de vigilancia masiva con graves violaciones de derechos humanos de las comunidades Uigures, Kazajos y otras minorías religiosas predominantemente musulmanas de la Región Autónoma de Xinjiang en China**¹⁹.

Otro *partner* estratégico de Herta es [Qognify](#), empresa con sede en New York y especializada en soluciones de *video management* y que fue creada a partir de la adquisición del departamento de seguridad física de la israelí **Nice Systems**, empresa que registra vulneraciones de derechos humanos por la venta de su tecnología a **países autoritarios en Asia Central como Kazajstán y Uzbekistán** según Transparency International²⁰.

La tecnología de Herta se [integra](#) también en la plataforma [Nx Network Optics](#) para gestionar y procesar la información capturada. Nx Network Optics también utiliza en sus sistemas la tecnología de video Synopsis de **BriefCam**²¹. La empresa israelí BriefCam ha desplegado su **sistema de videovigilancia con el sistema Synopsis en los Territorios Ocupados del Este de Jerusalén** para el control de la población palestina²².

Asimismo, **Axis Communication**, otro aliado de Herta especialmente en los proyectos de [Smart/Safe Cities](#), también integra en su plataforma la tecnología de **BriefCam**²³. Los sistemas de vigilancia de Axis Communication se han implementado en los proyectos de reconocimiento facial en estadios deportivos como Montevideo.

Smart cities y control fronterizo

La priorización, por parte de las instituciones públicas, de respuestas securitarias para afrontar el reto del terrorismo internacional a partir del 2015 y la pandemia a finales de 2019, ha permitido el crecimiento de empresas de seguridad y en particular corporaciones del ámbito tecnológico como Herta. Por ejemplo, Herta ha participado en varios proyectos europeos en estos ámbitos, como el proyecto H2020 [AWARE](#) desarrollado entre 2019 y 2020 y que tenía por objetivo el análisis del comportamiento de multitudes para prevenir ataques terroristas.

En este sentido, los proyectos *Safe/Smart City* que se desarrollan en muchas ciudades europeas adoptan esta perspectiva securitaria. Herta considera este sector fundamental para su desarrollo comercial y prueba de ello es la implementación de su tecnología en la **Estación del Sur (Madrid), en el proyecto Safe City de Niza y en la estación de tren de Berlín Südkreuz**²⁴.

¹⁷ UN Human Rights (2020). "UN rights office issues report on business activities related to settlements in the Occupied Palestinian Territory". Disponible en: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25542>

¹⁸ Para más información: <https://dramstechnology.com.ar/2016/10/08/avigilon-mas-alla-de-la-videovigilancia-de-alta-definicion-y-el-control-de-accesos/>

¹⁹ Nota informativa de la Comisión sobre China del Congreso de Estados Unidos: <https://www.cecc.gov/media-center/press-releases/chairs-ask-ceos-of-intel-and-nvidia-about-possible-involvement-in-human>

²⁰ Privacy International (2014). *Private Interests: Monitoring Central Asia. Special report*. Disponible en: https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf (Acceso: 09/03/2022)

²¹ Véase: https://www.youtube.com/watch?v=vW_meVL-6ko

²² Véase: <https://www.whoprofits.org/company/briefcam/>

²³ Para más información ver: <http://mass-surveillance.odhe.cat/>

²⁴ Ragazzi, F., et al. (2021). Op. Cit.

El proyecto "Sicherheitsbahnhof" de Berlín se desarrolló entre 2017 y 2018 y aparte de la empresa Herta participaron **Dell EMC AG, Morpho Video Investigator (MVI), IDEMIA AG y AnyVision**. Desde ODHE se han denunciado las prácticas de vigilancia contra la población palestina en Cisjordania y Este de Jerusalén vulnerando sus derechos de civiles y políticos utilizando la tecnología Anyvision²⁵.

Los espacios de control fronterizo son otras áreas de Herta. En 2010, la empresa realizó un proyecto piloto en el aeropuerto de Barajas en colaboración con la empresa Hoyos Corporation especializada en tecnología de escaneo de iris²⁶. Herta es proveedor de la tecnología de reconocimiento facial en el proyecto europeo iBorderCtrl²⁷. Como se describe en el informe "Vulneraciones de Derechos Humanos en el Sistema de Deportaciones", el proyecto iBorderCtrl pretendía verificar la identidad de los viajeros en pasos fronterizos a través de la autenticación de pasaporte, verificación de datos biométricos y detectores de engaños²⁸.

Desde 2020, Herta participa en un **proyecto piloto 5G** cofinanciado por la agencia nacional Red.es y el FEDER (Fondo Europeo de Desarrollo Regional) y liderado por Information Processing and Telecommunications Center (IPTC) de la Universidad Politécnica de Madrid en cooperación empresas como Huawei, Indra, Everis y Vodafone, entre otras, y el apoyo de otras 11 instituciones públicas, entre las que destaca el Ministerio de Economía y la Guardia Civil. El proyecto tiene múltiples aplicaciones en el sector agricultura, salud, ciudades inteligentes, seguridad y defensa, etc. El primer caso de uso se realiza en el Puerto de Algeciras para controlar el tráfico de vehículos y personas por el "paso del Estrecho". La tecnología de reconocimiento facial de **Herta reconocerá a personas sospechas registradas en las bases de datos de la Guardia Civil**²⁹.

Herta también disfruta de una **subvención de la Agencia Estatal de Investigación** del Ministerio de Ciencia e Innovación por un valor 76,834,50 euros para el período 2012-23 para el desarrollo de un proyecto alineado con el marco del plan estatal de investigación científica y técnica y de innovación 2017-2020³⁰.

El **Instituto español de Comercio Exterior (ICEX)**³¹ y la **Agència per la Competitivitat de l'Empresa Catalana (ACCIO)**³² considera Herta una buena práctica de internacionalización empresarial y apoyan a la empresa reforzando su visibilidad y promoviendo este modelo entre otras empresas del tejido empresarial del Estado español.

Resistencias y demandas

²⁵ Véase: <http://www.odhe.cat/anyvision/>

²⁶ Para más información: <https://www.aviationpros.com/home/news/10374713/hoyos-corporation-debuts-airport-security-solution-powered-by-iris-scanning-technology>

²⁷ Monedero-Sánchez, J. (2018). *The datafication of borders and management of refugees in the context of Europe. Working paper*. Datajustice. Cardiff University. Pág. 22. Disponible: <https://datajusticeproject.net/wp-content/uploads/sites/30/2018/11/wp-refugees-borders.pdf> (Acceso: 09/03/2022)

²⁸ García, A. et al (2021). *Vulneraciones de los derechos humanos en las deportaciones. Estudio de caso: Marruecos*. Disponible en: https://iridia.cat/wp-content/uploads/2020/11/Deportaciones_FinalMOD_Imprimir-2.pdf (Acceso: 09/03/2022)

²⁹ Para más información ver: <https://iptc.upm.es/proyecto-piloto-5g-en-el-puerto-de-algeciras>

³⁰ Para más información ver: https://www.aei.gob.es/sites/default/files/stfls/MICINN/Ayudas/PE_2017_2020/PE_Promocion_Talento_Empleabilidad/S_ubprograma_Estatal_Incorporacion/FICHEROS/Torres_Quevedo_2019/Resolucion_Concesion_PTQ2019.pdf

³¹ Véase: <https://icexnext.es/experiencias-next/herta-security-ganadora-de-los-premios-ifsec-y-nvidia>

³² Véase: http://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/herta_reconeixement_facial_mwc18

La empresa Herta se ha visto involucrada en dos proyectos que han encontrado resistencias desde la sociedad civil. Por un lado, el proyecto de "Sicherheitsbahnhof" de la estación de tren Südkreuz de Berlín in 2017/18 fue denunciado por la sociedad civil y organizaciones como Chaos Computer Club argumentaron que los resultados de los testeos, con bajas probabilidades de identificación, no justificaban aplicar una tecnología de control tan invasiva³³.

Por otro lado, el proyecto EU IBorderCtrl, donde Herta era el principal proveedor de la TRF, fue también objeto de un intenso debate público que finalizó con el reconocimiento público por parte del equipo motor de que la tecnología podía vulnerar los derechos fundamentales³⁴.

En este sentido, es importante destacar el trabajo realizado por la red EDRi y otras organizaciones especializadas en tecnología de seguridad y derechos digitales, para prohibir el uso de la vigilancia biométrica en Europa a través de la campaña [Reclaim your face](#). En el Estado español, nuevos grupos como [Algorights](#) están emergiendo para incidir política y socialmente sobre el uso de las tecnologías de inteligencia artificial desde una perspectiva de respeto de los Derechos Humanos.

También es importante destacar que el movimiento de solidaridad por Palestina formado por organizaciones como Al-Haq, están trabajando con múltiples instituciones públicas para limitar la contratación pública de empresas listadas en la Base de Datos de la ONU de empresas con actividades económicas ilícitas en los Territorios Ocupados de Palestina. En esta "lista negra" se encuentra la empresa Avigilon de Motorola Solutions, *partner* de Herta, que ha encontrado en el movimiento BDS una fuerte denuncia.

Recomendaciones

La Comisión Europea expresó en 2021 que algunas tecnologías y aplicaciones deben ser vigiladas por su alto riesgo en la vulneración de las libertades fundamentales. Expertos de varias universidades europeas y miembros del Parlamento Europeo, consideran que, a luz de vulneraciones de derechos fundamentales producidas por la vigilancia masiva biométrica analizadas en diferentes casos de estudio, este tipo de tecnologías deben ser prohibidas³⁵. En esta línea, la plataforma formada por 44 organizaciones de la sociedad civil, EDRi, afirma que la falta de rendición de cuentas, control y transparencia son motivos suficientes para prohibir el uso de esta tecnología³⁶.

El ODHE realizó en 2020 y 2021 la [investigación Mass Surveillance](#) donde detallaba las principales tecnologías de control y vigilancia masiva que estaban siendo utilizadas antes y durante la pandemia de Covid-19, incluyendo numerosos casos de estudio de uso donde el uso discrecional de estas tecnologías por parte de gobiernos, fuerzas de seguridad y otras empresas privadas había provocado graves vulneraciones de derechos humanos. Las siguientes recomendaciones son fruto de ese informe y se alinean con las demandas de miembros del Parlamento Europeo y la sociedad civil especializada en la materia. Concretamente:

Recomendaciones dirigidas a las autoridades públicas:

³³ Ragazzi, F. et al. (2021). Op. Cit.

³⁴ García, A. et al (2021). Op. Cit.

³⁵ Ragazzi, F. et al. (2021). Op. Cit.

³⁶ Véase: <https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>

- **Proteger los derechos digitales y las libertades civiles:** Exigimos respeto a la privacidad y libertad de las personas, y la protección de los datos personales. Para ello es necesario el uso democrático de la tecnología en los espacios públicos.
- **Prohibición de la Vigilancia Masiva Biométrica:** Las tecnologías de reconocimiento facial y otras herramientas que utilizan datos biométricos son altamente intrusivas en la vida cotidiana de las personas y violan los derechos fundamentales.
- Garantizar **la transparencia**, el acceso a la información y la rendición de cuentas de las tecnologías digitales utilizadas en los espacios públicos por los organismos encargados de hacer cumplir la ley y las corporaciones privadas.
- **Detener los acuerdos comerciales con empresas militares, de seguridad y ciberseguridad israelíes.** Prohibir la importación y exportación de tecnologías de vigilancia masiva que han sido desarrolladas en los contextos de ocupación israelí de Palestina. Excluir a las empresas que proporcionan la tecnología utilizada por las fuerzas israelíes para hacer cumplir la colonización israelí de Palestina y el asedio de Gaza de los procesos de licitación pública. Que en esta categoría se incluyan a todas las empresas nombradas en la base de datos de las Naciones Unidas involucradas en asentamientos israelíes ilegales.
- **Impedir que el cabildeo corporativo influya en la seguridad pública.** El desarrollo y la implementación de modelos *Smart City* y *Safe City* deben integrar un enfoque de la sociedad civil, teniendo en cuenta los derechos fundamentales. Las políticas públicas deben ser impulsadas por el público al que se supone que deben servir.

Recomendaciones dirigidas a movimientos sociales, activistas y público en general:

- **Protegeos** del estado de vigilancia mejorando las competencias digitales y la seguridad. Más información en: www.privacytools.io; www.eff.org/pages/tools; www.securityinabox.org/en;
- **Informaos sobre el efecto de las tecnologías de vigilancia digital y cread espacios para discutir los efectos del estado de vigilancia** en vuestra comunidad. Por ejemplo, qué datos se recopilan y cómo se procesan; el impacto de la vigilancia en la libertad; y cómo resistir la introducción de nuevas tecnologías por parte del estado y de los municipios locales.
- **Exigid el uso de tecnologías** democráticas en vuestra comunidad y municipio reclamando una contratación pública responsable que promueva los derechos humanos y la protección del medio ambiente.