Vigilancia masiva, tecnocapitalismo y estado policial: análisis crítico y estrategias de autodefensa digital

Por: La peste. 28/01/2021

El 4 de enero del 2021 WhatsApp anunció un cambio en su política de privacidad: sus usuarios fuera de la región europea deberán permitirle compartir su información con su empresa matriz, Facebook. Estos datos incluyen: el número de teléfono asociado al nombre del usuario, la lista de contactos, la marca y el modelo de teléfono que este usa, la empresa con la que obtiene el servicio y las direcciones de protocolo de internet (IP), cualquier pago y transacción financiera realizada a través de WhatsApp.com e incluso la ubicación de las conexiones de una persona. La empresa anunció que quienes no acepten los nuevos términos antes del 8 de febrero, no podrán seguir usando WhatsApp (1).

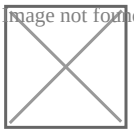
En abril del 2019, Piñera junto su primo, el entonces ministro del interior Andrés Chadwick, presentan el Sistema de Televigilancia Móvil, proyecto que implicó la compra de los primeros 30 drones con tecnología de reconocimiento facial para ser utilizados en la Región Metropolitana. En esa instancia declararon que el propósito sería “detectar incivilidades, realizar patrullajes preventivos en el territorio y obtener medios probatorios ante delitos flagrantes *(…) es nuestro deber hacer todo para llevar más tranquilidad y seguridad a los hogares chilenos”* (2)*.*

¿Qué relación tiene una empresa transnacional como Facebook con la creciente inversión de estados en tecnologías para la vigilancia en Abya Yala y en otras regiones del Sur Global? A nivel mundial, la implementación de sistemas de vigilancia a través de la identificación biométrica, el uso de nuevas tecnologías de información y comunicación, han sido uno de los grandes debates sobre tecnología, ética y derechos humanos durante los últimos años. Sólo en la región china haymás de 200 millones de cámaras de vigilancia instaladas, articuladas con un sistema centralizado de información controlado por el gobierno. En estados unidos, cerca de 150 millones de rostros de personas están registradas en una base de datos hechaa partir del reconocimiento facial. Huawuei, Apple, Facebook, Google y Amazon son sólo algunas de las empresas transnacionales que han invertido millones de dólares en el desarrollo de estas tecnologías en alianza con universidades y centros de investigación, cuyo mercado crece progresivamente.

Al mismo tiempo, la acumulación y mercantilización de nuestra información personal recopilada a través de motores de búsqueda, redes sociales y geolocalización por GPS en dispositivos móviles alimentan cada día las bases de datos. Estas, mediante sistemas de algoritmos de Inteligencia Artificial permiten a las empresas no sólo predecir nuestro comportamiento, sino que incluso pudiendo incidir en nuestras decisiones cotidianas. Casos como Cambridge Analytica en eeuu o Instagis en la región chilena reflejan la efectividad del uso político de estas tecnologías para manipular resultados de elecciones (3). El experto en Big Data, Albert Hilbert, advierte que las nuevas guerras no van a ser por petróleo: 8 de las 10 compañías más valoradas en el mundo son de tecnología digital. Hoy ya son más valiosas que las petroleras. Los datos son el nuevo petróleo. Y el que tiene el control sobre los datos, controla el país (4).

¿Existe una tendencia global de los estados de avanzar hacia sistemas de vigilancia total utilizando *nuevas tecnologías de información y comunicación*? ¿Qué dimensiones alcanza el capitalismo de vigilancia o T*ecnocapitalismo* en este contexto y qué rol cumplen las grandes corporaciones en el uso de esta información? ¿Cuál es el panorama en Abya Yala y en la región chilena, tras las insurrecciones populares del 2019 y la pandemia Covid-19? Revisaremos casos, perspectivas teóricas y prácticas políticas que se están llevando a cabo para comprender las implicancias de este fenómeno y finalmente proponer algunas alternativas de acción frente al avance de esta nueva forma de totalitarismo global.

CHINA: REALIZACIÓN DE LA DISTOPÍA ORWELLIANA



En algunas ciudades de la región china, monitores del tamaño de vallas publicitarias muestran los rostros de peatones imprudentes y la lista con los nombres de la gente que no paga sus deudas. Las cámaras con tecnología de reconocimiento facial vigilan estaciones de tren, aeropuertos, las entradas de los hoteles y residencias. Estos esfuerzos complementan otros sistemas que rastrean el uso del internet y las comunicaciones, los registros de alojamientos en hoteles, los viajes en tren, en bus, en avión e incluso los trayectos en auto en algunos lugares. Rastreo de IP, registro de transacciones con tarjetas bancarias y acceso a datos de geolocalización suministrados por el GPS de smartphones: toda esta información es parte de un sistema central de vigilancia, la *Plataforma Integrada de Operaciones Conjuntas del Estado chino* (IJOP, por sus siglas en inglés) (5). El sistema integra además una evaluación de las personas a través de puntos: un alto puntaje significa que eres “un buen ciudadano” y te permite acceder a servicios públicos como salud y transporte, mientras que un puntaje bajo se traduce en la restricción de actividades cotidianas como viajar a otras ciudades o tomar el metro. A este sistema se ha integrado sistemáticamente durante los últimos años la tecnología de reconocimiento facial y gelocalización, permitiendo al estado chino saber virtualmente *todo* lo que hace una persona determinada en un período de tiempo determinado, e identificar a partir de esta información quiénes son considerados “malos ciudadanos”.

Lentes con tecnología de reconocimiento facial usados por la policía china.

Un informe publicado el 2019 por Human Rights Watch (HRW) denunció que en la conflictiva región noroccidental de Xinjiang se estaban realizando arrestos arbitrarios con sesgos de discriminación religiosa y diversas violaciones a los derechos humanos a partir de la implementación de la IJOP. En este territorio, que vincula a la región china con medio oriente, la policía está utilizando una aplicación móvil articulada con este sistema de vigilancia, la cual distingue 36 perfiles de personas para la recolección de datos. Entre ellos se incluyen personas que hayan dejado de usar teléfonos inteligentes o *smartphones*, aquellas que no “socializan con los

vecinos" y las que "recogieron dinero o materiales para mezquitas". Una vez escrutados los datos, la aplicación selecciona a aquellas personas de las que desconfía y las somete a un escrutinio adicional (6).

El gobierno del estado chino actualmente está impulsando la investigación y el desarrollo de tecnologías que rastrean la vestimenta e incluso el movimiento de una persona, registrando particularidades en su forma de caminar o desplazarse. También han diseñado dispositivos experimentales, como las gafas reconocimiento facial utilizadas por la policía. Cada año, alrededor de 17 mil estudiantes en 60 escuelas primarias en Guangzhou reciben *smartwatches* relojes con GPS en el contexto del programa "Safe Campus Smartwatches" (7). Este es sólo uno de gran variedad de dispositivos *wearables* para geolocalización e identificación biométrica de personas en tiempo real.

El "gigante asiático", con una proyección de crecimiento económico de 8,2% el 2021, reemplazará en pocos meses a eeuu como la economía mundial más poderosa. Hoy es el estado más avanzado en materia de uso de tecnologías para la vigilancia masiva, y actualmente está siendo un referente para los estados que controlan territorios de occidente y del Sur Global para implementar estas tecnologías.

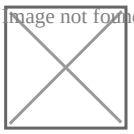
RECONOCIMIENTO FACIAL Y EYETRACKING: NUEVAS TECNOLOGÍAS AL SERVICIO DE LA VIGILANCIA MASIVA

Descripción del proceso de análisis e identificación que hace un software de reconocimiento facial.

La tecnología reconocimiento facial funciona con un sistema que extrae patrones de una imagen y los compara con modelos de caras definidos por patrones previamente registrados. El software asume que lo que está en la imagen es una cara. Un algoritmo de reconocimiento facial registra la cara utilizando dos tipos de parámetros: a) geométricos, calculando la ubicación y relación espacial entre ciertas características de una cara, como el entrecejo, la punta de la nariz y los extremos de la boca; b) parámetros fotométricos, que interpretan la cara como una combinación de caras previamente estandarizadas o 3) análisis de tez facial, el cual mapea la ubicación de lunares, cicatrices, piercings u otras marcas faciales en la piel de la persona (8). Tras realizar este análisis, el algoritmo buscará información en una base de datos para estandarizar la imagen, extrayendo información de las

características faciales para clasificar (registrar la imagen por género y edad estimada), verificar (comparar el molde de cara con otro molde de cara que tenga algún grado de similitud) o identificar a personas (comparar el molde de cara con muchos otros moldes de cara registrados en la base de datos).

El eyetracking, por otra parte, es una técnica de análisis biométrico utilizada en el neuromarketing para obtener información sobre los puntos en los que se fijan más las personas, a través del análisis de sus movimientos oculares captados por cámaras frontales de celulares o de notebooks. Permite identificar los puntos a los que más mira una persona (frecuencia o tiempo de fijación de la mirada), puntos de no atención, capacidad de localización de información (tiempo que tarda hasta encontrar X punto), etc. (10). Indicadores como la dilatación de las pupilas son indicio de emociones o interés generado por una publicación, entregándole valiosa información al algoritmo sobre el tipo de contenidos que pueden recomendarte a continuación, logrando de esta forma captar nuestra atención por la mayor cantidad de tiempo posible.



El desarrollo de tecnologías reconocimiento facial y eyetracking ha sido impulsado gracias a las millonarias ganancias en materia de publicidad y diseño de experiencia de usuario a través de redes sociales en empresas como Facebook y Amazon. Sin embargo no existen garantías de privacidad sobre el uso de esta información, la cual puede ser registrada y archivada por las empresas, generalmente sin nuestro consentimiento. Nuestras caras y perfiles de comportamiento en internet pueden terminar en muchos lugares, desde la empresa que paga por esa información para ofrecerte publicidad personalizada en Instagram, hasta el FBI o la IJOP china. Se registran numerosos casos de corporaciones como Apple y Google entregando información a gobiernos con el propósito de realizar investigaciones criminales (11)(12). En el territorio controlado por el estado de $hile se han instrumentalizado casos de robo en Malls o situaciones de violencia en estadios para eventos deportivos como argumento para justificar la implementación de sistemas de reconocimiento facial (13).

El reconocimiento facial ha recibido mucha cobertura mediática siendo indicado por

los gobiernos como la forma más eficiente de controlar la delincuencia por medio de la tecnología, argumentando desde un enfoque desarrollista y tecnocrático cómo la innovación tecnológica puede mejorar el bienestar subjetivo de las personas. Sin embargo la realidad nos dice algo distinto sobre la efectividad del uso de esta tecnología en materia de seguridad.

UN SISTEMA FALIBLE: LA BIOMETRÍA Y SUS SESGOS

Numerosas investigaciones han demostrado el alto porcentaje de falsos positivos arrojado por distintos sistemas de reconocimiento facial en funcionamiento alrededor del mundo, particularmente cuando se trata de personas de tez oscura, personas trans o no binarias. La policía en Londres reportó que identificó con esta metodología a individuos erróneos en un 92% de los casos, y en Nueva York la cifra de falsos positivos llegó a 80%. En la región argentina, un hombre estuvo seis días en la cárcel tras ser identificado por una cámara con reconocimiento facial como el culpable de un delito que nunca cometió. Su inocencia fue comprobada y la policía sólo le pidió disculpas. En la región chilena, el sistema del Mall Plaza resultó en un 90% de casos erróneos en el periodo de marcha blanca (14).

El intendente de la región metropolitana Felipe Guevara de la Felipe Guevara, quien recibió una acusación constitucional por violaciones a los derechos humanos durante la revuelta popular.

En un experimento realizado por la *American Civil Liberties Union* (ACLU) el software de reconocimiento facial desarrollado por Amazon reconoció erróneamente a 28 congresistas estadounidenses como autores de algún crimen, con un número desproporcionadamente alto de personas afrodescendientes entre ellos. El proyecto *Gender Shades*, desarrollado por la investigadora Joy Buolamwini, demuestra que las tecnologías de reconocimiento facial disponibles en el mercado tienen grandes dificultades identificando mujeres afrodescendientes y obtienen sus mejores resultados cuando los sujetos analizados son hombres blancos (15).

En definitiva, investigadores de la industria de la vigilancia y organizaciones civiles como Derechos Digitales reconocen que la tecnología de la actualidad tiene sesgos evidentes y en la práctica es incapaz de analizar tanta gente (16). Se requiere la digitalización de cientos de miles de archivos, fotos y videos guardados, y muchos de ellos no cuadran con facilidad debido a su mala resolución o incompatibilidad de archivos. Se requieren fotos de distintos ángulos de un rostro para que el software

pueda hacer el *match* (esa es la razón por la cual empresas como Facebook son tan peligrosas, debido a la cantidad de fotos y videos personales que almacenan). En la región china aún existen equipos de personas que revisan fotos y datos individualmente, de forma análoga, lo cual resulta demasiado lento y arbitrario, demostrando que la etapa actual de implementación de los sistemas de reconocimiento facial no se caracteriza (hasta el momento) por su precisión ni por su eficiencia, sino por su poder como herramienta mediática y psicológica de control social a través del miedo y la sensación de sentirse vigilado en todo momento.

En todos los países donde han sido implementados, los sistemas de reconocimiento facial han facilitado la institucionalización de sesgos asociados a la clase social y el color de la piel, reforzando prejuicios sociales, manteniendo sistemas de persecución criminal discriminatorios y basados en la sospecha del “otro” enemigo, del “terrorista”. Es otro reflejo de la tesis del *enemigo interno*, o como ha señalado Piñera el “enemigo poderoso, implacable, que no respeta a nada ni a nadie”. Sean musulmanes en la región china, afrodescendientes en EEUU o mapuche en Wallmapu, el Capital transnacional utiliza el mismo sesgo para criminalizar a un sector específico de la población, validando la persecución y la represión.

BIG DATA Y TECNOLOGÍAS DEL YO

El filósofo surcoreano Byung-Chul Han plantea que uno de los rasgos más característicos de nuestro periodo histórico es el “dataísmo”, o la tendencia a convertir todo en datos e información. Cualquier movimiento del individuo es susceptible de tener un valor comercial y ahí es donde gana toda su relevancia el concepto de macrodatos o *Big Data*, el uso de una cantidad de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento para analítica (17). Se utiliza principalmente en ámbitos tan amplios como economía y la publicidad, hasta el espionaje y el control de enfermedades infecciosas, pero uno de sus usos más comunes es realizar modelamiento de comportamiento del usuario, extrayendo valor de los datos almacenados, y formulando predicciones a través de los patrones observados.

Según Han, no solo todas las personas estamos vigiladas por todas, sino que incluso se fomenta la autovigilancia o autocontrol a través de las *tecnologías del yo*, con las que el individuo extrae datos sobre sí mismo: aplicaciones como Huawei Health o Google Fit registran datos como ritmo cardiaco, peso, sudoración, cantidad

de pasos, en tiempo real, con la excusa de ayudarnos a estar saludables y compartir en redes sociales nuestros gustos deportivos (18). De este modo se llega a tal punto que los objetos “inteligentes” controlan al individuo: la web 3.0 hace posible un registro total de la vida, siendo vigilades por los dispositivos que utilizamos de forma voluntaria y cotidiana.

Smart-Tee, polera que mide ECG, frecuencia cardiaca y calorías quemadas, desarrollada por SIMTech.

La adicción a las redes sociales como Instagram o TikTok son un problema creciente que facilita el trabajo de las empresas para obtener nuestra información personal. “Si tú no pagas por el producto, *TÚ* eres el producto” afirmaba Tristan Harris, ex trabajador de Google y actual activista por el uso ético de la tecnología. “Todos los ´me gusta´, todos los videos, todos los comentarios, se integran para construir un modelo más preciso y con eso pueden predecir mejor lo que la persona hará. Pueden predecir qué emociones te generará un video o una foto para así tenerte más tiempo frente a la pantalla”.

El investigador Luis Suárez-Villa realiza un aporte a la comprensión de este fenómeno en el libro *Tecnocapitalismo*. *Una perspectiva crítica sobre Innovación Tecnológica y corporativismo,* definiendo el concepto como una nueva versión de capitalismo que genera nuevas formas de organización empresarial diseñadas para explotar los bienes intangibles tales como la creatividad o necesidades psicológicas humanas (19). Según el autor, las relaciones de poder del Capital transnacional han permeado disciplinas que originalmente estaban orientadas a la investigación científica. Áreas como la biotecnología, la nanotecnología y la bioinformática han sido cooptadas por empresas como Google y Huawei para desarrollar nuevas tecnologías experimentales con el único propósito de mejorar sus ganancias.

La importancia del Big Data, asociado a las tecnologías del yo, no gira en torno a la cantidad de datos que tienes, sino en lo que haces con ellos. Las empresas toman datos de cualquier fuente y los analizan para encontrar respuestas que les permiten reducir los costos, tiempo, desarrollar nuevos productos, optimizar las ofertas y personalizarlas a través de redes sociales o sitios web (*targeting*). Tecnologías como el reconocimiento facial pueden ser una amenaza no tanto por la identificación individual de las personas, sino porque potencialmente pueden descubrir una gran cantidad de información personal asociada a esa cara: perfiles de redes sociales, comportamiento en internet, compras, patrones y frecuencias de viajes, entre otras.

El problema radica en que si bien la infraestructura para obtener la información es propiedad privada de empresas, esta información siempre podrá ser utilizada por las policias y gobiernos bajo el argumento de resguardar la seguridad nacional. “La democracia no está preparada para la era digital y está siendo destruida” (20) planteaba Albert Hilbert hace unos años a propósito del uso que dan los estados y las grandes empresas a las tecnologías para la vigilancia. Todo indica que hoy estamos enfrentando el inicio de una era de t*otalitarismo digital* a través de una alianza Capital-estado como un mismo ente complejo de vigilancia y control social.

Como respuesta al control social mediante tecnologías del Yo, surgen en europa durante la segunda mitad del siglo XX las teorías transhumanistas, que promueven el uso de tecnologías para transformar condición humana mediante el desarrollo y fabricación de tecnologías disponibles (21). La neuropsiquiatría ha permitido por ejemplo entender qué drogas son más efectivas para sacar el máximo rendimiento a nuestra energía física y mental, sin generar adicción o efectos secundarios no deseados. En el mundo del deporte se ha probado bastante la efectividad del uso de prótesis con biotecnología. Sin embargo la brecha digital y la mercantilización de la salud, la educación y la tecnología dificultan el acceso a este tipo de servicios y aplicaciones tecnológicas a la mayor parte de la población mundial, lo cual lo convierte en un planteamiento descontextualizado para la realidad del Sur Global.

VIGILANCIA SATELITAL, GEOLOCALIZACIÓN Y PANDEMIA

Google es un buen ejemplo de cuánta información personal puede obtener una sola empresa: además de su famoso buscador, que actualmente el sitio más visitado del mundo, la empresa estadounidense fundada por Larry Page y Serguei Brin integra a través de su matriz Alphabet Inc (22). la información proporcionada por Google

Earth, Google Maps, Google Chrome, Google Lens, Google Pay, Google Fotos, Google Street View, Google Drive, Google Docs, Gmail, Youtube, Android y últimamente Google Meet, permitiendo obtener a través de algoritmos e Inteligencia Artificial un patrón de comportamiento bastante detallado de sus usuarios.

El historial de ubicaciones de Google Maps almacena información a través de los datos GPS sobre tus desplazamientos diarios por lo cual puede anticipar dónde vas a ir a comprar hoy.

Los datos GPS de nuestro celular pueden ser una amenaza a nuestra privacidad, pero la vigilancia satelital es un problema mayor (23). En 2013, la policía de Grants Pass (eeuu), recibió un aviso de que un hombre llamado Curtis W. Croft cultivaba ilegalmente marihuana en su patio trasero. Para comprobarlo, utilizaron el servicio Google Earth. En efecto, la imagen del satélite que llevaba cuatro meses funcionando mostraba ordenadas filas de plantas que crecían en la propiedad de Croft. Los policías se dirigieron a ella e incautaron 94 plantas (24).

Captura de pantalla de un video del BeiDou Navigation Satellite System un sistema de vigilancia en tiempo real empleado por china.

Si bien tenemos algún control sobre el uso de dispositivos personales de vigilancia como smartphones y notebooks, la situación es algo más complicada cuando se trata de vigilancia satelital. Actualmente existen alrededor de 5000 satélites orbitando la tierra, 2000 de los cuales se encuentran activos controlados por estados y empresas transnacionales. Algunas compañías incluso ofrecen vídeos en directo desde el espacio ocupando satélites. En 2014, una *start-up* de Silicon Valley (eeuu) llamada SkyBox (que luego fue rebautizada como Terra Bella y comprada por Google y después por Planet) empezó a promocionar vídeos en tiempo real de alta definición de hasta 90 segundos de duración. Y una compañía llamada EarthNow asegura que ofrecerá monitorización “en tiempo real continuo, con un desfase de tan solo un segundo” (25). Si bien la resolución actual de las imágenes de satélites es de 25 cm (aproximadamente el tamaño de un zapato), los satélites militares de espionaje tienen una resolución aún mayor, pero el uso de esta información no es de acceso público.

Stuff in Space, el proyecto que visibiliza el enjambre de los cerca de 5000 satélites orbitando la tierra.

Desde el inicio de la pandemia han surgido en todo el mundo un gran número de proyectos que usan tecnologías Sistemas de Información Geográfica (SIG) como geoposicionamiento, *geofencing*, rastreo y registro de contactos a través de *bluetooth* , para generar una base de datos administrada por los gobiernos para enfrentar la crisis sanitaria (26). Mediante técnicas de análisis de datos masivos (*big data*) e inteligencia artificial se ha producido información para las instituciones sanitarias buscando así a afrontar de manera más eficiente la crisis sanitaria.

En la región chilena el Consejo para la Transparencia ha advertido de las consecuencias negativas que tiene el uso de la geolocalización, luego del anuncio de Enrique Paris de sumar a las compañías telefónicas a la labor de monitorear la movilidad de las personas que viven en comunas en cuarentena y además, realizar un seguimiento a los pacientes contagiados con coronavirus (27). Todo esto sumado al Estado de Excepción y toque de queda, con militares patrullando en las calles, además de la obligación de solicitar permisos en Comisarías Virtuales a la policía del estado de $hile para realizar actividades cotidianas como salir a comprar a la esquina o “pasear a la mascota”.

La pandemia ha propiciado una campaña de terror psicológico que busca aniquilar la voluntad, la dignidad, el tejido social y la capacidad de autodeterminación de un pueblo que hace poco más de un año perdió el miedo y se levantó en una insurrección popular que hizo temblar la institucionalidad de la región y la continuidad del modelo instaurado por Pinochet. Con personas como Bernardo Matte Larraín en su directorio, es esperable que empresas como Entel no duden en poner a disposición de la policía chilena toda su infraestructura de telecomunicaciones, como ya hicieron tras el estallido social, para perseguir y encarcelar a las personas consideradas una amenaza para un gobierno.

Militares patrullando las calles de una ciudad en la región chilena por toque de queda.

La geolocalización masiva de personas es una herramienta de control *a priori* extremadamente invasiva que puede vulnerar los derechos de protección de datos, así como producirse potenciales consecuencias adversas en caso de que dicha información sea objeto de algún ciberataque o pueda ser destinada a alguna finalidad diferente de la prevista. Las leyes actuales sobre privacidad se centran en las amenazas a los derechos de las personas. Pero según Nathaniel Raymond,

activista por derechos humanos y privacidadesas protecciones “son anacrónicas frente a la inteligencia artificial, las tecnologías geoespaciales y las tecnologías móviles” (28). Según Raymond, el problema sobre la vigilancia satelital y los alcances de la geolocalización “se trata nada menos que de el futuro de la libertad humana”.

5G: LA INFRAESTRUCTURA PARA EL IMPERIO TECNOCAPITALISTA CHINO

El rápido crecimiento de empresas chinas como Huawei y ZTE en Abya Yala y otras regiones del sur global ha llamado la atención de eeuu y la unión europea. Se han generado una serie de conflictos debido a lo que el ahora ex presidente de eeuu, Donald Trump considera una amenaza a la seguridad de su país, razón por la cual ha intentado boicotear en avance de estas empresas chinas frente a Google (29). Este conflicto con Huawuei ha reflotado la histórica rivalidad entre el estado chino y eeuu.

Sin embargo, existe otra batalla aún más estratégica: el 5G. El término 5G no es otra cosa que “quinta generación” de conectividad de internet móvil, la cual permitirá descargas mucho más rápidas, una cobertura mucho más amplia y conexiones más estables (30). Debido a su mayor ancho de banda, las nuevas redes no solo servirán a los teléfonos celulares como las redes actuales, sino que también podrá usarse como proveedores de servicios de internet para computadoras. Esto significa que también servirá para conectar automóviles y otros medios de transporte controlados por computadores, como barcos y aviones, además de redes de seguridad, medios de comunicación, casas inteligentes o incluso electrodomésticos. En definitiva: todos los sistemas y dispositivos que utilizamos diariamente.

¿Por qué genera polémica el control de la tecnología 5G? Antiguamente en período de guerras, los países cortaban la comunicación dinamitando puentes o atacando el suministro eléctrico de las ciudades atacadas. Hoy en día, la conexión a internet es el motor de los sistemas de comunicación y transporte. Controlar la infraestructura para la conexión a internet te entrega la facultad de espiar y eventualmente desconectar y simplemente paralizar una ciudad o un país entero. Si bien esta tecnología se está desarrollando también en Europa con empresas como Ericsson y Nokia, actualmente es el estado chino quien lleva la delantera. Eeuu y otras economías del Norte han desplegado campañas internas para evitar que países

occidentales implementen la tecnología del gigante asiático. Ejemplo de esto es la “alianza de inteligencia 5 ojos” (*Five Eyes*) con las regiones de canadá, nueva zelanda, australia y reino unido, quienes están intentando boicotear el avance del 5G chino en occidente, rememorando una verdadera nueva guerra fría del Big Data (31).

Las teorías conspiracionistas que asocian el 5G al origen de la pandemia Covid-19 han desviado la crítica que existe a las implicancias prácticas políticas y sociales sobre esta tecnología. El investigador Edward Bloom del Colectivo Rhizomatica plantea que la implementación del 5G no sólo implica la centralización de las comunicaciones a nivel global facilitando la vigilancia y el control social, sino que incluso podría empeorar la brecha digital (32).

Estado de licitaciones y operaciones para la instalación de 5G en Abya Yala.

En Abya Yala aún no comienza a instalarse esta tecnología, pero varios estados ya están en la fase de licitación, y a diferencia de los países del Norte Global, existe una gran receptividad hacia empresas chinas debido a la posibilidad de atraer inversionistas y mejorar las condiciones comerciales. Actualmente (2020) se está evaluando la implementación de 5G con los territorios controlados por los estados de méxico, brasil, uruguay, chile y argentina (33).

TECNOLOGÍAS DE VIGILANCIA EN LA REGIÓN CHILENA: CRIMINALIZACIÓN DE LA CIBERSEGURIDAD Y MODERNIZACIÓN DEL SISTEMA DE INTELIGENCIA NACIONAL

Image not found or type unknown

En abril del 2019, Piñera junto a Andrés Chadwick, impulsaron el proyecto “Sistema de Vigilancia Móvil” para combatir la delincuencia. El proyecto se enmarca en el programa de Innovación Tecnológica de la Subsecretaría de Prevención del Delito y consiste en el uso de sistemas de aeronaves remotamente piloteadas RPAS, por sus siglas en inglés: *Remotely Piloted Aircraft* (34).

Los 30 drones marca DJI, modelo Matrice210, se encuentran equipados con

cámaras de alta definición para obtener información visual y transmitirla en vivo a centrales de monitoreo ubicadas en las intendencias regionales. Vuelan a unos 120 metros de altura, asimilan a un araña de 4 patas. Cuentan con softwares de reconocimiento facial y de patentes, pudiendo identificar a personas o vehículos desde más de 300 metros de distancia. Además sus cámaras cuentan con tecnología de visión nocturna y detección térmica. Actualmente son pilotados por carabineros y la información que captan es analizada y registrada además de las intendencias, en la Central de Comunicaciones de Carabineros (Cenco).

A inicios del 2020 la misma Subsecretaría de Prevención del Delito licita el Sistema de Teleprotección a nivel nacional por más de 13 mil millones de pesos, comprometiendo la instalación de 1000 nuevas cámaras de vigilancia equipadas con tecnología de punta, con modelos PTZ, PanoVu (360º) y cámaras fijas de reconocimiento facial, integrándose a las cerca de 4000 cámaras ya existentes en el territorio (35).

Algo similar se puede observar en los territorios controlados por los Estados de Argentina, Paraguay y Brasil. Este último realizó recientemente una inversión de 13 millones de dólares en la instalación de un sistema de cámaras con reconocimiento facial en la ciudad de Sao Paulo, pese a la creciente presión por parte de organizaciones civiles para regular la gestión y transparencia en el uso de la información biométrica recolectada (36).

En nuestro territorio, la licitación del sistema de Teleproteción fue adjudicada por la empresa china Hikvision, misma empresa de vigilancia acusada por Human Rights Watch de persecusión política a musulmanes en Xinjiang. Las nuevas cámaras serán administradas por 87 centrales ubicadas en intendencias, comisarías y municipalidades de todo el territorio. Con estos proyectos de modernización del Sistema de Inteligencia Nacional, la entralización en un sistema integrado con reconocimiento facial y el uso de nuevas tecnologías para la vigilancia nos hacen pensar en el surgimiento de una versión local de la IJOP china. Actualmente se siguen desarrollando proyectos que apuntan a modernizar, centralizar y mejorar la infraestructura para la vigilancia y el monitoreo en tiempo real, como el proyecto *Santiago Smart City*, también conocido como panóptico, que pretende construir un centro de operaciones subterráneo que busca integrar información proporcionada por aplicaciones como Waze y las redes de cámaras de vigilancia de la ciudad (37).

Meses después, en medio de la revuelta popular y el inicio de una pandemia global,

el gobierno de Piñera impulsa un proyecto de modernización de la ANI, el Sistema de Inteligencia Nacional. Estas modificaciones permiten que las “Unidades de Inteligencia de las Fuerzas Armadas procedan a seguimientos y control sobre grupos nacionales que a criterio de la autoridad atenten contra la seguridad interior del estado” (38). Se limita el control del Congreso sobre la ANI; se otorga un gran presupuesto público para la ejecución, y por último se crea un Consejo Asesor electo por el presidente (39).

Gafas de escaneo térmico Rokid Glass T2 utilizadas por la policía chilena.

Esto se suma a la tramitación del TPP-11, y el Proyecto de Ley de Delitos Informáticos, ambos enmarcados en tratados y convenios internacionales como el Convenio de Budapest del Consejo Eurupeo, del cual el Estado de $hile es parte. El primero, un tratado internacional negociado inicialmente en secreto entre estados y empresas transnacionales, busca facilitar la obtención de información personal y acceso a dispositivos de “presuntos infractores” de las normativas de derechos de autor (art. 18.74 13), obliga a los países a permitir la transferencia de datos personales a empresas transnacionales (40). Además criminaliza publicaciones periodísticas o filtraciones que revelen secretos comerciales, como WikiLeaks, blindando de esta forma a las grandes corporaciones en casos de colusión.

El Proyecto de Ley de Delitos Informáticos por otra parte, bajo el argumento de fortalecer los sistemas de ciberseguridad del país, busca facilitar a la policía el acceso de la información en procesos de investigación. Tipifica conductas de “falsificación informática y la encriptación de la comunicación”. De aprobarse este proyecto de ley, afectaría directamente a la privacidad de las personas y a su capacidad para proteger su información, transformando la privacidad y la seguridad digital en un delito potencial (41).

La sucesión de estas reformas y el volumen de inversión en materia de vigilancia en sólo dos años dan cuenta de la creciente importancia que tiene este tema en la agenda política de gobiernos de la región. Casos como Operación Huracán y PacoLeaks en la región chilena reflejan cómo la policía ha utilizado tecnologías de vigilancia para realizar montajes y persecusión política. El problema que enfrentamos ante esta propuesta es que al abarcar tan ampliamente la actividad digital exclusivamente desde una ley penal, la ciberseguridad queda reducida a una tarea de persecución y castigo. En marzo de 2020, Carlos Saavedra, rector de la corporación Universidad de Concepción, realizó una querella contra 12

manifestantes y facilitó a la PDI más de 250 horas de grabación de las cámaras de vigilancia instaladas en el campus, facilitando la identificación y posterior encarcelamiento de estas personas, incluyendo a 5 niñes y adolescentes (42).

En definitiva, estamos experimentando la etapa inicial de la implementación de un sistema sin precedentes de vigilancia y control social en este territorio, en donde los estados y sus policías han comenzado a utilizar las más avanzadas herramientas tecnológicas para la represión y persecusión política. El estado chino aparece como un referente y como proveedor de tecnología para regiones importantes de Abya Yala, en un momento crítico para los gobiernos de la región, que frente a la crisis del capitalismo extractivista enfrentan hoy la mayor oleada de protestas e insurrecciones populares registradas en las últimas décadas.

UTOPÍAS PIRATAS: REFLEXIONES FINALES HACIA UNA AUTODEFENSA DIGITAL

> *Los piratas y corsarios del siglo xviii crearon una «red de información» que envolvía el globo: primitiva y dedicada primordialmente a negocios ilegales, la red funcionaba admirablemente. Repartidas por ella había islas, remotos escondites donde los barcos podían ser aprovisionados y cargados con los frutos del pillaje para satisfacer toda clase de lujos y necesidades. Algunas de estas islas mantenían «comunidades intencionales», una verdadera red mundial de agrupaciones invisibles que vivían conscientemente fuera de la ley y mostraban determinación a mantenerse así, aunque fuera sólo por una corta -pero alegre- existencia*.
>
> Zona Temporalmente Autónoma, Hakim Bey.

La reciente polémica por la política de privacidad de Whatsapp ha desencadenado una serie de debates sobre la importancia de la ciberseguridad y el rol de las corporaciones en el uso de la tecnología y la información personal. Lo que comenzó como una forma sofisticada de mostrarnos publicidad en internet, se está transformando en una herramienta política sin precedentes para los Estados, que utilizan estas tecnologías para la vigilancia, la represión y el control social.

Esto ocurre en un contexto local de revuelta y pandemia. La vigilancia satelital, la geolocalización vía GPS y la creciente inversión en infraestructura y tecnologías

para la vigilancia son la expresión de un estado policial que busca un mayor control social. Las excusas de la gestión de una crisis sanitaria y el mito neoliberal de la “seguridad ciudadana” son utilizadas para vulnerar el principio de inocencia del sistema penal al someter a la población a la constante mirada vigilante y omnipresente de la policía, facilitada por la tecnología.

Al mismo tiempo, en la región chilena se impulsan leyes represivas y dispositivos jurídicos para la persecusión política y la potencial criminalización de “ciudadanos peligrosos”. La modernización de la ANI, la Ley de Delitos informáticos y el TPP-11 buscan sentar bases institucionales para la implementación de sistemas de vigilancia. Estas iniciativas reflejan el rol del Estado como el brazo armado del Capital transnacional, utilizando el monopolio de la fuerza, la diplomacia de los tratados internacionales y el blindaje jurídico para facilitar el saqueo extractivista en la región.

Actualmente avanzamos en todo el mundo hacia sociedades de vigilancia total que nos recuerdan la distopía Orwelliana de 1984. Las grandes potencias se disputan la infraestructura y el control de la información, siendo el 5G la última de sus manifestaciones. Desde dispositivos móviles, micrófonos, cámaras de celulares y notebooks hasta drones y satélites, todos tributan a una red global de información al servicio de las grandes corporaciones y de los Estados más poderosos. El propósito es claro: el control del Big Data y la infraestructura de las comunicaciones permitirá a los gobiernos totalitarios saber virtualmente todo lo que hacen todas las personas en todo momento, en cualquier parte del mundo.

“Nada está fuera de nuestro alcance” Logo del satélite estadounidense USA-247, también llamado NROL-39. Fue puesto en órbita el 6 de diciembre de 2013..

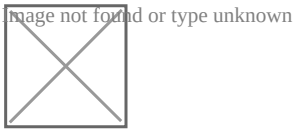
Donde hay poder hay resistencia. Hoy nos encontramos en una etapa de transición en la cual mantenerse informades y desarrollar una posición crítica resulta fundamental para anticiparnos a lo que viene. Las organizaciones civiles con enfoque de derechos han denunciado públicamente el sistema de videovigilancia por reconocimiento facial y la geolocalización como contrario a los derechos humanos, a la ley, a la constitución, y a los pactos internacionales de derechos civiles y políticos. Frente a esto han realizado campañas para solicitar mayor regulación e impulsar una reforma a la normativa sobre protección de datos personales, un debate democrático en el Congreso previo a la implementación de esta tecnología y solicitando aumentar la fiscalización por parte de autoridades estatales de control,

apelando a una reforma de los programas policiales de vigilancia. Sin embargo estas iniciativas parten de la premisa de que el propósito del estado es protegernos.

Desde una perspectiva ácrata, apuntamos a la organización y a la autodefensa digital como la mejor forma de enfrentar el asedio de vigilancia masiva por parte de los estados totalitaristas. Millones de personas alrededor del mundo están desarrollando colaborativamente sistemas operativos, navegadores y softwares que protegen nuestros datos de los gobiernos y las empresas, utilizando código abierto y los principios del software libre.

Navegadores y sistemas operativos de Software Libre.

Colectivos como RiseUp ofrecen aplicaciones y servicios de correo, VPN y almacenamiento seguro de datos, sustentados en los principios del software libre y el establecimiento de una red internacional de colaboración y comunicación entre experiencias y proyectos antiautoritarios. En la región chilena, grupos como el Colectivo Disonancia proporcionan información y material educativo totalmente gratuito sobre criptografía digital o cómo cifrar nuestras comunicaciones (43).



Existe una larga lista de aplicaciones y sistemas operativos disponibles para organización y comunicación cifrada. Motores de búsqueda como DuckDuckGo que no almacenan la información del usuario. Redes sociales como Mastodon y Diaspora o Jitsi son alternativas a Facebook, Twitter y Zoom. Aplicaciones de mensajería cifrada y de código abierto como Signal, Telegram o Briar se han vuelto cada vez más populares. El principal problema es el monopolio de las redes sociales y aplicaciones de mensajería de las grandes empresas transnacionales. Una red social no funciona sin personas. Sin embargo, no debemos subestimar el poder de la contrainformación y la capacidad de las personas de cambiar sus hábitos en el uso de tecnologías cuando alguien se da el tiempo de explicarles las implicancias de esta decisión: luego de la polémica por las políticas de privacidad, Telegram tuvo 25 millones de descargas en todo el mundo, en sólo 72 horas (44).

Maquillaje anti-reconocimiento facial: se prioriza distorsionar la simetría de la cara y puntos de referencia utilizados por softwares como ojos, cejas, nariz y boca.

Al mismo tiempo, artistas y diseñadores han desarrollado técnicas y dispositivos *Do It Yourself* para hackear el reconocimiento facial: maquillajes, joyas y jockeys con luces led (45). Otras personas han diseñado vestuario y estuches para celulares que impiden el rastreo satelital de celulares por GPS (46). Colectivos anarquistas y antidesarrollistas en la región europea están implementando el proyecto *Low Tech Magazine,* realizando tutoriales para implementar una red de internet autónoma con infraestructura de baja tecnología (47), además de redes de pares o P2P, que implican una participación colectiva en cómo se organiza la comunicación en línea (48). Grupos de economía social y solidaria en distintas regiones están utilizando blockchain y aplicaciones móviles de código abierto para realizar intercambios comerciales con moneda social, una forma de economía comunitaria anticapitalista (49). En 2018, una empresa de cartografía rusa hizo desaparecer los sitios de operaciones militares sensibles en Turquía e Israel, lo que acabó revelando su existencia e impulsó a algunos usuarios a localizar estos sitios en otros mapas de código abierto (50). En la región chilena, el grupo Evade la Vigilancia realizó un mapeo de las cámaras de vigilancia en el territorio con la plataforma *uMaps* basada en *Open Street Maps*, una plataforma gratuita, colaborativa y de código abierto (51).

Instalación de una antena de internet de baja tecnología en Berlin.

El capitalismo, en la medida en que adquiere mayores niveles de complejidad y dificultad para administrar sus contradicciones internas y el malestar latente, ha comenzado a implementar mecanismos de control social cada vez más eficientes, utilizando los últimos avances científicos y tecnológicos e impulsando a su vez el desarrollo de nuevas tecnologías con esta finalidad. El estado china es hoy la principal manifestación de esta forma de capitalismo, y su camino a controlar la infraestructura de comunicaciones en Abya Yala está pavimentado representando una importante amenaza a la autonomía de la región.

Lásers utilizados para cegar a la policía y cámaras de vigilancia, utilizados durate una protesta en Santiago, Cuenca del Maipo

Cuando la empresa de navegación asistida *Waze* de Google prohibió reportar controles policiales en las ciudades, la gente comenzó a reportarlos como “animales

muertos". Debemos aprovechar la inteligencia colectiva para utilizar las mismas tecnologías en nuestro beneficio. La adaptabilidad de nuestra especie a estas nuevas formas de represión parece necesaria, y los planteamientos teóricos del transhumanismo parecen coherentes. Sin embargo tenemos que considerar que no son aplicables en todos los contextos, como en zonas del no-ser, regiones del Sur Global devastadas por la guerra, el totalitarismo y el necrocapitalismo. Aprender nociones básicas sobre *baja* tecnología y computación permitiría fortalecer una red de agrupaciones invisibles como foros y comunidades internacionales compartiendo información de forma invisible a la vigilancia del Capital-estado gracias a plataformas de videollamada como Jitsi desarrolladas por personas anónimas que deciden colaborar en ello como forma de resistencia política pero no es una solución para todes.

Dmytri Kleiner, activista por el software libre, planteaba que los hackers no pueden solucionar el problema de la vigilancia: "La vigilancia masiva y el control social no son un problema técnico que requiera más expertes en programación ni en ingeniería: sólo a través de la vinculación con movimientos sociales y su organización podemos enfrentarlo" (52). Esto nos lleva a pensar en lo que Silvia Rivera Cusicanqui planteaba como la necesidad de desarrollar una *ética india* y una *técnica occidental.*

Grupo Solenopsis

gruposolenopsis[arroba]riseup.net

Walüng, 2021

Cuenca del Maipo, región chilena

NOTAS Y REFERENCIAS

1 https://www.whatsapp.com/legal/updates/privacy-policy/?lang=es

2 https://www.interior.gob.cl/noticias/2019/03/18/sistema-de-televigilancia-movil-se-implementa-en-la-region-metropolitana/

3 https://www.ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/

4 https://www.latercera.com/la-tercera-domingo/noticia/martin-hilbert-experto-en-redes-digitales-los-algoritmos-encontraron-nuestras-debilidades-y-las-estan-aprovechando

5 https://www.nytimes.com/es/2018/07/13/espanol/china-reconocimiento-facial.html

6 https://www.hrw.org/es/news/2005/04/12/china-represion-religiosa-de-musulmanes-uigur

7 https://www.lavanguardia.com/cribeo/geek/20190720/47437837351/una-ciudad-china-reparte-16-000-smartwatches-con-gps-integrado-para-controlar-a-los-estudiantes.html

8 http://drrajivdesaimd.com/2018/12/03/facial-recognition-technology/

9 https://designthinking.gal/eye-tracking-que-es-y-para-que-sirve/

11 Un caso emblemático fue cuando el FBI solicitó a Apple acceso a toda la información de los dispositivos personales de Syed Rizwan, un hombre acusado de asesinar a una persona en San Bernardino. Cualquier gobierno puede forzar a Apple a facilitar información para identificar a una persona argumentando motivos de investigación, transformándola en una empresa muy atractiva para los gobiernos que pretenden avanzar en un nuevo orden de vigilancia masiva. Si bien Facebook tiene un poderoso sistema de reconocimiento facial, y se complementa con otras aplicaciones como Instagram y Whatsapp, no controla los hardwares de las cámaras y micrófonos de los dispositivos como celulares, tablets y notebooks que nos observan y escuchan diariamente. Apple en cambio cuenta con un sistema unificado de reconocimiento facial integrado en algunos de los dispositivos más populares del mundo: iPhones, iPads y Macs, el hardware que faltaba para escanear e identificar caras alrededor del mundo y almacenar toda esa información en una sola empresa.

12 Google ha sido criticada por colaborar con determinados países en la censura de Internet con el afán de expandirse comercialmente en ellos y por la infracción reiterada de derechos de autor. También es objeto de críticas por presunta ingeniería fiscal en diferentes países, y por ser una de las empresas que colaboran

con las agencias de inteligencia en la red de vigilancia mundial, sacada a la luz en 2013).

13 http://repositorio.uchile.cl/bitstream/handle/2250/146569/Videovigilancia-en-el-espacio-p%C3%BAblico-el-monitoreo-de-la-ciudad-como-dispositivo-del-control-poblacional.pdf?sequence=1&isAllowed=y

14 https://www.eldiario.es/tecnologia/limites-estadisticos-vigilancia-masiva_0_963804507.html

15 https://www.derechosdigitales.org/wp-content/uploads/glimpse-2019.pdf

16 https://scielo.conicyt.cl/pdf/rchdt/v6n1/0719-2584-rchdt-6-01-00067.pdf

17 https://www.sas.com/es_cl/insights/big-data/what-is-big-data.html

18 https://core.ac.uk/download/pdf/141667769.pdf

19 https://www.researchgate.net/publication/37707311_Technocapitalism_A_Critical_Perspectiv

20 https://www.bbc.com/mundo/noticias-47331817

21https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-43602015000100014

22 Alphabet Inc. es un conglomerado, servicios como Google Maps o Gmail entre muchos otros; Calico, compañía biotecnológica de South San Francisco, California, que diseña y fabrica termostatos y detectores de humos impulsados por sensores, habilitados para Wi-Fi, autoaprendientes y programables; GV (anteriormente Google Ventures); Google X, división de investigación y desarrollo de nuevos productos; y Sidewalk Labs, que investigará sobre cómo mejorar ciudades para elevar la calidad de vida).

23 La humanidad ha enviado alrededor de 9 mil satélites al espacio desde 1957, de los cuales alrededor de 5 mil todavía están en el espacio, y solo alrededor de 2 mil están en funcionamiento. SpaceX la empresa de Elon Musk ha puesto en órbita recientemente 180 nuevos satélites y planean poner 12 mil más durante lospróximos diez años.

24 https://www.technologyreview.es/s/11282/si-no-regulamos-las-imagenes-de-satelite-nos-vigilaran-las-24-horas

25 https://www.bbc.com/mundo/noticias/2014/05/140516_tecnologia_satelites_caja_zapatos_m

26 https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/79450

27 https://www.latercera.com/nacional/noticia/cplt-plantea-dudas-sobre-geolocalizacion-y-monitoreo-de-movilidad-durante-la-pandemia-autoridades-no-pueden-utilizar-este-tipo-de-informacion-sin-consentimiento/RU4EZNKDUNHDXLWLNDP5WWUN6Q/

28 https://www.technologyreview.es/s/11282/si-no-regulamos-las-imagenes-de-satelite-nos-vigilaran-las-24-horas

29 https://www.bbc.com/mundo/noticias-48372800

30 https://www.voanoticias.com/tecnologia-ciencia/cosas-que-debemos-saber-de-china-america-latina-y-5g

31 https://www.bbc.com/mundo/noticias-47331817

32 https://www.rhizomatica.org/la-tecnologia-5g-no-reducira-la-brecha-digital-y-podria-incluso-empeorarla/

33 https://www.bbc.com/mundo/noticias-55352307

34 https://www.interior.gob.cl/noticias/2019/03/18/sistema-de-televigilancia-movil-se-implementa-en-la-region-metropolitana/

35 https://interferencia.cl/articulos/prevencion-del-delito-adquiere-mil-camaras-de-televigilancia-cuestionadas-por

36 https://www.derechosdigitales.org/14207/la-sociedad-exige-explicaciones-sobre-la-implementacion-de-sistemas-de-reconocimiento-facial-en-america-latina/

37 https://www.eldesconcierto.cl/2020/04/15/intendente-guevara-pidio-7-000-millones-para-un-centro-de-vigilancia-tecnologica-en-el-subterraneo-de-la-intendencia/

38 Nota: Los seguimientos por Inteligencia no son una cosa nueva, ya que en octubre del año pasado se filtraron 15 gigas de información de Carabineros del departamento de Inteligencia, dejando en evidencia el espionaje policial sobre distintos movimientos y organizaciones sociales y sus dirigentes, conglomerado en el famoso caso *PacoLeaks*.

39 https://www.ciperchile.cl/2020/06/16/mas-poder-para-el-presidente-nudos-criticos-del-proyecto-que-moderniza-el-sistema-de-inteligencia/

40 https://colectivodisonancia.net/2019/03/no-al-tpp11/

41 https://www.senado.cl/delitos-informaticos-y-ciberseguridad-proyecto-que-actualiza/senado/2020-03-05/175410.html

42 https://resumen.cl/articulos/emplazan-al-rector-de-la-universidad-de-concepcion-a-retirar-querella-contra-manifestantes-detenidos-por-protestas-en-la-casa-de-estudios

43 https://colectivodisonancia.net/

44 https://www.technologyreview.es/s/11282/si-no-regulamos-las-imagenes-de-satelite-nos-vigilaran-las-24-horas

45 https://umap.openstreetmap.co/en/map/ubicacion-de-camaras-de-vigilancia-en-chile_2598#4/-38.34/-71.46

46 https://www.dw.com/es/telegram-gana-25-millones-de-usuarios-en-72-horas/a-56211248

47 https://blogs.publico.es/strambotic/2019/10/burlar-reconocimiento-facial/

48 https://cnnespanol.cnn.com/2012/04/29/como-enganar-a-la-tecnologia-de-reconocimiento-facial/

49 https://solar.lowtechmagazine.com/es/2015/10/how-to-build-a-low-tech-internet.html

50 https://colectivodisonancia.net/autonomia/redes-p2p/

51 https://monedapar.com.ar/funcionamiento-del-sistema/

52 https://colectivodisonancia.net/2020/11/un-desafio-colectivo-para-enfrentar-la-vigilancia/

LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ

Fotografia: La peste

Fecha de creación
2021/01/28