Hipervisible

Sobre cámaras de red y sociedades de control[1]

Hypervisible

About network cameras and Societies of Control

Hipervisível

Sobre câmeras de rede e sociedades de controle

DOI: https://doi.org/10.18861/ic.2024.19.2.3725

▶ AGUSTINA LAPENDA

amlapenda@gmail.com – Ciudad Autónoma de Buenos Aires – Universidad Nacional de San Martín, Argentina.

ORCID: https://orcid.org/0000-0002-3137-1547

CÓMO CITAR: Lapenda, A. (2024). Hipervisible. Sobre cámaras de red y sociedades de control. *InMediaciones de la Comunicación, 19*(2). DOI: https://doi.org/10.18861/ic.2024.19.2.3725

Fecha de recepción: 20 de febrero de 2024
Fecha de aceptación: 19 de junio de 2024

RESUMEN

Este artículo reflexiona críticamente sobre el uso de cámaras de red como tecnologías de vigilancia en el contexto de las actuales sociedades de control. El análisis se desarrolla a través de la práctica de observación y recopilación de imágenes provenientes de dispositivos de vigilancia que se transmiten en línea de forma desprotegida. Si estas cámaras no se aseguran debidamente, pueden ser vistas e incluso operadas en forma remota por cualquier persona o robot que esté conectado a Internet. De allí que sus transmisiones puedan ser objeto de usos no previstos e intervenciones anónimas de diversa índole. El trabajo dialoga con estudios clásicos y contemporáneos sobre el tema e indaga el funcionamiento técnico de estos dispositivos, su relación con las prácticas de vigilancia y los discursos de seguridad contemporáneos, su exposición en Internet y el potencial político derivado de los riesgos que promueve su vulnerabilidad.

PALABRAS CLAVE: *cámaras de red, vigilancia, sociedad de control, Internet, seguridad.*

ABSTRACT

This article discusses the use of network cameras as surveillance technologies in the context of today's control societies. The analysis is through the practice of observation and collection of images from surveillance devices that are transmitted online in an unprotected way. If these cameras are not properly secured, they can be viewed and even operated remotely by any person or robot connected to the Internet. Hence, their transmissions can be subject to unintended uses and anonymous interventions of various kinds. The work dialogues with classic and contemporary studies on the subject and investigates the technical functioning of these devices, their relation with surveillance practices and contemporary security discourses, their exposure on the Internet and their political potential derived from the risks promoted by their vulnerability.

KEYWORDS: *network cameras, surveillance, Society of Control, Internet, security.*

1 Una versión previa de este trabajo fue presentada en las "XV Jornadas de la Carrera de Sociología" realizadas en la Universidad de Buenos Aires en 2023.

RESUMO

Este artigo reflete criticamente sobre o uso de câmeras de rede como tecnologias de vigilância no contexto das atuais *sociedades de controle*. A análise é desenvolvida através da prática de observação e coleta de imagens de dispositivos de vigilância que são transmitidas online de forma desprotegida. Se essas câmeras não estiverem devidamente protegidas, pode ser visto e até mesmo operado remotamente por qualquer pessoa ou robô conectado à Internet. Assim, as suas transmissões podem estar sujeitas a utilizações imprevistas e intervenções anónimas de vários tipos. O trabalho dialoga com estudos clássicos e contemporâneos sobre o assunto e indaga o funcionamento técnico desses dispositivos, sua relação com as práticas de vigilância e discursos de segurança contemporâneos, sua exposição na Internet e o potencial político derivado dos riscos promovidos pela sua vulnerabilidade.

PALAVRAS-CHAVE: *câmeras de rede, vigilância, sociedade de controle, Internet, segurança.*

1. INTRODUCCIÓN: ¿POR QUÉ PUEDO VER ESTAS IMÁGENES?

"Sentada frente al ordenador,
siento los músculos de la espalda inervados por un cable cibernético
que crece desde el suelo de la ciudad y sale por mi cabeza
hasta engancharse a los planetas más alejados de la Tierra".

Beatriz Preciado (2014)
Testo yonqui

El empleo de *cámaras de red* –también llamadas *cámaras Internet Protocol* (IP)– en prácticas de vigilancia de espacios y sujetos se ha vuelto un fenómeno frecuente dentro de nuestras *sociedades de control* (Deleuze, 2006)[2]. Dispositivos de esta clase se utilizan a diario para monitorear personas, calles, plazas, transportes públicos, gimnasios, el interior de un bar, la entrada de un hotel o, incluso, nuestra propia casa. A menudo, quienes se sirven de estas cámaras desconocen sus implicancias: dada su conexión a redes de datos y su indexación en buscadores en línea, las imágenes que transmiten –si no se protegen– pueden ser vistas y hasta manipuladas en remoto por cualquier persona o robot que esté conectado a Internet. Es decir, ciertos modos de uso de estas tecnologías comportan inseguridades y fugas de información que son poco difundidas por sus fabricantes o ignoradas por quienes las emplean. De ese modo, aquello que fue adoptado como medida de protección puede volverse un riesgo.

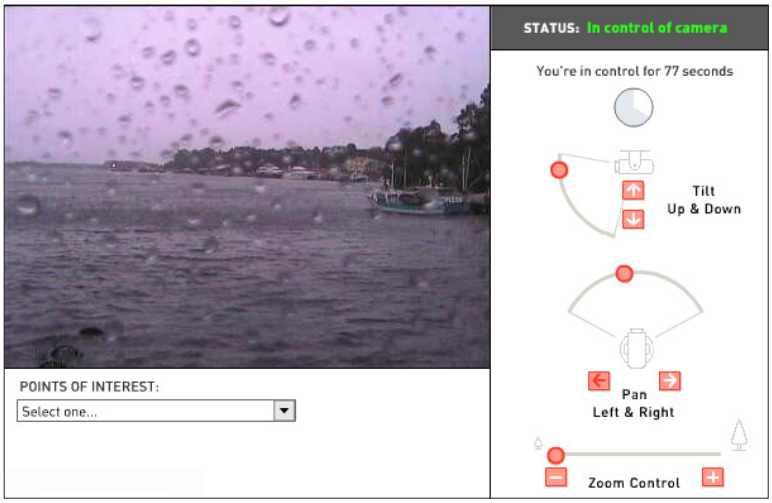
En ese marco, el artículo propone una reflexión crítica sobre las prácticas de videovigilancia contemporáneas por medio de imágenes provenientes de cámaras de red expuestas: es decir, que transmiten en línea de manera desprotegida o sin contraseñas. El abordaje de este objeto de estudio se inició una década atrás a partir de la observación de transmisiones en vivo de cámaras públicas de carácter turístico o comercial emplazadas en distintos lugares del mundo. A través de estos dispositivos, y por varios meses, capturé paisajes, personas y situaciones que acontecían simultáneamente en mi pantalla y, tan próximas como distantes, en otros puntos del planeta: madrugadas en un caserío de la Antártida, tormentas en Australia (Imagen 1), amaneceres en una playa de Francia, autopistas en Estados Unidos, calles en China, antílopes africanos, árboles japoneses[3].

2 Siguiendo a Deleuze (1990), quien en el artículo "Posdata sobre las sociedades de control" amplía la conceptualización de Michel Foucault sobre las *sociedades disciplinarias* y propone referirse a las *sociedades de control*, Pablo Rodríguez (2008) sintetiza el planteo deleziano diciendo que el control, en esta nueva concepción postdisciplinaria, "no necesita de la modalidad del encierro, como ocurre con la disciplina, para ejercer la vigilancia sobre los sujetos", dado que en las sociedades de control la vigilancia "está más relacionada con tecnologías que con instituciones, al punto que las primeras rompen los tabiques de las segundas (…). Hoy la vigilancia ha podido soltarse del amarre institucional y reconfigura el paisaje de la disciplina" (pp. 1 y 2).

3 En aquel entonces, cuando la videovigilancia se encontraba menos extendida que en el contexto actual, mis inquietudes e interrogantes orbitaban sobre el problema de la autoría de dichas capturas: ¿Quién era el autor/a de esas imágenes? ¿Pertenecían a quienes habían emplazado y puesto en funcionamiento las respectivas cámaras de video? ¿En qué sentidos se reformula la relación tradicional entre autoría/obra con la irrupción de Internet?

InMediaciones de la Comunicación 2024 - VOL. 19 / Nº 2 - ISSN 1510-5091 - ISSN 1688-8626 (EN LÍNEA) - MONTEVIDEO (URUGUAY)

Imagen 1. Panel de control y transmisión de cámara de red en Australia



Fuente: captura de pantalla, 28 julio 2014, 21:14hs. (arg) – 11:14hs. (aus).

En 2021, la virtualización forzada por la pandemia y el encierro fruto de las "medidas biopolíticas de gestión del contagio impuestas frente al coronavirus" (Preciado, 2020, s/p) abrieron una vía de retorno a esos dispositivos productores de representaciones y subjetividades. La pantalla volvió a poblarse de transmisiones de territorios, cuerpos e instantes foráneos, aunque, esta vez, con otras motivaciones e interrogantes.

Entre ambos actos de observación –aquel realizado en 2014 y el reanudado en el marco de las nuevas preguntas sobre el carácter técnico de esas imágenes y sus implicancias sociales y políticas–, el uso de estos aparatos se incrementó exponencialmente y el trabajo se reenfocó en transmisiones de cámaras instaladas con fines de vigilancia. Escenas extraídas de su fuga incesante por lentes, redes, conectores y pantallas (Imagen 2): ¿por qué es posible acceder a estas imágenes? A través de las capturas seleccionadas como corpus y el diálogo con referentes clásicos y contemporáneos que abordan cuestiones afines a la problemática, se exponen en este artículo algunas ideas sobre las condiciones de existencia de esas representaciones, su visibilidad y las vulnerabilidades técnicas de las cámaras que las producen en el contexto de las sociedades de control.

Imagen 2. Transmisión de cámara de red en Noruega

Fuente: captura de pantalla, 12 mayo 2021, 22:27hs. (arg) – 13 mayo 2021, 03:27hs. (nor).

La primera parte del análisis se centra en las características técnicas de dichos dispositivos de video, la forma en que transmiten imágenes mediante redes de datos, su indexación en motores de búsqueda en línea y su modo de funcionamiento. Es decir, cómo los registros captados por esas cámaras de red pueden llegar a ser rastreables y visibles por cualquiera que disponga de una conexión a Internet, y cómo ese compendio de elementos y procesos se enlaza con sistemas más extensos de extracción y gestión de datos.

Luego, se aborda el empleo de cámaras de red como tecnologías de vigilancia, el vínculo de estos aparatos con la idea y los discursos de seguridad, y los riesgos que pueden derivarse de su uso desinformado y/o desprotegido.

Finalmente, se analiza un conjunto de intervenciones realizadas por individuos anónimos sobre las transmisiones en línea de estos dispositivos a raíz de su exposición pública en la red. Estas acciones suponen una alteración en el flujo de imágenes emitido por las cámaras y traen a la superficie su carácter vulnerable. En función de eso, se identifica la dimensión política que pueden asumir las imágenes –y los actos sobre ellas– en el contexto contemporáneo.

El análisis se desarrolla en base a la práctica de observación y captura de imágenes provenientes de cámaras de red, su cuestionamiento y la puesta en relación con estudios sobre las *sociedades postdisciplinarias*, sus mecanismos de control social, el rol de las imágenes y la videovigilancia. El corpus total de capturas recopilado a lo largo de los años es significativamente más extenso que el aquí publicado y su selección ha estado regida por la relación de las imágenes con las conceptualizaciones y los argumentos expuestos en el artículo.

2. DE UNA CÁMARA A LA PANTALLA: PROTOCOLOS, DATOS Y MOTORES DE BÚSQUEDA

En términos informáticos, los protocolos son conjuntos de reglas que rigen la comunicación y transmisión de datos entre distintos dispositivos o sistemas[4]. El *Protocolo de Internet* (IP, por sus siglas en inglés) "es quizás el más importante para el funcionamiento global de Internet en general, ya que es el responsable de hacer llegar los datos de un *host* [anfitrión] a otro" (Hall, 2000, p. 32)[5]. Las cámaras de red se sirven de dicho protocolo –motivo por el que también se las denomina cámaras IP– para transferir video mediante redes de datos cableadas o inalámbricas[6].

Estos dispositivos cuentan con su propia dirección IP[7] y pueden ponerse en funcionamiento en cualquier ubicación donde exista una conexión de red. Mediante esta última es posible observar en forma remota y en tiempo real las imágenes audiovisuales registradas por la cámara. El acceso a ellas puede ser restringido sólo a personas autorizadas. Pero si no se cifra la información transmitida por el aparato, quedará accesible a terceros: breves combinaciones de operadores de búsqueda avanzados ingresados en *Google*, unos pocos clics y un *CAPTCHA* (*Completely Automated Public Turing test to tell Computers and Humans Apart*) que determina si somos seres humanos o máquinas, es la distancia que nos separa de aquello que acontece en el campo visual de estas cámaras (Imagen 3).

Este procedimiento de rastreo de cámaras en línea puede ser automatizado y efectuado a gran escala por medio de *scripts*. Así, algunos foros y páginas web –*EarthCam, Insecam, IP24*, entre otras– recopilan y exhiben numerosas transmisiones en vivo, públicas o desprotegidas, organizadas según criterios diversos (emplazamiento, contenido de las transmisiones, fabricante de las cámaras, etc.)[8].

4 Según Alexander Galloway (2004), "el protocolo es a las sociedades de control lo que el panóptico a las sociedades disciplinarias" (p. 13); es decir, es el modo de existencia del control luego de la "descentralización" (p. 147). Para este autor, el protocolo delimita el campo de juego para lo que puede ocurrir. Si se ignora un determinado protocolo, la comunicación en ese canal será inviable: "Sin protocolo, no hay conexión" (p. 167).

5 "Is perhaps the most important to the overall operation of the Internet in general, since it is responsible for getting data from one host to another" (Hall, 2000, p. 32). [Todas las traducciones son de la autora de este artículo].

6 Conectada a Internet en 1991 por Quentin Stafford-Fraser y Paul Jardetzky, *The Trojan Room Coffee Pot* fue la primera cámara del mundo habilitada para la web. Apuntaba a una cafetera ubicada en la sala "Trojan" del Laboratorio de Computación de la Universidad de Cambridge, proporcionando una imagen en vivo del artefacto –de 128x128 píxeles y escala de grises– a todas las computadoras de escritorio en la red. Su propósito era mostrar si había café hecho en la cafetera a quienes trabajaban lejos de la sala. La transmisión se actualizaba unas tres veces por minuto. La última imagen captada por el dispositivo –el 22 de agosto de 2001 a las 10:54hs.– muestra unos dedos a punto de desconectar el servidor que alojaba la cámara. Aunque esta no era en sí misma una cámara IP, sino una cámara de video conectada a una computadora que transmitía las imágenes a través de la red local de la universidad, su modo de funcionamiento sentó las bases para la tecnología de las cámaras que aquí nos competen. En tal sentido, se la considera una precursora de aquellas dado que habilitó la visualización remota de imágenes en tiempo real mediante una red de datos. Harun Farocki (2015), por su parte, ha establecido antecedentes más lejanos: "En 1895, la cámara de los Lumière enfocó al portón de la fábrica, y se convirtió en la precursora de las tantísimas cámaras de vigilancia que hoy en día producen a ciegas y automáticamente una cantidad infinita de imágenes para proteger la propiedad privada" (p. 194).

7 Una dirección IP consiste en una serie única de cuatro números que identifica a cada *host* o anfitrión conectado a una red. Por ejemplo: 186.33.234.104.

8 Todas las capturas de pantalla incluidas en este artículo han sido realizadas sobre transmisiones de cámaras IP rastreadas y publicadas en webs de dicha naturaleza.

Las cadenas de texto o palabras clave presentes en la URL, el título o el contenido de una página web facilitan el hallazgo de dispositivos, vulnerables o no, conectados a una red. Así como se puede preguntar a *Google* el clima, el resultado de un partido de fútbol o el mejor camino para llegar de un punto a otro, es posible pedirle que liste accesos a cámaras de red (y a bases de datos, archivos, mensajes, información personal).

Para operar, un motor de búsqueda descarga a sus centros de datos todo lo que es público en la red (Hacking Google, 2022, 7:00); "[r]astrea datos (o los *navega*), a cuatro patas, arrastrándose, nadando, pastando, recorre la red como una araña, o como un gusano (el robot que es el motor de búsqueda es un enjambre proteico de metáforas) y luego los indexa" (Cassin, 2018, p. 29)[9].

Imagen 3. Transmisión de cámara IP frente a un mar de Japón

Fuente: captura de pantalla, 24 julio 2023, 20:24hs. (arg) – 25 julio 2023, 08:24hs. (jpn).

Al mismo tiempo, la propia actividad de rastreo de cámaras alimenta a la plataforma de búsqueda utilizada. Es decir, ayuda a ese "aparato extractor de datos" (Srnicek, 2018, p. 50) a que sus algoritmos se vuelvan más eficaces y a que identifique deseos expresados en nuestras interacciones digitales (p. 47). Como explica Shoshana Zuboff (2020),

9 "It '*crawls*' data (or *browses* it), on all fours, creeping around, swimming, grazing, it goes around the web like a *spider*, or like a *worm* (the robot that is the search engine is a protean swarm of metaphors), and then it indexes them." (Cassin, 2018, p. 29).

> Google logró imponer la mediación informática en nuevos y muy extensos dominios de la conducta humana a partir de las búsquedas que los usuarios de los ordenadores hacían en línea y a partir también de la implicación de esos usuarios en la red a través de un creciente elenco de servicios de la propia Google. Al informatizarse por primera vez, todas esas actividades nuevas produjeron recursos de datos totalmente nuevos también (p. 100).

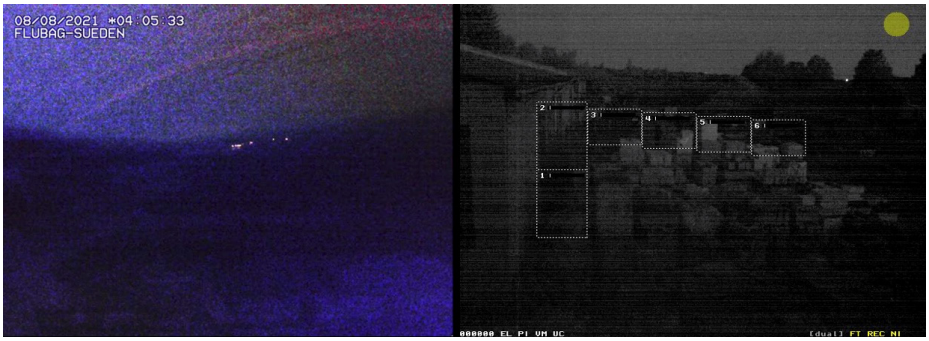
Esos datos –cuyo registro y recopilación requieren además de una vasta infraestructura y consumo de energía– pueden ser, luego de su procesamiento, *inputs* para otras acciones o procesos (Costa, 2021)[10]: su análisis, agrupación en series, desarrollo de estadísticas, establecimiento de correlaciones, construcción de perfiles, anticipación de comportamientos individuales, etc. Es decir, se insertan en un entramado más amplio y complejo de *gubernamentalidad algorítmica*[11] (Rouvroy & Berns, 2016): una clase de racionalidad que busca modelizar, anticipar y afectar comportamientos posibles en base a la "recolección, agrupación y análisis automatizado de datos masivos" (p. 96).

Junto a las imágenes, las cámaras de red registran y transmiten metadatos que pueden, o no, estar impresos sobre la escena captada (Imagen 4). Estos incluyen fecha y hora de transmisión, ubicación, tipo, fabricante, serie y/o modelo del dispositivo empleado, resolución y calidad de la imagen, compresión del video, velocidad de fotogramas, información sobre la red a la que está conectada la cámara y los datos transmitidos, seteo de alarmas o eventos (detección de movimiento o sonido, uso del dispositivo, etc.), entre otros detalles técnicos posibles de ser registrados.

10 Un ejemplo sencillo de recopilación y análisis de datos e interacciones digitales por parte de *Google* son los ya mencionados *CAPTCHA* que algunas veces interrumpen las búsquedas. La frecuencia, el tipo de consulta o la ubicación desde la que se realiza, entre otros factores, pueden llevar al buscador a dudar de la naturaleza humana de quien ejecuta la acción. En este caso, nuestros patrones de uso de las herramientas ofrecidas por la plataforma son comparados con lo que sería -según sus propios parámetros- un comportamiento humano esperable. Luego, por el modo en que la prueba propuesta es resuelta, el algoritmo determina si se trata de un ser humano o un bot automatizado y, según sea el caso, permite o rechaza la acción que se pretendía realizar.

11 Este concepto avanza sobre la categoría de *gubernamentalidad* presentada por Foucault en 1978 para designar un conjunto de técnicas, saberes y estrategias que hacen posible el ejercicio de un modo complejo y específico de poder, que tiene como blanco la población, como forma mayor de saber a la economía política y como instrumento técnico o tecnologías esenciales a los dispositivos de seguridad (Foucault, 2006).

Imagen 4. Izq.: Transmisión de cámara IP en Suiza / Der.: Transmisión de cámara IP en Alemania



Fuente: Izq.: captura de pantalla, 7 agosto 2021, 23:05hs. (Arg.) - 8 agosto 2021, 04:05hs. (Sui.) / Der.: captura de pantalla, 8 agosto 2021, 23:34hs. (arg) - 9 agosto 2021, 04:34hs. (ale).

Así pues, los datos producidos y enviados por estas cámaras pueden emplearse para recuperar información tanto de los lugares, situaciones y/o sujetos observados como de los propios dispositivos que transmiten las imágenes vía Internet. Al mismo tiempo, como ya fue referido, pueden utilizarse como *inputs* para otros procesos. Las imágenes, las direcciones IP de origen, las URL, el código HTML, los textos que aparecen en las consolas de configuración de las cámaras o impresos sobre el video, entre otros elementos, son portadores de esa información que cumple un rol fundamental en nuestras sociedades contemporáneas. Y que es, a la vez y por eso mismo, un terreno en disputa (Rodríguez, 2016).

3. VIGILANCIA, VISIBILIDAD, IN/SEGURIDAD

Las sociedades de control son "maquinarias de producción de miedos y de dispositivos para enfrentarlos" (Diego Galeano en Rodríguez, 2008, p. 3). Buena parte de las cámaras que aquí nos competen pueden –además de transmitir y almacenar imágenes en vivo– girar, inclinarse, acercarse, alejarse y son controlables y configurables en forma remota. En base a tales características, son tipificadas como tecnologías "de seguridad" o "de vigilancia" y comercializadas bajo dichos conceptos. Sus fabricantes –Axis, HikVision, Mobotix, Toshiba, entre otros– las proponen como idóneas "para los requisitos de las redes de vigilancia y seguridad más exigentes", "para reducir el crimen y el desorden", "proteger todos los alrededores", o "ayudar a mantener la paz". Quienes las adquieren y utilizan ponen en acto dichas construcciones de sentido.

Como apunta David Lyon (2007), las respuestas técnicas a una variedad de problemáticas sociales, económicas y/o políticas se han vuelto un lugar común en las sociedades contemporáneas. Hoy en día, las cámaras operan como tecnologías de supervisión del espacio público, de prevención de delitos, disuasión de

comportamientos y acciones indeseadas, identificación y seguimiento de personas, por mencionar solo algunas. Estas técnicas y tecnologías de visibilidad nos protegen, supuestamente, "no contra peligros concretos, sino contra unos riesgos amorfos y misteriosos" (Bauman & Lyon, 2013, p. 107), contra peligros ubicuos o amenazas en potencia, contra un *otro* indeterminado.

A su vez, las prácticas de vigilancia en las cuales estas soluciones técnicas son aplicadas no se restringen a poblaciones o espacios clasificados como "peligrosos" o "sospechosos"; alcanzan todo tipo de ámbitos públicos, semipúblicos y privados (Bruno, 2013, p. 8) (Imagen 5). Se han incorporado a la cotidianeidad de "la vida urbana, las relaciones sociales, familiares y las formas de entretenimiento" (p. 23). Se vigila al aire libre tanto como en la intimidad de los hogares. Se vigila porque la vigilancia ofrece una promesa de seguridad: "[u]na de sus principales fortalezas es la capacidad disuasoria que posee: la mera presencia de las cámaras puede abortar un intento de allanamiento o hurto", se explica en la página web de la empresa *PROSEGUR*.

Imagen 5. Arriba: capturas de páginas webs de fabricantes de cámaras IP (Axis y Hikvision) / Abajo: fotografías tomadas en espacios públicos y privados de la Ciudad Autónoma de Buenos Aires en 2022-2023

Fuente: elaboración propia.

Pero: ¿puede un dispositivo técnico de captura de imágenes proveer protección y seguridad por sí mismo? ¿Bajo qué condiciones y regulaciones se ejerce la videovigilancia? ¿Qué sucede con los registros permanentes de la actividad social y personal que producen estos artefactos? ¿Cómo afectan estas prácticas a la privacidad de las personas?

Como fue señalado más arriba, la incorporación de estos aparatos productores y transmisores de imágenes como elemento central en prácticas de vigilancia está fundamentada en el discurso de la seguridad. No obstante, la forma en que se utilizan estas tecnologías en el marco de dichas prácticas conlleva inseguridades, vulnerabilidades, fugas. Son estas las que hacen factible que los dispositivos puedan ser encontrados, vistos y manipulados en línea.

Esto es especialmente relevante si se considera que la videovigilancia contemporánea es puesta en práctica no sólo por estados o grandes compañías y empresas, sino también por particulares que instalan y gestionan sus propias redes de control hogareñas o en pequeños comercios. Al hacerlo con desconocimiento de los modos de funcionamiento o métodos de protección y cifrado de los dispositivos que emplean, dejan expuestas las herramientas de configuración, las transmisiones y la información de los sistemas que montan con fines de vigilancia. Ceden sus imágenes e impresiones.

Así, es posible hallar en Internet representaciones de los más diversos espacios y situaciones (imágenes 2, 3, 6, 7 y 8), que proporcionan un inventario visual de todo aquello que es objeto de vigilancia pública y privada en las sociedades actuales: instituciones, comercios, fábricas y oficinas, interiores y exteriores de hogares, ascensores, calles, rutas y autopistas, parques, playas y montañas, hoteles, atracciones turísticas.

Las vulnerabilidades de la videovigilancia y las formas de atenuarlas son menos difundidas o comprendidas, y quedan por lo general invisibilizadas tras el discurso de la seguridad[12]. Tales riesgos y desconocimiento respecto de los usos imprudentes de las cámaras de red, junto a su débil regulación, son tanto la fisura que habilita la observación de las imágenes que motivaron este escrito como el espacio para reflexionar sobre su producción, circulación y usos. ¿Quién es responsable por la información que queda accesible a cualquiera en Internet debido a esas fisuras? ¿Por qué estos dispositivos son expuestos en resultados de búsqueda en línea?

12 David Lyon, Zygmunt Bauman, Didier Bigo o Hille Koskela son referentes que han desarrollado el problema de las inseguridades asociadas al empleo de nuevas tecnologías en prácticas de vigilancia por seguridad.

InMediaciones de la Comunicación 2024 - VOL. 19 / Nº 2 - ISSN 1510-5091 - ISSN 1688-8626 (EN LÍNEA) - MONTEVIDEO (URUGUAY)

Imagen 6. Transmisión de cámara IP de la *Submillimeter Array* (SMA) del Observatorio Astrofísico Smithsoniano y el Instituto de Astronomía y Astrofísica de la Academia Sinica, en Mauna Kea, Hawái

Fuente: captura de pantalla, 19 julio 2021, 20:01hs. (arg) – 13:01hs. (eeuu).

En suma, responder por qué es factible rastrear, ver y capturar imágenes en vivo provenientes de cámaras de red requiere abarcar distintos niveles de análisis: en primer lugar, porque dentro de un marco más general de desarrollo de una "nueva gestión semiotio-técnica digital" del cuerpo y la subjetividad contemporáneos (Preciado, 2020, s/p)[13] existen formas y procesos específicos de rastreo, extracción, indexación, tratamiento de datos y de producción de información y conocimiento sobre los sujetos que los generan. También, porque dentro de esa nueva gestión, el fenómeno de la vigilancia se extiende "hasta constituirse en una experiencia vital generalizada, ubicua, distribuida" (Costa, 2021, p. 39). Tanto los procesos nucleados alrededor de los datos como las prácticas de vigilancia y los dispositivos y redes allí empleadas tienen vulnerabilidades, zonas grises, desreguladas, y/o modos de funcionamiento poco transparentes, que abren vías a la exposición y circulación de información personal sensible (como podrían ser imágenes provenientes de cámaras IP con rostros humanos identificables).

A lo antedicho debe sumarse además el lugar privilegiado de las cámaras en los sistemas de vigilancia, así como la justificación y legitimación de su uso mediante prácticas y discursos securitarios. Ligado a esto último, Fernanda

13 "La extensión planetaria de Internet, la generalización del uso de tecnologías informáticas móviles, el uso de la inteligencia artificial y de algoritmos en el análisis de big data, el intercambio de información a gran velocidad y el desarrollo de dispositivos globales de vigilancia informática a través de satélite son índices de esta nueva gestión semiotio-técnica digital" (Preciado, 2020, s/p.).

Bruno (2008) aclara que si bien la vigilancia se justifica o se ejerce por el miedo o por la promesa de seguridad, expresa también todo un circuito de libidos, placeres y deseos: ver y ser visto. Las "imágenes de vigilancia son también imágenes de espectáculo" (p. 49)[14].

Imagen 7. Izq.: transmisión de cámara IP en fábrica de Japón / Der.: transmisión de cámara IP en lavandería de Japón

Fuente: Izq.: captura de pantalla, 27 julio 2021 21:58hs. (arg), 28 julio 2021, 09:58hs. (jpn) / Der.: captura de pantalla, 7 agosto 2021, 23:52hs. (arg) – 8 agosto 2021, 11:52hs. (jpn).

Imagen 8. Izq.: transmisión de cámara IP en Austria / Der.: transmisión de cámara IP en Estados Unidos

Fuente: Izq.: captura de pantalla, 11 noviembre 2022, 00:42hs. (arg) – 05:42hs. (aus) / Der.: captura de pantalla, 9 diciembre 2021, 21:57hs. (arg) – 19:57hs. (eeuu).

14 En dirección similar, Vanesa Lio (2024) ha destacado la creciente introducción de representaciones provenientes de cámaras empleadas para vigilancia en los medios de comunicación: "las imágenes de las cámaras se incorporaron a la industria de la noticia y el espectáculo, como emergente de una tendencia a la espectacularización de la videovigilancia" (p. 163).

4. INTERFERENCIAS E INTERRUPCIONES

Junto a la expresión de deseos y placeres –en el sentido señalado por Bruno (2008 y 2013)– hay otro aspecto que ubica estas transmisiones de cámaras inseguras en el cruce entre la vigilancia, la información y el espectáculo: su exposición pública las vuelve superficies de inscripción de mensajes o intervenciones por parte de sujetos no identificados.

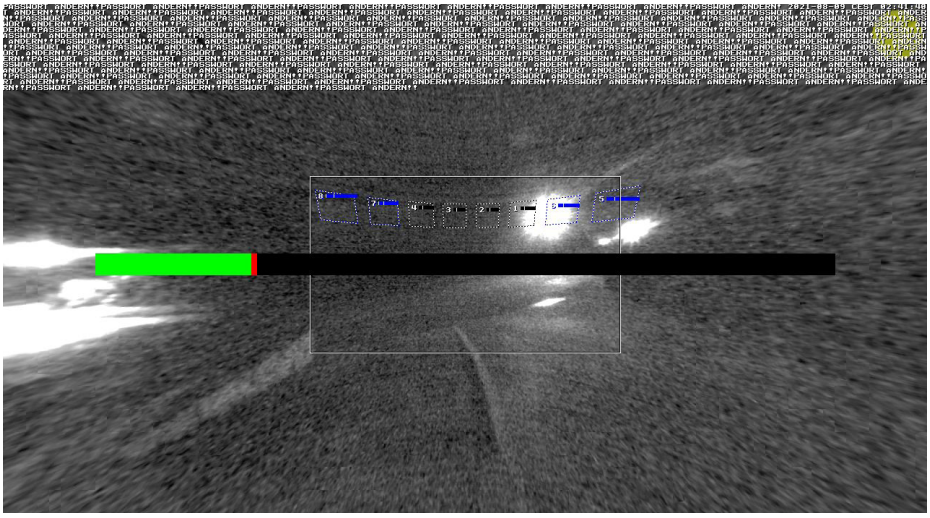
Dichas alteraciones sobre el caudal de imágenes emitido por estos dispositivos se encuentran dirigidas a receptores-espectadores de diverso tipo. Por un lado, a quienes adquieren e instalan las cámaras: son advertencias sobre el estado de vulnerabilidad de sus tecnologías empleadas para vigilancia. Por el otro, a un conjunto más amplio que incluye ya no sólo a quienes poseen los aparatos sino también a cualquier otra persona que los encuentre en línea y acceda a ellos. Estas últimas, son intervenciones que refieren a contextos que trascienden el marco de producción y emisión de las imágenes y que, en ocasiones, incluyen expresiones de carácter político.

En su texto sobre las sociedades de control, Deleuze (2006) postula que estas "actúan mediante máquinas de un tercer tipo, máquinas informáticas y ordenadores cuyo riesgo pasivo son las interferencias y cuyo riesgo activo son la piratería y la inoculación de virus" (párr. 7). Estas intervenciones, cada una a su manera, imprimen en la superficie de las transmisiones en vivo esos riesgos pasivos y activos, el ruido y el *hackeo*, inherentes a las condiciones de producción de las imágenes para vigilancia generadas por cámaras IP. Ponen a la vista elementos que quedan perdidos tras las promesas de seguridad y los mecanismos opacos de estas tecnologías: la cara insegura de las prácticas de videovigilancia, la exposición pública de los dispositivos en Internet, las posibilidades de emplear las imágenes que emiten en sentidos no previstos por sus propietarios/as, el uso acrítico y desinformado de los objetos o sistemas técnicos.

Esto es explícito en los mensajes dirigidos a quienes instalan las cámaras y las ponen a transmitir sin protección (imágenes 9, 10 y 11): "Fix your webcam. It's not password protected" [Arregla tu webcam. No está protegida con contraseña], "You need to secure your camera!" [¡Necesitas asegurar tu cámara!] o "You got hacked" [Te han hackeado] son algunas de las advertencias que pueden leerse estampadas sobre las transmisiones.

Si las herramientas de configuración de la cámara están visibles y sin contraseña, es sencillo llevar a cabo acciones como estas (u otras); basta entrar al panel de ajustes, alterar el texto original y guardar la modificación realizada. La permanencia de estos enunciados anónimos sobre las transmisiones por tiempo prolongado o indefinido, así como la desprotección de las cámaras pese a las advertencias formuladas, podría indicar que sus propietarios/as ignoran cómo configurar y/o asegurar los dispositivos que emplean. O bien, que no les preocupa que sus imágenes puedan ser vistas por personas desconocidas.

Imagen 9. Transmisión de cámara IP en Austria / Texto sobre la transmisión: "Cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña! cambia la contraseña!". [original en alemán]

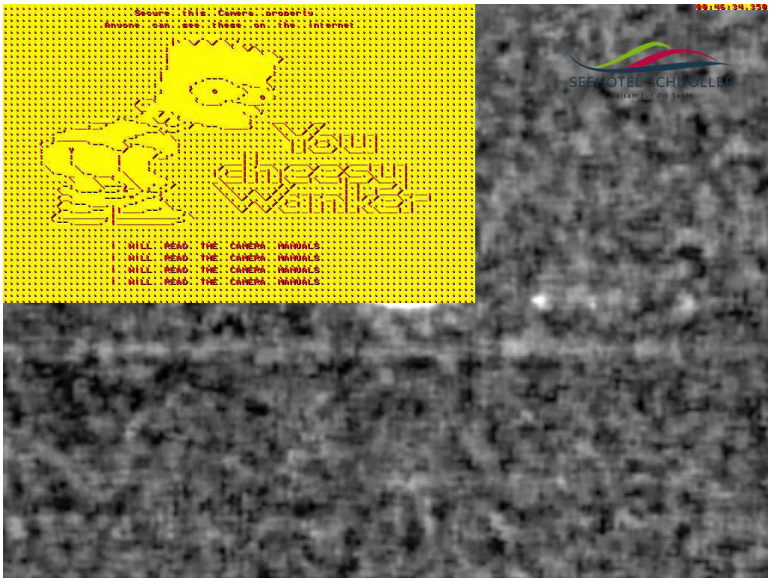


Fuente: captura de pantalla, 8 agosto 2021, 21:41hs. (arg) - 9 agosto 2021, 02:41hs. (aus).

Imagen 10. Transmisión de cámara IP en Francia / Texto sobre la transmisión: "Spikehunter está de vuelta :-)) y lo estará mientras mantengas la cámara en internet" [original en inglés]

Fuente: captura de pantalla, 3 de diciembre de 2023, 21:57hs. (arg) - diciembre 2023, 1:57hs. (fra).

Imagen 11. Transmisión de cámara IP en hotel de Alemania / Texto sobre la transmisión: "Asegure esta cámara correctamente (…) Cualquiera puede verlos en Internet / "LEERÉ LOS MANUALES DE LA CÁMARA - LEERÉ LOS MANUALES DE LA CÁMARA - LEERÉ LOS MANUALES DE LA CÁMARA - LEERÉ LOS MANUALES DE LA CÁMARA" [original en inglés]



Fuente: captura de pantalla, 17 septiembre 2021, 20:46hs. (arg) – 18 septiembre 2021, 00:46hs. (ale).

A su vez, pueden hallarse sobre los videos en línea expresiones que apuntan más allá de la propia condición de inseguridad y visibilidad de las cámaras que los emiten. Por ejemplo, críticas al gobierno ruso sobre la transmisión de una calle en Ucrania, o insultos dirigidos al presidente de los Estados Unidos en las imágenes de una cámara emplazada en el interior de una lavandería japonesa (Imagen 12). Dichas acciones son propicias para señalar aun otra cuestión: el potencial político de las imágenes y los objetos técnicos. Los actos, afirma Vilém Flusser (2017), "ya no se dirigen más contra el mundo para modificarlo sino contra la imagen para modificar y programar al receptor de la imagen" (p. 84). Para este autor, "las preguntas técnicas son actualmente las únicas preguntas políticas interesantes" (p. 92).

Imagen 12. Izq.: transmisión de cámara IP en lavandería de Japón / Der.: transmisión de cámara IP en vías de tren de Japón

Fuente: Izq.: captura de pantalla, 20 octubre 2022, 13:38hs. (arg) - 21 octubre 2022, 01:38hs. (jpn) / Der.: captura de pantalla,13 agosto 2021, 22:03hs. (arg) – 14 agosto 2021, 10:03hs. (jpn).

Estas acciones, que tienen como soporte imágenes de cámaras inseguras, se deslizan por las zonas grises de los sistemas de control y vigilancia contemporáneos introduciendo un ruido ligero, algo que no debería –¿o sí?– estar allí: muestran la hendidura desde la que fueron producidas. Los desvíos del control, la puesta en visión de sus vacíos, pueden abrir camino hacia las preguntas técnicas, indispensables para actuar y pensar políticamente en las sociedades de hoy en día. ¿Cómo los aparatos producen lo que muestran?, se cuestiona Flusser (2017). ¿Cómo crear estrategias y tácticas "de interrupción de los regímenes luminosos de hiper-visibilidad y auto-revelación que sostienen los actuales sistemas de auto-control y de seguridad"? (Cano, 2021, p. 51). ¿Qué otros modos de relación y uso podemos establecer con los dispositivos técnicos que nos rodean?

Para Alexander Galloway (2004), el *hacking* evidencia que los modos de resistencia al poder han cambiado en la posmodernidad. Ya no se forman en torno a jerarquías rígidas y estructuras de poder burocráticas como en la época moderna: las redes han transformado el concepto de "resistencia" (Galloway & Thacker, 2007, p. 78). Luchar contra poderes descentralizados requiere el uso de medios descentralizados, de nuevos métodos de disrupción que hagan frente a los (no)centros de poder a nivel electrónico (Critical Art Ensemble, 1996). Es allí donde las acciones sobre imágenes de esta clase, y sobre los dispositivos que las producen y propagan, podrían encontrar un rol político.

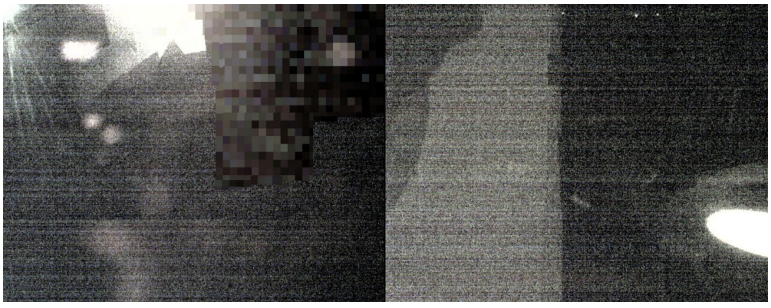
5. PALABRAS (E IMÁGENES) FINALES

A partir de la práctica de búsqueda y observación de transmisiones en vivo de cámaras de red desprotegidas se ha procurado desnaturalizar y abordar críticamente el rol de estos dispositivos en el marco de las sociedades de control. De acuerdo con lo analizado en las páginas que anteceden, dar cuenta de las condiciones de producción, circulación y usos –previstos o no– de dichas imágenes requiere considerar un conjunto heterogéneo de actores, elementos

y procesos que incluye: los protocolos de comunicación y transmisión de datos en Internet, los modos en que las plataformas de búsqueda rastrean, indexan y operan sobre esos datos y cómo los exponen en los resultados de las búsquedas, el desconocimiento técnico sobre los dispositivos utilizados, la extensión general y ubicua de una nueva cultura de la vigilancia, el lugar central asignado a las cámaras en tal contexto y su estrecho vínculo con discursos sobre seguridad[15]. Todo esto, a su vez, se integra en mecanismos más amplios de ejercicios de poder y control en nuestras sociedades actuales: como indica Bruno (2008), "la vigilancia contemporánea es inseparable de la maquinaria informacional, reticular y modular del capitalismo posindustrial"[16] (p. 46).

La posibilidad que habilita Internet de hallar, ver y/o manipular en forma remota transmisiones de cámaras de red públicas y privadas desprotegidas, pone de manifiesto vacíos –tecnológicos, informáticos, legales, éticos, etc.– que existen en el empleo de estas tecnologías. Asimismo, subproducto de sus niveles de complejidad técnica, los espacios informáticos presentan fallos y agujeros que los hacen vulnerables a la penetración y el cambio (Galloway & Thacker, 2007, p. 82), tal como evidencian los actos anónimos de intervención sobre aquellas imágenes concebidas en su origen como herramientas para vigilar. Sus autores encuentran en esas vulnerabilidades canales y superficies de enunciación e imprimen sobre ellas mensajes que perturban el flujo de transmisión de información de las cámaras (Imagen 13).

Imagen 13. Transmisión de cámara IP en Alemania



Fuente: captura de pantalla, 8 agosto 2021, 23:29hs. (arg) – 9 agosto 2021, 04:29hs. (ale).

15 "Según David Lyon, pionero en los estudios sociales de la vigilancia, tras los atentados a las Torres Gemelas el 11 de septiembre de 2001 se ha promovido una nueva 'cultura de la vigilancia', en la que ser observados puede significar un riesgo para la intimidad o la privacidad, pero también una ayuda o una 'asistencia' permanente, muy bienvenidas incluso en la vida cotidiana. Las personas ya no solo están familiarizadas con la vigilancia: al mismo tiempo le temen, la reclaman y hasta se divierten con ella. Lyon pone el acento en aquellas prácticas que incluyen la participación en la entrega de datos personales 'por nuestro propio bien', en un vaivén entre 'seguridad' y 'privacidad', entre exposición y anonimato. Incluso más: esta vigilancia parece estar siendo –de una manera diferente pero no del todo escindida del panoptismo– una incitación, una provocación tecnológica a decir una verdad acerca de nosotros mismos en la que se enlazan mecanismos de identificación y dispositivos de subjetivación" (Costa, 2021, p. 94).

16 "A vigilancia contemporânea é inseparável da maquinaria informacional, reticular e modular do capitalismo pós-industrial".

Es decir, si en las sociedades postdisciplinarias los mecanismos de control y vigilancia se articulan con tecnologías antes que con instituciones, y ciertas prácticas, procesos y sistemas tales como la gubernamentalidad algorítimica se sustentan en la recolección y análisis de datos, las interferencias e interrupciones lumínicas, electrónicas, informáticas pueden operar sobre los actuales regímenes de hipervisibilidad o, cuando menos, dejar expuestas algunas de sus fisuras.

REFERENCIAS

Bauman, Z. & Lyon, D. (2013). *Vigilancia líquida*. Ciudad Autónoma de Buenos Aires: Paidós.

Bruno, F. (2008). Controle, flagrante e prazer: regimes escópicos e atencionais da vigilância nas cidades. *Revista FAMECOS*, *15*(37), pp. 45-53. DOI: https://doi.org/10.15448/1980-3729.2008.37.4799

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina.

Cano, V. (2021). *Borrador para un abecedario del desacato*. Ciudad Autónoma de Buenos Aires: Madreselva.

Cassin, B. (2018). *Google Me: One-click democracy.* New York: Fordham University Pres.

Costa, F. (2020). ¿Qué hay de mí en esos datos? Políticas de la materialidad y estrategias críticas en las prácticas bioartísticas en América Latina. En Tello, A. M. (ed.), *Tecnología, política y algoritmos en América Latina* (pp. 111-129). Santiago de Chile: Cenaltes Ediciones.

Costa, F. (2021). *Tecnoceno. Algoritmos, biohackers y nuevas formas de vida.* Ciudad Autónoma de Buenos Aires: Taurus.

Critical Art Ensemble (1996). *Electronic civil disobedience and other unpopular ideas*. New York: Autonomedia.

Deleuze, G. (2006). Posdata sobre las sociedades de control. *Polis. Revista Latinoamericana,* (13), pp. 1-13. Recuperado de: http://journals.openedition.org/polis/5509

Farocki, H. (2015). *Desconfiar de las imágenes*. Ciudad Autónoma de Buenos Aires: Caja Negra.

Fisher, M. (2016). *Realismo capitalista: ¿no hay alternativa?* Ciudad Autónoma de Buenos Aires: Caja Negra.

Flusser, V. (2017). *El universo de las imágenes técnicas: elogio de la superficialidad*. Ciudad Autónoma de Buenos Aires: Caja Negra.

Foucault, M. (1978). Nuevo orden interior y control social. En *Saber y verdad* (pp. 163-166). Madrid: La Piqueta.

Foucault, M. (2006). *Seguridad, territorio, población*. Ciudad Autónoma de Buenos Aires: Fondo de Cultura Económica.

Galloway, A. & Thacker, E. (2007). *The exploit: a theory of networks*. Minneapolis: University of Minnesota Press.

Galloway, A. (2004). *Protocol*: *how control exists after decentralization*. London: MIT Press.

Hacking Google (2022). *Documentary Hacking Google* (Episodio 001) [Serie]. *Youtube.* Recuperado de: https://www.youtube.com/watch?v=N7N4EC20-cM

Hall, E. (2000). *Internet core protocols: the definitive guide*. Sebastopol: O'Reilly.

Koskela, H. (2006). 'The other side of surveillance': webcams, power and agency. In Lyon, D. (ed.), *Theorizing Surveillance: The panopticon and beyond* (pp. 163-181). Portland: Willan Publishing.

Lio, V. (2024). Imágenes del delito. Del uso preventivo a la eficacia mediática de las cámaras de seguridad. *InMediaciones de la Comunicación*, *19*(1), pp. 161-187. DOI: https://doi.org/10.18861/ic.2024.19.1.3506

Preciado, B. (2014). *Testo yonqui. Sexo, drogas y biopolítica*. Ciudad Autónoma de Buenos Aires: Paidós.

Preciado, P. B. (2020). Aprendiendo del virus. *El País*. Recuperado de: https://elpais.com/elpais/2020/03/27/opinion/1585316952_026489.html

Rodríguez, P. (2008). ¿Qué son las sociedades de control? *Revista Sociedad*. Recuperado de: http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9-son-las-sociedades-de-control.pdf

Rodríguez, P. (2016). Diez preguntas a una posdata misteriosa. Sobre las sociedades de control de Gilles Deleuze. En Estevez, R., Saidel, M. L., Sacchi, E., Rios Roso, C. & Velázquez Ramírez, A. (comps.), *Libro de Actas de las VI Jornadas de Debates actuales de la teoría política contemporánea* (pp. 371-390). Rosario: Ediciones Debates Actuales.

Rodríguez, P. (2018). Gubernamentalidad algorítmica. Sobre las formas de subjetivación en la sociedad de los metadatos. *Barda*, *4*(6), pp. 14-35. Recuperado de: https://www.cefc.org.ar/assets/files/rodriguez.pdf

Rouvroy, A. & Berns, T. (2016). Gubernamentalidad algorítimica y perspectivas de emancipación. ¿La disparidad como condición de individuación a través de la relación? *Adenda Filosófica,* (1), pp. 88-116.

Sadin, E. (2018). *La humanidad aumentada: la administración digital del mundo*. Ciudad Autónoma de Buenos Aires: Caja Negra.

Srnicek, N. (2018). *Capitalismo de plataformas.* Ciudad Autónoma de Buenos Aires: Caja Negra.

Virilio, P. (2011). *Ciudad pánico. El afuera comienza aquí*. Ciudad Autónoma de Buenos Aires: Capital Intelectual.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), pp. 75-89. DOI: https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2020). *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder.* Barcelona: Paidós.

* Contribución de autoría: la conceptualización y el desarrollo integral del artículo fue realizado por la autora.
* Nota: el Comité Académico de la revista aprobó la publicación del artículo.

* El conjunto de datos que apoya los resultados de este estudio no se encuentran disponibles para su uso público. Los datos de la investigación estarán disponibles para los revisores, si así lo requieren.

IDENTIFICACIÓN DE LA AUTORA

Agustina Lapenda. Doctora –candidata– en Ciencias Sociales, Universidad de Buenos Aires (Argentina). Magister en Ciencia Política, Universidad Nacional de San Martín (Argentina). Diplomada en Genocidios y Violencia de Estado, Universidad de Buenos Aires. Licenciada en Artes, Universidad de Buenos Aires. Becaria doctoral, Consejo Nacional de Investigaciones Científicas y Técnicas (Argentina). Integrante, Área de Fotografía Patrimonial, Centro de Investigaciones en Arte y Patrimonio, Universidad Nacional de San Martín y Consejo Nacional de Investigaciones Científicas y Técnicas. Docente adjunta, seminario de posgrado "Historias de la Fotografía I", Maestría en Estudios sobre Imagen y Archivos Fotográficos, Universidad Nacional de San Martín. Ha trabajado en parametrización y elaboración de bases de datos y catalogación de colecciones fotográficas públicas y privadas.