COMUN.AL
MALPAÍS EDICIONES

VIOLENCIA_DIGITAL_EN_MÉXICO:

EL_ESTADO_VS_LA_SOCIEDAD_CIVIL

ALEXANDRA ARGÜELLES
(COORDINADORA)

BRENDA BATTAGLIA
(ILUSTRACIONES)

VIOLENCIA_____DIGITAL EN MÉXICO:_____

EL ESTADO_____VS_____ LA SOCIEDAD CIVIL

COMUN.AL
Laboratorio de resiliencia digital

10 MALPAÍS EDICIONES

Nombres: Argüelles, Alexandra (coordinadora) | Battaglia, Brenda (ilustradora)
Título: Violencia digital en México: El Estado vs la sociedad civil / Alexandra Argüelles (coordinadora), ilustraciones de Brenda Battaglia.
Descripción: Primera edición | México: Malpaís ediciones: COMUN.AL, 2021.
Temas: Tecnología – Tecnopolítica, Derechos Humanos

PRIMERA EDICIÓN: OCTUBRE 2021

ESTA ANTOLOGÍA FUE CREADA CON EL APOYO DE MOZILLA Y LA FUNDACIÓN FORD, A TRAVÉS DEL PROGRAMA TECNOLOGÍA Y SOCIEDAD 2020-2022.

VIOLENCIA_____DIGITAL EN MÉXICO:_____ EL ESTADO_____VS_____ LA SOCIEDAD CIVIL

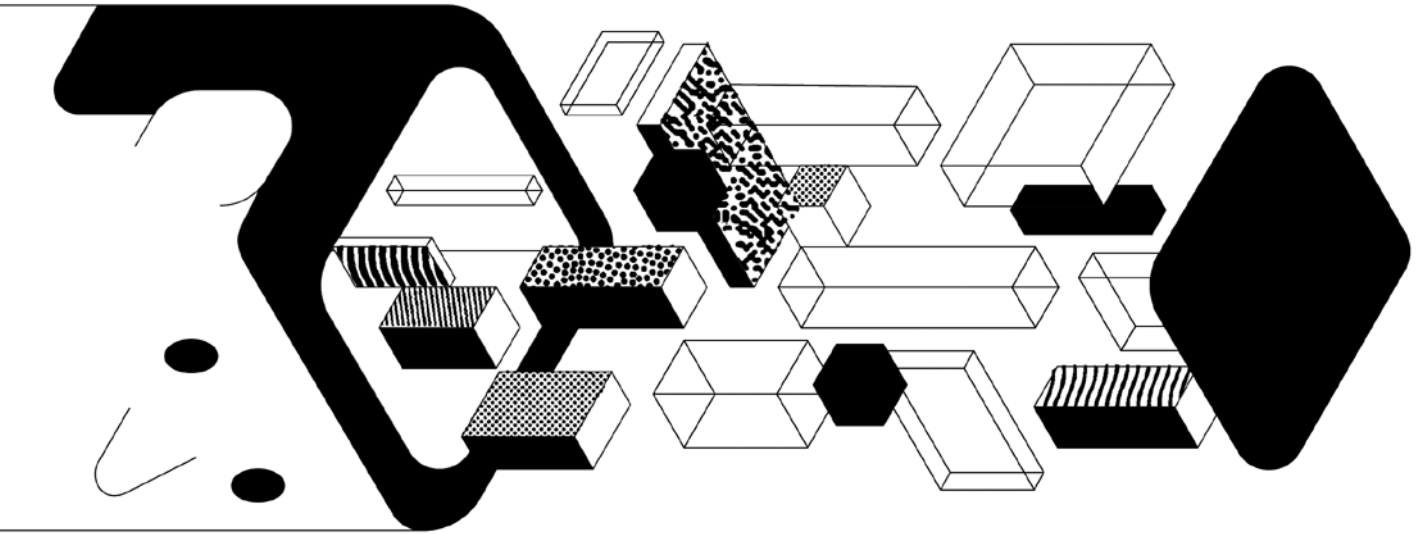
ALEXANDRA _____ ARGÜELLES

(COORDINADORA)

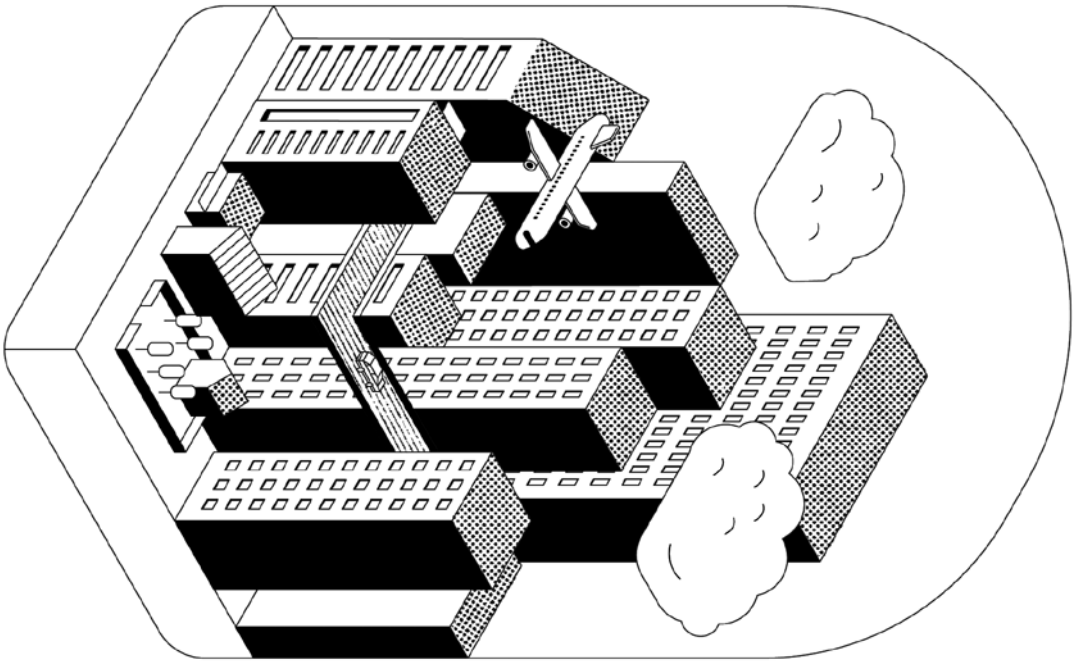
BRENDA _____ BATTAGLIA

(ILUSTRACIONES)

COMUN.AL
MALPAÍS EDICIONES



ÍNDICE



ALEXANDRA ARGÜELLES

México es un país marcado por la violencia. Nuestra historia resuena también con el eco de abusos de poder, dictaduras, violaciones a derechos humanos y crímenes de lesa humanidad que forman parte de la historia de América Latina.

México es un país marcado por la resistencia. Nuestra historia carga la experiencia de cientos de personas defensoras de derechos humanos que han alzado la voz para proteger a sus comunidades y territorios: su dignidad, nuestra dignidad.

México es un país marcado por la falta de memoria. Nuestra historia está fragmentada, así como los conocimientos que surgen de las experiencias de quienes, haciendo frente al constante abuso de poder, viven en pie de lucha.

Nuestro contexto refleja cómo la falta de acceso a la justicia ha permeado en distintas áreas de nuestras vidas y, a la vez, también da testimonio de cómo las tecnologías están utilizándose como instrumentos de vigilancia, control y criminalización social. Ante esto, varias rutas de acción se han puesto en marcha desde la sociedad civil organizada en torno a la defensa de los derechos humanos, que también se afectan o amplifican a través de las tecnologías; derechos como la li-

bertad de expresión, el acceso a la información, la privacidad o el mismo acceso a internet. Sin embargo, en los últimos 12 años hemos visto que hay una tendencia latente a ignorar sus voces y seguir apostando por medidas que acrecientan la dependencia tecnológica, incrementan la brecha digital y reproducen patrones de abuso sobre las poblaciones vulnerables o quienes abiertamente muestran una postura crítica hacia el gobierno.

Por otro lado, no podemos ignorar que México lleva varios años calificado como el país más peligroso para ejercer el periodismo en América Latina. Esto, más allá de las consecuencias que tiene para el ejercicio de la democracia en nuestro país, también es un reflejo del costo que asumen las personas que buscan informar, alertar o señalar sobre las situaciones de violencia, corrupción, abuso o despojo que nuestro gobierno —sin importar el partido en turno— ejerce sobre la población cada vez más vulnerable, víctima de la desinformación y, en algunos casos, incluso incomunicada.

Lo anterior se suma a las condiciones de corrupción e impunidad que también son parte de nuestra historia: la colaboración entre el Estado y los cárteles, la impunidad hacia grupos y acto-

res que ostentan posiciones de poder oligárquico, el silencio cómplice que obstruye el acceso a la justicia y la represión incesante hacia quienes asumen el riesgo que implica hacer frente a todo esto. En estas condiciones, a través de las herramientas digitales comenzó a difundirse de forma masiva el abuso de poder en sus distintas dimensiones. Sin depender de medios privados masivos, las redes socio-digitales comenzaron a abrir nuevas posibilidades para combatir la desinformación y generar espacios de encuentro que facilitaran la organización civil. Así, las personas han podido acceder a información que les permite tomar decisiones para desarrollarse individual y colectivamente: las tecnologías han sido herramientas que han servido para resistir y construir nuevas rutas hacia la justicia, transformando nuestra impotencia y dependencia en posibilidades y autonomía.

A finales de la primera década del siglo XXI hubo un auge en el despliegue de programas de vigilancia masiva a nivel mundial. Si bien esto se potenció a raíz del pánico tras los ataques terroristas de 2001 en Estados Unidos, las revelaciones de WikiLeaks en 2011 y la información compartida por Edward Snowden en 2013 evidenciaron el interés internacional por explotar

las capacidades de vigilancia y control social que las tecnologías —al ser utilizadas de forma abusiva— brindan a los gobiernos. En el caso de México, siguiendo la "tradición" establecida por Estados Unidos, estas tecnologías han sido promovidas como soluciones de seguridad o elementos clave en las estrategias de combate al crimen organizado. Sin embargo, la realidad ha demostrado que se han usado principalmente para perseguir activistas, periodistas, personas defensoras de derechos humanos y disidentes. Esto se agrava cuando la única salvaguarda para proteger nuestros derechos reside en la capacidad de respuesta de la sociedad civil, mientras surge evidencia sobre la cada vez más documentada colaboración entre las agencias estatales de inteligencia y el crimen organizado, que también ha aprovechado estas tecnologías para su beneficio.

A través de distintas ONG e iniciativas locales se ha buscado generar los contrapesos necesarios para frenar el abuso de poder que se oculta tras la implementación de medidas desproporcionadas que pretenden consolidar más capacidades de persecución estatal a costa de nuestros derechos, por medio de herramientas que —sin medidas de rendición de cuentas— han ser-

vido para dificultar la responsabilización sobre el abuso de estas tecnologías que comprometen la privacidad, menoscaban la autonomía y atentan contra la dignidad de las personas en el país.

En este sentido, es importante poner en marcha estrategias que nos permitan compartir las memorias y experiencias haciendo frente a estos abusos. Para entender la complejidad y las implicaciones que las vulneraciones a través de las tecnologías tienen para nuestros derechos y nuestro desarrollo —tanto individual como colectivo—, es necesario ampliar la conversación para incluir a más personas y su diversidad, descentralizando estas discusiones y abriendo la posibilidad de encontrar respuestas múltiples que nos permitan hacer frente al abuso de poder mientras transformamos las estructuras que nos imponen autoritarismo por justicia.

Las historias que conforman este texto buscan ofrecer un acercamiento a las resistencias y resiliencias que han surgido en México, abordando las distintas manifestaciones de la violencia digital en voz de personas que conforman iniciativas y comunidades, que han sido victimizadas a través de las tecnologías que el Estado ha usado para perseguir a quienes defienden derechos humanos y buscan justicia en nuestro país. A tra-

vés de las experiencias compartidas pretendemos apostar a que más personas tengan acceso a la información que entre nosotras, integrantes de la sociedad civil organizada, compartimos para generar estrategias de incidencia y acompañamiento; con la esperanza de que estas vivencias provoquen el surgimiento de más propuestas que nos permitan ampliar los esfuerzos para hacer frente a las violencias y transformar las estructuras que nos gobiernan.

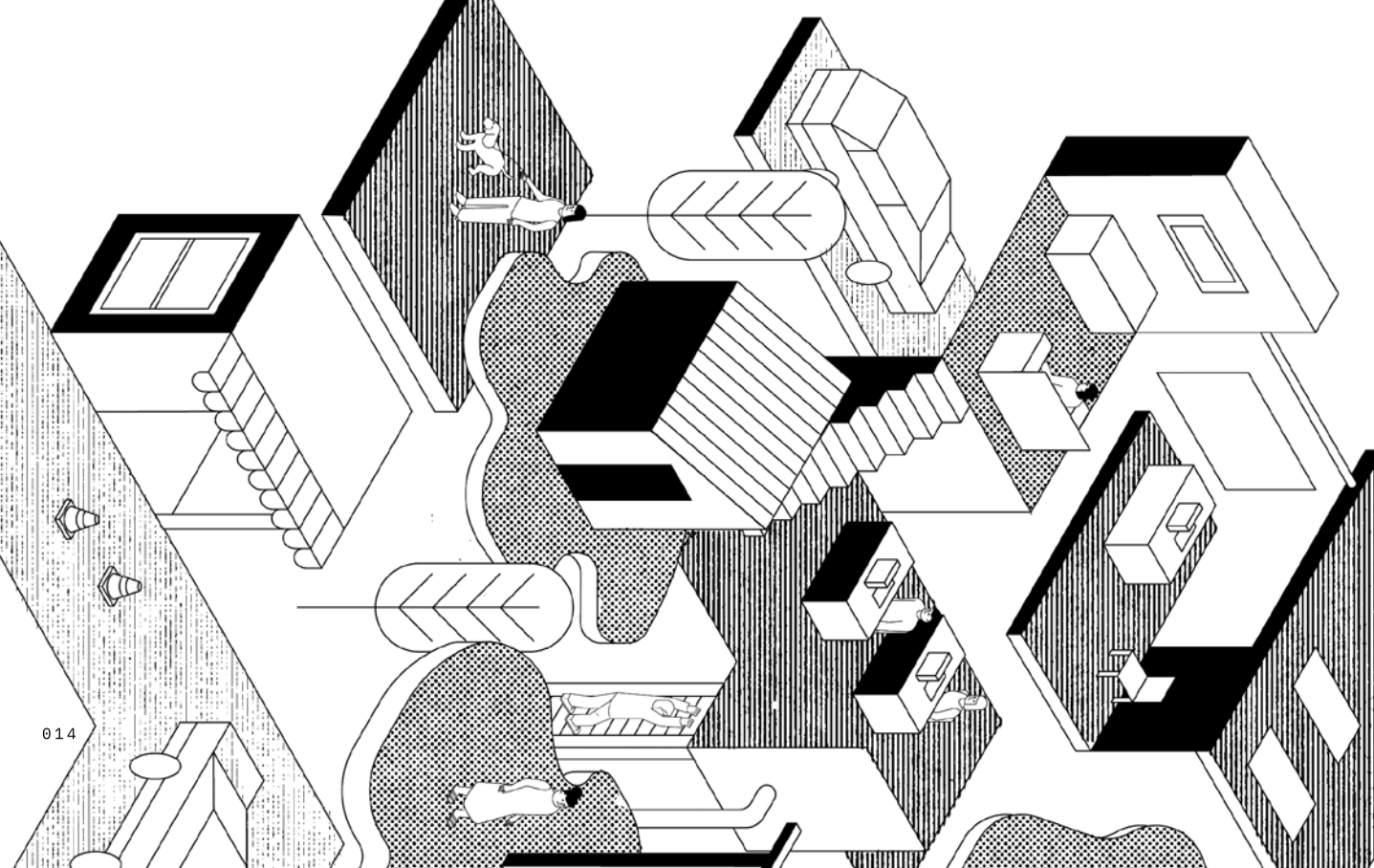
En las siguientes páginas compartimos historias de abuso, despojo y represión, pero también compartimos testimonios de dignidad y resistencia. En un país donde se ha normalizado la impunidad frente a la violencia sociopolítica que ejerce el Estado, es necesario nombrar las diferentes formas que ella toma para construir y compartir estrategias que nos permitan hacerle frente y proteger nuestros derechos.

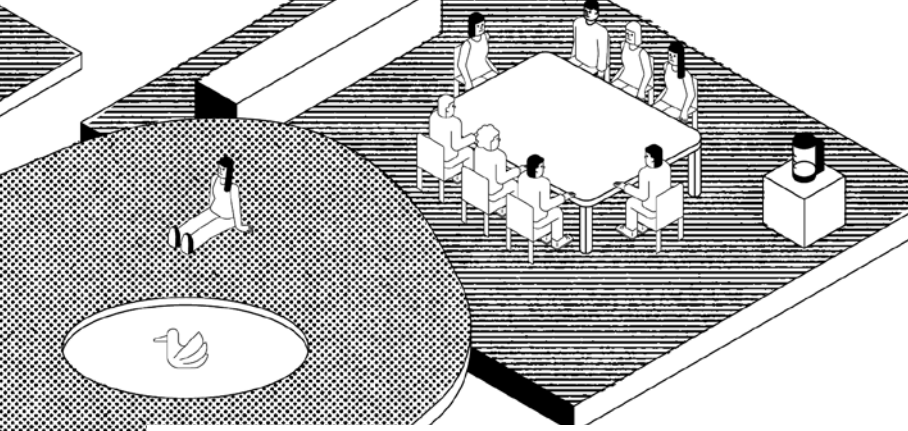
Aún nos falta mucho por recorrer en esta búsqueda de justicia; sin embargo, la experiencia también nos ha dejado aprendizajes en torno a la importancia de crear comunidades para avanzar colectivamente en este camino. Para crear comunidad necesitamos construir confianza, para crear resiliencia necesitamos preservar la memoria.

Si queremos que las tecnologías sean herramientas para el acceso a la justicia y dejen de utilizarse como instrumentos de control, nos corresponde entender cómo estas herramientas se instauran en las estructuras que nos gobiernan, a quién benefician, a quiénes excluyen y qué salvaguardas podemos construir para impedir que sus sesgos amplifiquen las desigualdades y violencias estructurales que hoy combatimos desde otros frentes. Las personas juntas somos más fuertes, compartiendo conocimientos y aprendizajes somos más resilientes. Creemos más espacios de participación, donde podamos colaborar en la construcción de otros futuros posibles: informadas y organizadas.

Con el deseo de que estas palabras nos inspiren y den esperanza, confío que este fragmento de memoria colectiva nos permita seguir construyendo resistencia y resiliencia que contagien cada rincón de nuestro país y resuenen con las experiencias de nuestras hermanas de América Latina. Hablemos de la violencia digital como violencia sociopolítica.

Por un mundo donde quepan muchos mundos, por un mundo donde prevalezcan la memoria y la dignidad, por un mundo donde podamos acceder a la verdad, la justicia y la reparación.





En búsqueda de un cambio de narrativas en torno a la brecha digital y la marginalización en México

KARLA PRUDENCIO

Karla ha trabajado con comunidades rurales e indígenas en México, abordando las complejidades en torno a la conectividad y los derechos digitales. Además, ha sido jefa de Incidencia legal en Redes A.C. e investigadora del Centro Mexicano de Tecnología y Conocimiento Comunitario (CITSAC) y en la iniciativa Rhizomatica. Es licenciada en Derecho por parte del CIDE y maestra en Derecho, Ciencia y Tecnología por la Universidad de Stanford. Fue asesora legal del Instituto Federal de Telecomunicaciones de México y jefa de la Oficina de Transparencia y Protección de Datos del Centro de Investigación y Docencia en Economía (CIDE).

016

EN EL CONTEXTO DE LA PANDEMIA por COVID-19, en México, como en el resto del mundo, se expusieron de manera violenta las desigualdades estructurales que subyacen en el país. La discriminación sistemática e institucional, aunada a la ausencia de un enfoque preventivo cultural y socialmente adecuado —incluyendo la falta de provisión de servicios básicos, personal médico y de abasto continuo de medicamentos—, delineó un panorama desalentador para las comunidades históricamente vulneradas por el Estado, como los pueblos y comunidades indígenas y las zonas rurales[1].

La respuesta de muchos países ante la pandemia fue la digitalización de las actividades de la vida cotidiana y el uso de la conectividad como una medida paliativa para el ejercicio de derechos fundamentales —dígase acceso a la educación o la salud, por mencionar algunos ejemplos—. Sin embargo, en México, un país multinacional y con múltiples realidades, se hizo todavía más evidente que los beneficios de la tan esperada "revolución digital" sólo habían llegado a unas cuantas personas y territorios.

---

[1] Aura Investigación Estratégica, Centro de Capacitación en Ecología y Salud para Campesinos, Defensoría del Derecho a la Salud (CCESC), et al. (2020). *Los pueblos y comunidades indígenas frente al COVID-19 en México*. Recuperado el 6 de junio de 2021, disponible en https://www.ohchr.org/Documents/HRBodies/SP/COVID/NGOs/Centro_de_Derechos_Humanos_de_la_Monta%C3%B1a_Tlachinollan.pdf

Aun así, la problemática de la brecha digital predominó en la agenda pública del gobierno, del sector privado y del sector social. A pesar de la diferencia de enfoques y perspectivas, se reforzó una narrativa dominante y utilitarista que desde entonces parece apuntar a objetivos y soluciones unidimensionales, enfocados en acelerar la reducción de la brecha digital para combatir la marginalización de estos territorios. De acuerdo con esta narrativa, la pandemia parecía el pretexto perfecto para dar el último "empujón digital" en México. Con esto, se podría, entre otras cosas, potenciar la economía, impulsar a las pequeñas y medianas empresas y facilitar determinados procesos industriales[2].

Pero ¿qué significa reconocer una multiplicidad de experiencias y realidades?, ¿cómo podemos encontrar soluciones que sean respetuosas con la diversidad de metas y sueños dentro de los distintos territorios que existen en México?, ¿cómo desarrollamos políticas de conectividad que sean congruentes con un enfoque de derechos humanos? En el presente texto no pretendo responder de manera exhaustiva a estas preguntas, sino mostrar que existen alternativas contrahegemónicas que responden a la problemática de la "bre-

[2] Algunos ejemplos de estas narrativas se encuentran en las siguientes ligas: https://www.forbes.com.mx/como-la-digitalizacion-puede-ser-una-palanca-para-enfrentar-los-efectos-del-covid-19/ y https://www.forbes.com.mx/negocios-digitalizacion-pymes-clave-crisis-covid/

cha digital" desde otras cosmovisiones y que tienen, por consiguiente, distintos resultados.

Primero, busco contestar a la pregunta de quiénes son y por qué están desconectadas estas personas, según las estadísticas oficiales. Después, planteo algunas hipótesis de por qué estos números no nos dejan ver las particularidades y diversidades que existen en el país y cuáles son las narrativas implícitas que están detrás de estas estadísticas. En la tercera sección propongo ideas para cambiar estas narrativas y, en la cuarta, expongo por qué los distintos modelos de conectividad son necesarios para poder lograr este cambio. Finalmente, busco hacer una defensa de la utopía y muestro algunos ejemplos donde estos sueños se han hecho realidad.

LOS DATOS DUROS: ¿QUIÉNES SON Y POR QUÉ ESTÁN DESCONECTADOS?

Si analizamos los datos oficiales sobre la brecha digital en el país, es posible observar una diferencia significativa entre aquellas personas que tienen acceso a internet —u otras tecnologías— y las que no. En México, sólo el 70.01% de la población es usuaria de internet[3]. Es decir, que al-

[3] INEGI. (2019). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2019*. Recuperado el 10 de julio de

rededor del 30% de la población no cuenta con acceso a esta tecnología. Este 30%, además, se encuentra mayoritariamente en zonas rurales, con una diferencia comparativa con las zonas urbanas del 28.9%[4]. Por otro lado, alrededor de 5,200 localidades en las que existe población indígena —al menos un 40% de las localidades con esta población— se encuentran completamente fuera de los circuitos de cobertura de redes de telecomunicaciones fijas y móviles de banda ancha. Estamos hablando de aproximadamente 3 millones de personas que no tienen acceso a ninguna tecnología digital[5].

Al analizar las estadísticas a nivel hogar, es posible encontrar una diferencia aún más significativa entre las personas que tienen acceso y las que no, pues sólo el 44.3% de las personas tienen acceso a un dispositivo en su hogar (computadora de escritorio, computadora portátil o tableta electrónica)[6]. Esto, por supuesto, tiene

---

2021, disponible en https://www.inegi.org.mx/programas/dutih/2018/.

[4] Ídem.

[5] Secretaría de Comunicaciones y Transportes. (2019). *Programa de cobertura social 2019*. Disponible en https://www.gob.mx/cms/uploads/attachment/file/500252/2019-10-02_PCS_version_web_miercoles_9_octubre.pdf

[6] IFT con datos de la ENDUTIH 2015-2019. La ENDUTIH 2019 no es representativa a nivel estatal, por lo que sólo se muestran resultados a nivel nacional. Disponible en http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/evolu-

impacto —no necesariamente negativo— en lo que las personas pueden o no hacer con la conectividad y cómo pueden ejercer sus derechos a través de internet. A estas alturas parecería una obviedad mencionarlo, pero cualquier política pública que se diseñe y se ejecute en pos de la digitalización de determinadas actividades cotidianas, tiene que tomar en cuenta esta variación de realidades y contextos.

La primera pregunta que nos tendríamos que hacer cuando observamos estas cifras es: ¿por qué no tienen acceso estas personas? De acuerdo con las estadísticas oficiales, la principal razón por la que no tienen acceso a internet en sus hogares es porque aún es un servicio inaccesible para una gran parte de la población. Es decir, el 56.4% de las personas reportan que el mayor obstáculo es el costo que tiene el servicio, seguido de la falta de interés en contar con esta tecnología (20.9%). Por último, el 10.6% de las personas reportan que no tienen acceso en sus hogares porque no lo saben usar y el 8.0% por falta de infraestructura —es decir, en sus localidades no hay cobertura[7].

---

ciondelastic2015-2019_0.pdf

[7] Ídem.

Las estadísticas oficiales no están suficientemente desagregadas para permitirnos saber exactamente quiénes son y dónde se encuentran las personas que no tienen acceso a internet u otras tecnologías de la información. Tampoco nos dicen qué significa la "falta de interés" de las personas usuarias o cuáles son las decisiones de consumo que tienen que hacer estas personas y que resultan en que sea incosteable el servicio de acceso a internet. Es importante tener datos claros, abiertos y desagregados, para que estos nos permitan hacer un buen diagnóstico de la problemática y, consecuentemente, generar soluciones acordes a las distintas realidades que conviven dentro de nuestro país.

Sin embargo, la creación de políticas públicas que respondan solamente a datos estadísticos generados por el propio Estado —por más completos y desagregados que estén— lleva consigo algunos problemas de fondo que vale la pena explorar, pues suponen un tipo de arreglo del mundo en conjuntos o categorías predeterminadas. Estas categorías suelen responder a las preguntas e inquietudes de las personas que observan (en este caso los distintos Estados) y no de aquellas personas o comunidades que son observadas (que se encuentran del otro lado de la brecha digital).

En el caso de pueblos indígenas, por poner un ejemplo, se utilizan conceptos que no son los

pertinentes no sólo respecto del contenido, sino también en relación con el control y la gestión de la información. Además, se muestra continuamente el desconocimiento de los sistemas de información y conocimiento de los pueblos indígenas, desechando las categorías que ellos establecen para medir su bienestar, como el buen vivir o vivir bien[8]. A continuación, se explican algunas de estas problemáticas más a fondo.

La primera pregunta a la que responden de manera poco adecuada las estadísticas es: ¿quiénes son estas personas que habitan del otro lado de la brecha? Como mencionamos anteriormente, lo que no nos dicen estos números y porcentajes es quiénes están detrás de las cifras y cómo son sus territorios y realidades. La diversidad de sueños, formas, cosmovisiones y ecosistemas en los que habitan se desdibuja con el fin de insertar la diversidad en categorías fijas que dividen al mundo en zonas urbanas, rurales e indígenas, sin reconocer los matices y la pluralidad que existen dentro de estas mismas clases. Esto no es menor, pues la invisibilización constante de las particularidades y diferencias resulta en el diseño y ejecución de políticas públicas encaminadas a "cerrar la brecha digital" que no

[8] Comisión Económica para América Latina (CEPAL). (2014). *Los pueblos indígenas en América Latina. Avances en el último decenio y retos pendientes para la garantía de sus derechos*. Chile: ONU. Disponible en https://repositorio.cepal.org/bitstream/handle/11362/37050/4/S1420783_es.pdf

atienden de manera concreta a las necesidades, objetivos y sueños de las personas o de las comunidades destinatarias de las políticas.

Lo anterior nos lleva a la segunda problemática: ¿qué es lo que realmente estamos midiendo? El concepto o la idea de la brecha digital divide a las personas mediante dos categorías absolutas y cerradas: "desconectados y conectados", y lleva implícita la narrativa de que las personas desconectadas están en evidente desventaja frente aquellas personas que están conectadas[9]. Por lo tanto, se asume que la conectividad tiene que "otorgarse" a estas comunidades o pueblos, pasando por alto quiénes son o qué es lo que quieren y cuáles son sus objetivos en cuanto a la adopción de tecnologías[10].

El académico Ulises Mejía hace notar que, aunque algunos países "en desarrollo" siguen teniendo problemas para cerrar la brecha digital —de internet—, esto no necesariamente significa que las personas que sin acceso estén completamente desconectadas, pues en muchas ocasiones existen otras tecnologías que permiten la comunicación y conexión entre los miembros de la comunidad[11]. Un ejemplo es la penetración de

[9] Bloom, P. y Prudencio, K. (2021). Keeping it Analog: A framework for opting out of connectivity. *Rhizomatica*. Disponible en https://www.rhizomatica.org/mantenlo-analogo-parametros-para-una-exclusion-voluntaria-de-la-conectividad/

[10] Ídem.

[11] Mejías, U. (2013). *Off the network: Disrupting*

comunicaciones móviles o los proyectos de radios comunitarias que permiten la comunicación efectiva en zonas donde no hay conectividad a internet. Las comunidades, en muchas ocasiones, están ejerciendo sus derechos, aunque no sea como lo imaginamos.

Observar cómo algunos grupos y comunidades indígenas ya utilizan ciertos métodos de comunicación análogos (y en algunas ocasiones digitales, distintos al internet) para compartir conocimiento referente a la autonomía y la autodeterminación —contando historias, compartiendo información y datos con unos y otros— pueden darnos alguna luz sobre cómo estos pueblos ya utilizan de manera subversiva los sistemas de información y las tecnologías para su propio desarrollo[12]. Estas historias no son contadas por las estadísticas oficiales.

Lo que también invisibilizan estos números es la causa de esa falta de acceso en ciertas comunidades y territorios. La división simplista basada en cuatro razones por las que las personas no están conectadas no permite entender las raíces estructurales que hay detrás. En muchas ocasiones, las causas son la discriminación, marginalización y exclusión de estos pueblos, de sus for-

---

the Digital World. EUA: University of Minnesota Press. Disponible en https://www.jstor.org/stable/10.5749/j.ctt3fh6jh.4

[12] Marisa Duarte, M. (2017). *Network Sovereignty, Building the Internet Across the Indian Country*. EUA: University of Washington Press.

mas de vida y de su cosmovisión. Por ejemplo, "el no interés", que es la segunda causa por la cual las personas no tienen acceso a internet dentro de sus hogares, se puede interpretar de distintas maneras. La falta de contenido en su lengua[13] o la falta de condiciones para que las comunidades generen contenido culturalmente pertinente es una manera estructural de entender el problema de acceso que va más allá de la falta de un interés individual. Ir a las causas de fondo permite también observar cuáles son las condiciones necesarias para hacer del internet una tecnología que sirva para el ejercicio de derechos humanos de todas las personas y en todos los lugares.

Por último, lo que estas estadísticas no dicen es lo que sí hay y lo que ya se está construyendo. Frente a estos contextos de marginalización y exclusión existen alternativas que se gestan dentro y por las propias comunidades, y dentro de las zonas sin acceso a internet. Alternativas en las que no sólo se resiste a las iniciativas que vienen de fuera y que pretenden homogenizar con soluciones unidimensionales, sino que también se reapropian de las Tecnologías de la Información (TIC) y que generan otras maneras de alcanzar los sueños, de contar historias y de forjar sus propios destinos y realidades tecnológicas.

[13] Para ver algunas estadísticas: https://www.internetworldstats.com/stats7.htm

El primer paso para generar un ambiente habilitador en el que las personas puedan acceder a las tecnologías, y estas signifiquen un mejor ejercicio de los derechos humanos, es reconocer quiénes son realmente estas personas y escucharlas. Generar un espacio en el que puedan contar sus historias, "asumiendo que las personas son expertas de sus vidas, que la experiencia es política y que todas las personas están en un proceso constante de significar y resignificar su experiencia"[14].

En este sentido, un diagnóstico efectivo y completo implica conocer más que datos duros y porcentajes sobre la situación general de la brecha digital, sino que tiene que mostrar los resultados de procesos de reflexión profundos y acordes a los distintos contextos. Las agendas públicas, por más urgentes que sean, tienen que realizar este ejercicio para crear políticas públicas, leyes e iniciativas que sean realmente significativas en estos lugares y para estas personas.

El segundo paso es generar espacios para que las comunidades repiensen y cuestionen la introducción de determinadas tecnologías en sus territorios. Como mencionamos anteriormente, conectarse no significa necesariamente conec-

[14] Para conocer más sobre las prácticas narrativas: https://colectivo.org.mx/

tarse a internet, sino que hay un sinfín de opciones tecnológicas que responden a los objetivos comunicativos o de información de estos lugares.

Algunas experiencias nos dan un poco de luz sobre cómo hacer esto. Por ejemplo, Redes por la Diversidad Equidad y Sostenibilidad A.C. (REDES A.C.)[15] es una organización que trabaja para generar condiciones que permitan a los pueblos indígenas contar con medios de comunicación propios que atiendan a sus principios y valores, así como acceder a medios no indígenas sin discriminación. A lo largo de su caminar, REDES A.C. se ha cuestionado cómo tienen que generarse estas condiciones para que se les permita a los propios pueblos decidir sobre el uso e introducción de determinadas tecnologías.

A través del manual *¿Y si repensamos las tecnologías de la información?*[16], REDES A.C. propone una metodología que pone en el centro estos cuestionamientos sobre el uso y la apropiación de las tecnologías en las comunidades "desconectadas". Partiendo de la idea de que las TIC no son herramientas neutrales, sino que han sido creadas por intereses particulares y con fines muy específicos, la propuesta consiste en gene-

[15] Para más información sobre la organización: https://www.redesac.org.mx/

[16] Parra, D. y Baca, C. F. (2020). *¿Y si repensamos las tecnologías para la comunicación?* México: REDES A.C. Disponible en https://ed8169c2-0818-439d-b473-11f6b06914e9.filesusr.com/ugd/68af39_f3ccc6549625453ba8ef88a00b69f558.pdf

rar procesos en los que las tecnologías se conviertan en "aliadas para la preservación de la vida comunitaria"[17].

Hacer esto realidad pasa por comprender que la conectividad no es un fin en sí mismo, sino que tiene que estar al servicio de los distintos pueblos y comunidades, y de cómo deciden ejercer sus distintos derechos, incluyendo el de la comunicación. Es decir, la conectividad tiene que ser percibida como una herramienta que ayuda a "fortalecer la identidad, la autonomía, la defensa del territorio y la vida, entre otros objetivos"[18].

La creación de sistemas de información y diagnósticos adecuados, así como la creación y aplicación de este tipo de metodologías que nos permitan generar cuestionamientos sobre el uso y la apropiación de ciertas tecnologías, son indispensables si queremos trabajar a favor del acceso a las TIC. Como se mencionó anteriormente, una vez realizado este proceso es más fácil generar soluciones que sean acordes con los sueños, las cosmovisiones y los modos de vida de las comunidades y de las zonas no conectadas.

---

17 Ídem.

18 Ídem.

¿POR QUÉ SON IMPORTANTES LAS ESTRATEGIAS LOCALES DE CONECTIVIDAD?

Decidir conectarse a internet no es una decisión sencilla ni tiene respuestas predeterminadas. Sin embargo, existen comunidades que deciden hacerlo porque ven en esta tecnología una herramienta útil para el ejercicio de sus derechos humanos, como la libertad de expresión, el acceso a la información o el derecho a la comunicación. En este punto, es importante recalcar que la decisión no debería de quedarse ahí, pues cómo se llega o establece esta conectividad es casi tan importante como el acceso mismo. En este sentido, existen modelos que potencian el ejercicio de los derechos humanos, mientras que otros lo socavan o lo dificultan. Unos modelos son más respetuosos del proceso de decisión de las comunidades sobre cómo quieren forjar sus destinos digitales y sobre los principios alrededor de los que se tiene que construir esta conectividad.

Las redes comunitarias son redes de telecomunicaciones (intranet, internet o telefonía móvil) que son propiedad de las comunidades y no tienen fines de lucro. Las mismas comunidades diseñan, gestionan y operan estas redes. Más que una solución técnica, las redes comunitarias son "un tejido que está compuesto por personas, tecnologías, acuerdos, que se entrelazan en re-

laciones que constituyen la red"[19]. Numerosos estudios y artículos apuntan a las ventajas técnicas y económicas de instalar estas redes —sobre todo en comparación de otros modelos provenientes del Estado—[20]. Sin embargo, su mayor ventaja es que en su proceso de instalación, desarrollo y mantenimiento siempre está involucrada la comunidad, por lo que el proceso de reflexión se encuentra de alguna manera garantizado. Esto no sólo implica que tomarán decisiones técnicas más acordes a sus realidades y necesidades, sino que se construirán bajo los principios de uso que les parezcan más convenientes. Las redes comunitarias, entonces, generan círculos virtuosos en los que las comunidades tienen más oportunidades de moldear su futuro digital.

EN DEFENSA DE LA UTOPÍA

Para las personas que toman decisiones y para las que diseñan políticas públicas lo aquí expuesto parece una utopía. Reconocer la diversidad de realidades implica también reconocer que las fórmulas predeterminadas no existen, que los procesos son lentos y en muchas ocasio-

[19] Redes Comunitarias en Colombia. *¿Qué son las redes comunitarias?* Disponible en: https://redes-comunitarias.co/es/que-son-las-redes-comunitarias

[20] Para más información: https://www.apc.org/en/topic/community-networks

nes es imposible medirlos con los indicadores de éxito tradicionales. Comprometerte con estas metodologías implica también analizar y hacerse cargo de las desigualdades estructurales y de las problemáticas de raíz, buscando soluciones de fondo y que sean definitivas. Finalmente, resulta imprescindible comprender que lo que significa progreso para algunas personas es dañino para otras, pues no se respetan los principios fundamentales desde los que se observa la vida.

En la mayoría de las ocasiones, lo que tienen que hacer las personas que quieren involucrarse en estos procesos es simplemente facilitar lo necesario para que estas comunidades, en ejercicio de su autonomía y autodeterminación, planteen y ejecuten las soluciones que crean más convenientes. En otros casos, si las personas involucradas así lo desean, pueden generar condiciones para el diálogo e intercambio entre distintos actores, y la facilitación y acercamiento de algunas herramientas. Lo importante es reconocer que existen muchas maneras de hacer realidad estas utopías, pues al final lo que exige el marco aquí planteado es un compromiso con la vida, con la pluralidad, con la libertad, con la justicia social y con los derechos humanos. Lo que tenemos que hacer para que esto se vuelva realidad es observar respetuosamente lo que ya existe, los futuros que se han imaginado y poner las tecnologías al servicio de estos sueños. Esta es la única manera permanente de "cerrar la brecha digital".

Frente a las personas incrédulas de que estos procesos son posibles, siempre existen las experiencias y las vivencias que muestran que las utopías son realizables. Frente a aquellas personas que insisten en una categoría fija para insertar a los desconectados, siempre existe la posibilidad de enseñarles procesos de comunicación autogestivos. Procesos que muestran que estos pueblos y comunidades están conectados a lo que verdaderamente importa: la defensa de la tierra, de la vida y de la comunicación. Procesos que muestran que no hay cajitas o categorías fijas en las que quepan la diversidad y la pluralidad de estas experiencias e historias. Frente a un contexto de mercantilización y colonización tecnológica, siempre estarán las experiencias de las personas que se reapropian y resisten, que crean y que sueñan con otros destinos tecnológicos. No necesariamente mejores, sino distintos. Cuando las preguntas son impuestas, es importante generar las propias, que tengan sentido y que reflejen lo que somos.

En un panorama de desinformación y, en el mejor de los casos, de información no pertinente para ciertas poblaciones, nace la Iniciativa Tlayolchikawalis[21]. Tayolchikawalis es una palabra que deriva de la palabra yolchikawalis, que en

[21] Para más información sobre la iniciativa: https://tayolchikawalis.org/

náhuatl significa “la fuerza del corazón”. Esta iniciativa fue lanzada por la Unión de Cooperativas Tosepan —ubicada en Cuetzalan, Puebla— y busca generar acciones de largo aliento para responder a la pandemia causada por COVID-19.

Estas acciones incluyen generar información específica, reforzar acciones de prevención de la salud y prever acciones solidarias desde las comunidades ante la posibilidad de contagio. Es, entre otras cosas, una campaña de comunicación muy efectiva que utiliza todas las tecnologías y medios que tiene a su alcance la comunidad. En última instancia, lo que se busca es “desde las prácticas indígenas, cambiar la inercia actual de miedo y alejamiento entre las personas, en el contexto de la enfermedad”[22]. La iniciativa Tlayolchikawalis, entonces, es una prueba de lo que sí puede hacerse y de cómo las comunidades cuentan con sus propios sistemas de información y comunicación.

Otro ejemplo de lo que sí es posible lo encontramos en Oaxaca, donde reside Telecomunicaciones Indígenas Comunitarias (TIC A.C.)[23]. TIC A.C. es una asociación civil conformada por comunidades indígenas y rurales de México y por un equipo operativo que acompaña a personas y comunidades que buscan construir, gestionar y operar sus propias redes de comunicación. Jun-

[22] Ídem.

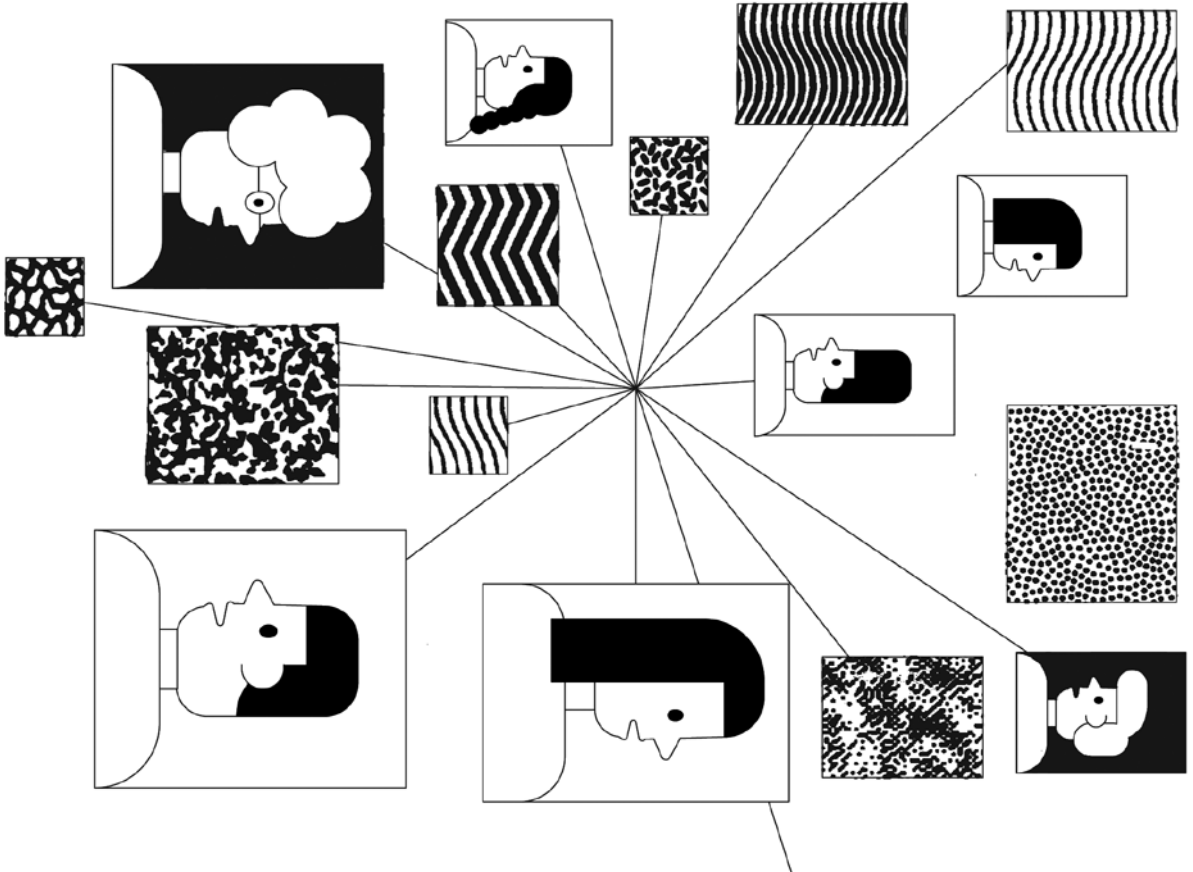
[23] Para más información sobre la organización: https://www.tic-ac.org/

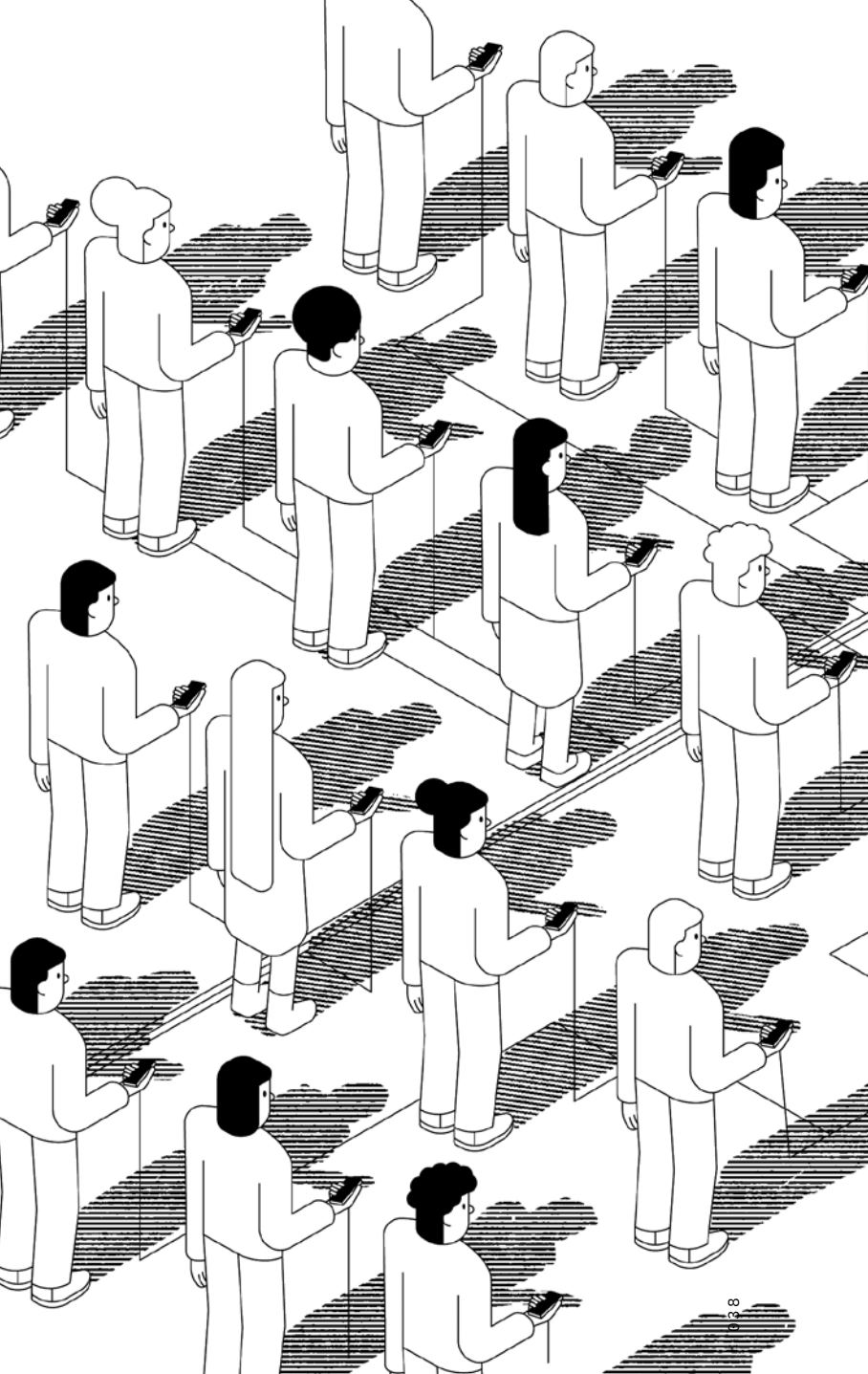
to con 16 comunidades indígenas, obtuvo en 2016 una concesión de uso social para administrar y operar redes de telecomunicaciones y radiodifusión autónomas, entre ellas, la telefonía celular. TIC A.C. busca construir alternativas de telecomunicaciones autónomas, seguras y asequibles, que fortalezcan los procesos de comunicación, el buen vivir y el marco de derechos humanos. Iniciativas como TIC A.C. muestran que es posible generar modelos de conectividad autónomos, desarrollados y gestionados por las propias comunidades y que respondan a sus requerimientos y necesidades. En la actualidad, esta iniciativa busca transitar de sus redes de telefonía celular (2G) a redes 4G, como resultado de un proceso cuidadoso de diagnóstico en el que se determinó que esto es lo que las comunidades pertenecientes a la asociación necesitan.

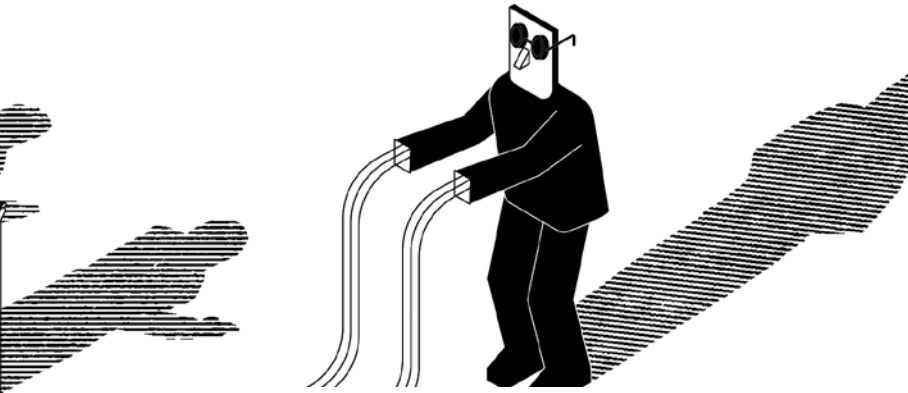
Como estos dos ejemplos, existen muchos más en el país. Territorios que se están organizando para usar las tecnologías de manera creativa y al servicio de las comunidades, con una perspectiva de derechos humanos. Cerrar la brecha digital implica también ver estas soluciones y modelos, aprender de ellos, replicarlos y adaptarlos cuando sea necesario.

El tema de la brecha digital es complejo. A menudo, escuchamos soluciones que parecen simples y discursos que simplifican la problemática. Ante este tipo de narrativas y respuestas rápidas es necesario parar y reflexionar sobre las perspectivas y los mandatos en materia de derechos humanos, ¿qué implica entender la brecha digital desde esta perspectiva?, ¿cómo generamos estrategias acordes y respetuosas de la diversidad y pluralidad?

Los cambios que se requieren no son menores, pero tampoco son imposibles. Ante una realidad donde se han construido tecnologías dominantes que han causado perjuicios a los derechos humanos, buscamos procesos distintos que nos permitan reapropiarnos y transformar los entornos digitales en los que vivimos. Ante la brecha que divide al mundo en dos, respondemos con una multiplicidad de realidades y soluciones. Ante la clasificación desde la mirada ajena, la creación de sistema de información propios. Ante lo que invisibiliza, la visibilidad de nuestra palabra y de nuestros sueños.







Autoritarismo y vigilancia: frente a las distopías tecnológicas, caminemos hacia utopías sociales

SURSIENDO, COMUNICACIÓN Y CULTURA DIGITAL

Sursiendo nació en mayo del 2011 como una iniciativa para abordar la defensa de la comunalidad digital, los derechos digitales colectivos y los hackfeminismos; aportando al cambio social desde la autonomía digital. En 2015, esta organización radicada en Chiapas se conformó como asociación civil para seguir promoviendo reflexiones en torno a internet como un espacio social que posibilita un gran número de las acciones que ejercemos en la actualidad y los componentes políticos detrás de ellas, a partir del trabajo que realizan con grupos y organizaciones civiles en el sureste mexicano.

“NO ESPERES A SER CAZADO
PARA ESCONDERTE...”

SAMUEL BECKETT

(EN MARCUSE, 1965)

IMAGINA QUE UN GRUPO de jóvenes se moviliza en algún estado del sur de México porque no tienen acceso a realizar exámenes de admisión en una universidad o escuela. Imagina que a las y los integrantes de ese grupo movilizado reivindicando sus derechos les vigilan desde drones y desde cámaras de reconocimiento facial situadas en las calles, después los rastrean desde sus dispositivos móviles, les bloquean sus cuentas en redes o sus números de teléfono. Imagina que después de ubicarles y silenciarles son detenidos y detenidas, sufren torturas y violaciones, sin ninguna repercusión ante el gran flujo constante de información que nos rodea.

Imagina que después de pasarle esto a los y las estudiantes, le ocurre algo parecido al magisterio movilizado, a campesinos y campesinas, al sector salud inconforme, a las movilizaciones feministas, a quienes escriben en Twitter o Facebook críticas a decisiones políticas.

Parece el argumento de algún relato futurista, pero existe la posibilidad realista de que pueda ocurrir. Y de hecho, están ocurriendo sucesos parecidos. Existen las capacidades tecnológicas y, en algunos casos, la voluntad política para que estemos dando pasos hacia ese tipo de situaciones que vulneran gravemente derechos democráticos básicos, como son la libertad de expresión, el derecho de manifestación y reunión, a la crítica y la protesta, y, en definitiva, también contra el derecho a la intimidad, al trabajo, a la educación, al conocimiento, a tener una vida digna.

En Sursiendo venimos acompañando en cuidados digitales a organizaciones sociales y colectivos del sur-sureste de México desde hace ya varios años, y nos encontramos con cada vez más casos de incidentes digitales. Conocer el contexto de vigilancia global y los usos de las tecnologías digitales nos sirve para mejorar nuestras prácticas y formaciones, y en el trabajo en el entorno local nos ayuda a comprender la magnitud del problema y los retos que enfrentamos. Lo vemos como un puente que transitamos en los dos sentidos, para fortalecer las prácticas de defensoría de activistas y defensoras de derechos humanos.

La tecnología a lo largo de la historia ha servido y sirve para el crecimiento humano, pero también para ir contra las poblaciones y sus derechos, y la mayoría de las veces depende de decisiones políticas, no técnicas. Es decir, las decisiones técnicas que se toman para hacer uso de las tecnologías dependen de concepciones políticas, de formas de concebir los entornos sociales.

Un ejemplo clásico de los usos perversos de las tecnologías es el de la Alemania nazi. Cuando el partido de Hitler llegó al poder, impulsó el Ministerio de Propaganda, dirigido por Joseph Goebbels desde 1933, que tomó el control de todas las formas de comunicación de Alemania: periódicos, revistas, libros, música, cine y radio. Desde ese momento la censura a voces diferentes y el uso de las tecnologías al servicio de la propaganda se convirtió en la norma. Particular-

mente interesante es el caso de la radio, que ofrecía todas las posibilidades de ser arma de propaganda masiva, ya que era la forma más popular de informarse en aquel entonces. Consignas, criminalización, violencia verbal e intimidaciones se lanzaban de forma constante. Por si no llegaba a todo el mundo, Goebbels ideó la "radio del pueblo" (la Volksempfänger), un aparato simple y barato, que por su escasa sensibilidad impedía sintonizar emisoras extranjeras. Así, Alemania se convirtió a finales de los años treinta en el país con más radios de Europa, el 70% de los hogares contaba con uno. Y no sólo en los hogares se escuchaba la radio, también colocaron centenares de bocinas en espacios públicos para transmitir la programación. Esas bocinas se multiplicaban cuando había mítines y actos políticos, que usaban con atronadora música militar o sinfónica, y con los teatrales efectos lumínicos para acompañar los discursos. También el cine, que empezaba a cobrar popularidad, fue utilizado para la propaganda nazi.

Es un caso paradigmático, que se estudia en las facultades de comunicación, pero los hay más cercanos y más actuales. El expresidente de los Estados Unidos Donald Trump utilizó Twitter para difundir noticias falsas y generar polarización; Facebook se ha alimentado de las fake news, e influyó de forma poco ética en la elección del propio Trump; de Jair Bolsonaro, en Brasil; del referéndum para la separación del Reino Unido de la Unión Europea (Brexit), y muchos

otros casos documentados. Como decía el propio dirigente nazi Goebbels: "una mentira repetida mil veces se convierte en una verdad", y ahora los gobiernos, partidos, corporaciones y demás organismos con poder tienen los mecanismos —en forma de redes y algoritmos— para que esa mentira llegue personalizada a cada grupo o persona, y la repiten muchas veces.

Una tecnología digital personalizada que también sirve para ubicarnos, perfilarnos, escucharnos y vigilarnos. En México, hace algunos años nos sorprendió saber que la Procuraduría General de la República (PRG) y la Policía Federal (PF) tenían departamentos en los Estados de toda la República con personas encargadas de monitorear las redes sociales y dar seguimiento a personas activistas, periodistas y organizaciones y movimientos sociales del país, ya no nos sorprende.

Con los años, hemos conocido, a través de filtraciones e informes independientes, que existe vigilancia en México —y en otros países del entorno— contra voces críticas, activistas e investigadores. Además de la posibilidad de la vigilancia y el control social contra amplios sectores de la población. El reciente intento de aprobar la creación un padrón de datos personales y biométricos de todas las personas que tengan una línea telefónica apunta a esta posibilidad, que atenta contra derechos básicos.

Las herramientas tecnológicas dependen mucho de la forma en las que se usen, pero, aun así,

hay que decir que las tecnologías no son neutrales, sino que pueden estar, consciente o inconscientemente, creadas con características que generen ciertos tipos de conductas políticas, sociales y económicas. Como dice la investigadora Lila Pagola: "Las tecnologías no son inocentes, ni neutrales. Forman un todo con un programa económico y político que las promueve en algunos de sus aspectos e invisibiliza otros". Dependen de quien las diseñe, programe, promueva, compre y utilice.

INTERNET

Pongamos por ejemplo a internet. La llamada "red de redes" de la que tanto dependemos en la actualidad es una serie de máquinas, antenas, cables y herramientas de software, que finalmente hacen que sea un conjunto descentralizado de redes de comunicación interconectadas, que lamentablemente cada vez está más concentrado en un puñado de corporaciones.

Internet nació con dinero de fondos militares. Un grupo de investigadores convenció a finales de los años sesenta al Departamento de Defensa de los Estados Unidos para crear una red descentralizada de información para que, en el caso de ocurrir un ataque soviético, no se perdiesen las comunicaciones. Así nació ARPANET, con el primer nodo creado en la Universidad de California en Los Ángeles (UCLA), y su primera conexión

con el enlace con la Universidad de Stanford. Con los años fue creciendo y siendo impulsada desde la investigación y la academia, por personas con ideales de libertad y solidaridad. Recordemos que en los Estados Unidos en los años sesenta se produjo el boom de la contracultura, de las libertades, el espíritu crítico y la experimentación, y de alguna forma se plasmó en esta red.

Pero internet se usaba y se mantenía entre cientos de personas relacionadas con las tecnologías, y no es hasta 1990 cuando comienza a extenderse la World Wide Web, lo que conocemos por "la web", creación de Tim Berners-Lee, quien no patentó su protocolo, sino que lo ofreció libre y abierto a la sociedad. Este "simple" hecho abrió la posibilidad de hacer crecer la red hacia lugares inimaginables por ese entonces. Con los años se han ido sumando millones y millones de personas a usar la web, a navegar, intercambiar información, encontrarse, crear, expresarse, trabajar, estudiar, explorar su sexualidad, pasar su tiempo de ocio.

Un punto de inflexión se produjo en el año 2006, cuando la empresa Google compra la plataforma de videos YouTube y se lanza la red social Facebook para que pueda registrarse cualquier persona mayor de 13 años. En la efervescencia de la internet participativa, la web 2.0, estas empresas aprovecharon para posicionar sus productos e ir haciéndose con todo el pastel. Desde entonces han ido creciendo tanto que no solamente son corporaciones monopóli-

cas, sino que también tienen poder para influir en las decisiones políticas de las grandes potencias mundiales.

Así, a partir de la segunda década del siglo XXI este cambio se fue agudizando: la mitad de la población se conecta a internet, aunque sigue habiendo grandes desigualdades entre los países del norte y los del sur, entre las ciudades y el mundo rural, entre hombres, mujeres y personas de la disidencia sexual, entre jóvenes y ancianas; pero, sobre todo, uno de los cambios más decisivos ha sido el gran poder adquirido por las corporaciones tecnológicas. De la descentralización se ha pasado a la gran concentración. De la libertad que dan los sitios web se ha pasado a las aplicaciones y plataformas cerradas. Monopolios y cercamientos creados desde el Imperio GAFAM (Google, Amazon, Facebook, Apple y Microsoft), que controlan y deciden cómo nos manejamos en las redes sociales.

Incluso Berners-Lee muestra gran preocupación por la deriva que está tomando internet y en los últimos años está impulsando diversos proyectos que buscan "restaurar el poder de los usuarios en la red", y así volver a los valores originales. En ese camino habrá que considerar que esos valores originales necesitan ser revisitados y actualizados para fortalecerlos de acuerdo con lo que hoy muchas personas y movimientos sociales consideran inclusión, atendiendo a las brechas de conectividad, género y apropiación existentes, por mencionar sólo algunas, porque

estos imperios y sus alianzas políticas basan su economía e infraestructura en la comercialización de nuestra identidad personal, de nosotros y nosotras. Es el nuevo extractivismo, el nuevo colonialismo corporativo.

No sólo existe el problema de la vigilancia, de la comercialización de nuestros datos personales, de la gran influencia política y el monopolio económico, todo ello muy grave, sino también el exponencial aumento de los residuos electrónicos y de las emisiones de gases de efecto invernadero, la extracción de materias primas para los aparatos e infraestructuras, el uso masivo de agua para enfriar los centros de datos, el inmenso consumo energético, la precarización de las condiciones laborales, más problemas de salud, polarización social y violencias machistas, racistas y clasistas en redes. Y la cada vez mayor dependencia de conexiones a internet y el uso de dispositivos electrónicos, se exacerba con el big data, la Inteligencia Artificial (AI), la robótica y, pronto, mucho más cuando se extienda el 5G y el Internet de las Cosas (IoT), internet puede llegar a ser una pesadilla.

VIGILANCIA

En 2010, la plataforma WikiLeaks publicó un video sobre crímenes de guerra del ejército de Estados Unidos en Irak y se hizo muy conocida. La viralidad de este contenido proporcionó un alta-

voz a esta organización internacional de filtraciones, que durante los siguientes años reveló documentos importantes sobre el uso que hacen de las tecnologías algunos gobiernos. Una de las filtraciones más famosas fue el llamado Cablegate, que suponía hacer públicos miles de documentos confidenciales y secretos del Departamento de Estado de los Estados Unidos, involucrando a decenas de otros países, y en los que se revelaban mensajes, informes y reportes sobre conflictos diplomáticos, espionaje a políticos, maniobras opacas y más, WikiLeaks ha sido atacada de todas las formas posibles.

En 2013, el analista estadounidense Edward Snowden, quien trabajó para diversas agencias de seguridad de Estados Unidos, reveló documentos confidenciales sobre espionaje digital, acuerdos entre corporaciones tecnológicas y el gobierno para hacer una recolección masiva de datos de la ciudadanía conectada a internet, y sus planes para aumentar esta vigilancia. Como explica Paola Ricaurte: "Las filtraciones de Snowden colocaron en la agenda política y mediática a nivel local y mundial la discusión acerca del poder del Estado y los derechos de los ciudadanos. La seguridad es el argumento que sostienen los Estados para justificar la vigilancia: un paradigma que se sitúa por encima del derecho a la privacidad". Snowden tuvo que huir y, tras ser perseguido, se encuentra refugiado en Moscú.

En 2017, en México, diversas organizaciones sociales hicieron pública la campaña "#Gobier-

noEspía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México". En ella exponían que desde 2011 distintas agencias públicas mexicanas han gastado millones de dólares en programas de espionaje, y destacados defensores de derechos humanos, periodistas y activistas han sido afectados por ellos. Desde la Policía Federal hasta el CISEN compraron software para espiar, entre los que destacan FinFisher, DaVinci y Pegasus. Con el apoyo de Citizen Lab, de la Universidad de Toronto, se analizaron mensajes y dispositivos. Por ejemplo, el malware Pegasus, vendido por la empresa israelí NSO Group a varios gobiernos del mundo, incluido el de México, funciona contagiando el teléfono celular a través de enlaces en mensajes, dando el control del aparato y su contenido al atacante. La mayoría de los casos que se conocen de Pegasus en México corresponden a 2016 y afectaron a periodistas (como Carmen Aristegui o Javier Valdés), a investigadores (Simón Barquera, del Instituto Nacional de Salud Pública) y a activistas (Alejandro Calvillo, director de El Poder del Consumidor, Luis Encarnación, coordinador de la Coalición ContraPESO y Mario Patrón, Stephanie Brewer y Santiago Aguirre, miembros del Centro Prodh, entre otras). Se sospecha por investigaciones independientes que este malware también fue adquirido por la Secretaría de la Defensa Nacional, la Procuraduría General de la República y el Centro de Investigación y Seguridad Nacional.

Ya antes sucedieron casos en Chiapas, Veracruz, Puebla y Ciudad de México, que se sepa, de casos en que se espiaba y se encarcelaba a activistas y comunicadores críticos, como con Gustavo Maldonado, Héctor Bautista o las iniciativas #OP5 Puebla y 1dmx.org; pero el caso de #GobiernoEspía es un salto cualitativo y cuantitativo, por usar software sofisticado que infecta al dispositivo, que es más rápido y eficaz, además de ilegítimo y violatorio de más derechos básicos.

Son ejemplos que se han ido conociendo. Muchos casos quedan aún en la oscuridad, sin ser hechos públicos. Y vemos alianzas público-privadas, de empresas del sector tecnológico y de la cibervigilancia con gobiernos nacionales, estatales o locales. Al día de hoy, la forma en la que la ciudadanía puede conocer el uso de este tipo de software vigilancia es por medio de filtraciones. En la mayoría de los casos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se niega a entregar este tipo de información aludiendo cuestiones de seguridad nacional.

Miramos con preocupación la deriva que esta situación toma de forma acelerada, ¿será que el tan criticado sistema de vigilancia chino es en realidad un horizonte deseado por nuestros gobiernos? El gobierno chino ha desarrollado una política de vigilancia que convierte al país asiático en una dictadura digital, con casi una cámara de vigilancia con reconocimiento facial por cada dos habitantes (600 millones repartidas por todo

el territorio), software de última generación, ejército especializado, y el ya famoso sistema de crédito social, que sanciona gravemente a millones de personas por no ser "buenas ciudadanas", basándose para su calificación en información que recoge del espionaje digital. Este mismo gobierno chino está invirtiendo millones de dólares en exportar su sistema a otros países, y ya hay algunos interesados.

Sin duda, esto es una distopía, cada vez más cercana, ¿ya vivimos en ella?, ¿podemos avanzar hacia una utopía? Distopía y utopía, dos palabras que tienen una raíz común, pero son opuestas. Una utopía se puede entender como la "representación imaginativa de una sociedad futura de características favorecedoras del bien humano", según las definiciones oficiales. Y una distopía, por el contrario, es "una sociedad ficticia indeseable en sí misma", una "utopía negativa". Muchas autoras y autores plantean que vamos hacia una distopía por culpa de las tecnologías, algo que la cultura popular también se encarga de imaginar. Recordemos las películas *Matrix, Blade Runner* y *V de Vendetta*, las novelas *1984* de George Orwell, *Fahrenheit 451* de Ray Bradbury y *The Hunger Games* de Suzanne Collins, o la serie *Black Mirror*; son sólo algunos ejemplos de cientos de obras, pasemos a desarrollarlas.

DISTOPÍA TECNOLÓGICA

Las distopías han servido a lo largo de la historia del arte para ser advertencias o sátiras de las tendencias presentes, imaginadas hasta sus consecuencias más extremas. Son el llamado de los peligros de perder valores esenciales: libertad, solidaridad, convivencia.

Los ejemplos tecnológicos abundan, además de los más populares que señalábamos antes. Siempre han ido de la mano el autoritarismo y el espionaje a la población. Ejemplos hay cientos en los últimos dos mil años, pero regresemos a Alemania, esta vez a la República Democrática Alemana (RDA), creada tras la Segunda Guerra Mundial. La Stasi, el órgano del servicio secreto de la RDA, es recordada por tener métodos de espionaje muy sofisticados, y mano dura contra las y los disidentes. *La vida de los otros*, muy buena película de 2006, que basándose en casos reales nos muestra cómo en 1984 un agente de la Stasi espía la casa de una familia de artistas por sus opiniones contra el gobierno.

Con las tecnologías en el siglo XXI, hemos vivido situaciones similares, con el añadido de las posibilidades que brinda lo digital: mayor alcance, mayor número, mayor invisibilidad, mayor velocidad y mayor sofisticación.

En México, como en la mayoría de los países, los casos del software espía y las alianzas público-privadas dan cuenta de lo que explicaban

hace unos años Javier de Rivera y Ángel Gordo: "En las primeras etapas de este fenómeno de informatización, celebramos los avances técnicos, las comunidades y nuevas opciones que traían: eliminando barreras a la comunicación social, estimulando a los movimientos sociales, fomentando la difusión del conocimiento, etcétera. Sin embargo, cada vez son más patentes los peligros y las amenazas detrás de esta hiperdigitalización del medio social, que se produce bajo las condiciones del tecnocapitalismo del siglo XXI". Las prácticas de las tecnológicas actuales responden al modelo disciplinario y las sociedades de control que teorizaba el filósofo Deleuze, con la referencia al panóptico foucaultiano, es decir, la posibilidad de ser vigilados en todo momento —y de forma retroactiva— gracias a los rastros digitales de nuestra actividad, sin que podamos, en ningún momento, darnos cuenta de cuándo y qué está siendo mirado, principal característica de la vigilancia electrónica; pero esta ya no busca solamente "disciplinar" los cuerpos en instituciones cerradas, sino "modelar" las actitudes a través de la estructura del sistema tecnológico.

Actitudes, expresiones, decisiones, opiniones, consumo, sueños que cuando son sociales pueden ser hechos predicciones y pueden ser condicionadas a través del big data. Este concepto comprende el desarrollo de sistemas de recopilación, gestión y procesamiento de cantidades enormes de datos que exceden la capacidad del software de hace pocos años. No se refiere ex-

clusivamente al volumen, sino también a la variedad y a la velocidad con la que estos datos pueden ser cruzados, representados y convertidos en información. Sectores empresariales de todo tipo y administraciones públicas ya han puesto sus ojos en esta tecnología como herramienta de gestión social a través del tratamiento de la información personal. En 2014, un informe encargado por la Casa Blanca concluye que, gracias a sus facultades para el rastreo a discreción, la publicidad dirigida o la predicción del comportamiento a partir de la huella digital, un nuevo poder está emergiendo alrededor del big data, y señala cómo está llamado a cambiar la manera en que nos comunicamos, trabajamos y vivimos en un entorno en el que la recolección de datos es cada vez más ubicua, multidimensional y permanente.

Cuando escuchamos la frase: "No importa que me espíen, no tengo nada que esconder", se cae en el error de no darse cuenta de que un poder que tenga acceso a toda información puede elegir a quién perseguir, cuándo y por qué. Y puede haber muchos intereses en juego, porque a la vigilancia "tradicional" que han vivido las organizaciones de derechos humanos, por parte de instancias públicas, empresas y delincuencia organizada —como recogimos en un informe de 2017— se suma ahora la vigilancia digital mediante dispositivos y redes sociales, junto al aumento de ataques pishing, ransonware y malware, suplantación de antenas para interceptar

información, apagones de señal, clonación de tarjetas, etcétera.

UTOPÍA TECNOLÓGICA

La palabra utopía casi siempre va en sintonía con las palabras liberación y equidad. Las utopías surgen en la Europa del siglo XV, a partir de Tomás Moro, con relatos sobre sociedades que funcionan bien, donde hay altos grados de felicidad. Suelen tener el objetivo de criticar el estado actual de las cosas, proponiendo cambios para obtener mejores resultados, señalando las desigualdades sociales que existen. Buscan mostrar el disfrute de los bienes comunes con equidad, por encima del individualismo. Y como podemos encontrar en la Wikipedia: aparece la crítica social "pero, a diferencia de las narraciones moralizantes o las sátiras, se propone una alternativa en la forma de una comunidad imaginada, la cual se ubica en los límites del espacio habitado".

En el mundo tecnodigital encontramos experiencias reconocidas que han buscado y siguen buscando la utopía. Hacemos un repaso rápido a algunas de ellas, que han inspirado a Sursiendo en nuestra trayectoria.

El software libre primero fue un gesto que después se convirtió en movimiento social. De la necesidad de adaptar un aparato a unas características concretas se ha pasado al fomento masivo de obtener y garantizar las libertades que permi-

ten a las personas usuarias de software el ejecutarlo, estudiarlo, cambiarlo y redistribuir copias del mismo con o sin cambios. Son las cuatro libertades del software libre, que se basa en tradiciones y filosofías de la cultura hacker y el mundo académico de los años setenta. Transparentar, compartir, colaborar, apasionarse y publicar son verbos que se conjugan en este movimiento, tan importante para que aún haya utopías tecnológicas. El movimiento copyleft nace con los aprendizajes del software libre, pero aplicado a licencias de obras y contenidos, contrario a la propiedad intelectual restrictiva. Liberar, compartir, adaptar, reparar están presentes en las posibilidades del copyleft, el inverso del copyright. Conformado por gente diversa, este movimiento quiere que todo el mundo tenga acceso a la cultura y el conocimiento, muy importante para habitar internet de formas no impuestas.

El movimiento zapatista se dio a conocer el 1 de enero de 1994 e influyó en diversos movimientos a lo largo del planeta y de las décadas posteriores. Llegó a muchos rincones gracias a sus postulados políticos y sociales, y también porque fue el primer movimiento que hizo activismo en internet. El EZLN en 1996 colocó el conflicto en el ciberespacio obteniendo apoyo internacional para su lucha. Lowy señala que para luchar de manera eficaz contra el "sistema" es preciso actuar simultáneamente en tres niveles: local, nacional y mundial. Para este autor, el EZLN es un buen ejemplo de esta dialéctica: en-

raizado en las comunidades indígenas de Chiapas, en lucha al mismo tiempo contra la dominación sobre la nación mexicana y contra la hegemonía del neoliberalismo. Así, el zapatismo utilizó la red para difundir su mensaje y mantener conversaciones con cientos de actores sociales de todo el mundo, siendo la primera vez que un movimiento político lo utilizaba de forma masiva para comunicarse con personas y grupos de diversas geografías, es decir, dando un uso político alternativo a la red.

El zapatismo es un claro referente para los movimientos altermundistas de finales del siglo XX y principios del XXI, con las vistosas y multitudinarias contracumbres allá donde se celebraban los encuentros de las instituciones del capitalismo (OMC, FMI, Banco Mundial), para impugnarlo, enfrentarlo, pararlo. Porque otros mundos son posibles, sin tanta desigualdad, individualismo, despojo y violencia. Desde ese movimiento nació Indymedia, también llamado Independent Media Center, que tenía como lema: "No odies a los medios, sé los medios", y tomaba las redes digitales para ofrecer una plataforma de información ciudadana, crítica y desde lo local. Fue el producto de la alianza entre activistas tecnológicos y activistas mediáticos, que empiezan a trabajar conjuntamente a finales de la década de los noventa, simbolizando el acceso de los movimientos sociales en internet. Una plataforma que se extendió por decenas de ciudades, cuando no existían las redes sociales

ni las de mensajería, que fue de utilidad para la comunicación de los movimientos, desde la horizontalidad, la apertura y la colaboración.

Dando un salto de casi una década, encontramos la Primavera árabe, el 15M, el Movimiento Occupy, #YoSoy132 o Nuit Debout, que conforman un movimiento global de indignación por el manejo político de las crisis previas e injusticias sociales que conllevaron. Fueron movilizaciones espontáneas y heterogéneas, ocupando espacios públicos, convocadas a través de las redes sociales. Miles de jóvenes expresando su palabra, sobre todo a través de los dispositivos digitales, creando narrativas, criticando formas discriminatorias, desiguales y verticalistas de los representantes del capitalismo en la tierra: partidos políticos, organismos sociales, corporaciones empresariales; pero estos movimientos no se quedan en la denuncia o la crítica, ni tampoco imitan en espejo aquello que desafían, sino que abren espacios para experimentar otros modos de organización y otras relaciones humanas, espacios donde vivir una democracia real.

Hemos recogido en otros textos, mencionando afectos, territorios y resistencias en relación a la tecnología digital, varios ejemplos más de experiencias y propuestas que abonan a la construcción de otro tipo de habitar las redes digitales. Desde los hackfeminismos, los servidores autónomos, las redes de telecomunicaciones libres comunitarias, las redes sociales distribuidas y federadas o las plataformas de servicios digita-

les alternativos, hasta repositorios y páginas web de aprendizajes de uso de herramientas más seguras y libres.

Todos estos ejemplos tienen relación con habitar internet de otra forma a la que nos intentan imponer. Invitan a imaginar otras formas de relacionarnos (dentro y fuera de las redes), nuevas narrativas más allá del individualismo y el consumo; buscan fomentar y practicar la cultura del cuidado, frente a la cultura de la seguridad y el miedo.

Y estamos viendo cómo grandes organizaciones de Latinoamérica, como la CLOC-Vía Campesina, el Movimento dos Trabalhadores Rurais Sem Terra (MST) o redes de educadores y educadoras populares, se están interesando en formarse en habilidades digitales, porque entienden que se necesita dar esa batalla también. Y pensamos que las decenas de talleres, pláticas, foros y plataformas que han tratado el tema de los cuidados digitales con organizaciones y movimientos sociales han ido creando un poso que finalmente está ahí, que va creando conciencia y habilidades. Quizás en unos años, muchos millones de jóvenes —y no tan jóvenes— estén ocupando las redes digitales al margen de las corporaciones para construir otras formas de habitar internet, de usar los dispositivos, de gestionar infraestructuras autónomas, el entorno tecnológico va a formar parte importante en la transición a esas utopías.

A MODO DE CONCLUSIÓN

Nadie se imaginaba hace 15 años que íbamos a aceptar tranquilamente tener un aparato casi constantemente pegado al cuerpo con más de diez sensores prendidos constantemente que dan cuenta de nuestra ubicación, nuestros datos y nuestro entorno social, pero así es. A esto se suma la multiplicación de cámaras de reconocimiento facial, manejadas por algoritmos creados por empresas privadas, un software con una intencionalidad y muchas falencias.

Como dice Paola Ricaurte: "La tecnovigilancia sistemática, permanente y total constituye un hecho innegable que promueve y requiere formas de resistencia civil multivariadas". Quizás empecemos a exigir herramientas que hagan lo que queremos que hagan y no hagan lo que no queremos que hagan; o crearlas, porque el tema de la privacidad y los cuidados digitales es algo colectivo, y por lo tanto político: hagamos política entonces; pero, como explica Gary Marx, probablemente es más preciso concebir el fenómeno de la vigilancia y sus resistencias como procesos complejos e interactivos cuyas dinámicas varían en función del tipo de actores y las relaciones de poder que se analicen. Como puede ser que asumir la naturaleza vigilante del big data en un sentido único "arriba-abajo" sería incongruente con las iniciativas de control ciudadano "abajo-arriba" que también existen. Apo-

yemos estas, creemos más, prestemos atención. Necesitamos tecnologías al servicio de las personas para acompañarnos a ser más humanas y sociales. Dando importancia a los procesos, a los afectos y no dejar que nos alejen de nuestros cuerpos, de nuestros círculos sociales, de nuestros territorios, de nuestro entorno. Necesitamos habitar las redes digitales de forma más sana, equitativa, colaborativa, creativa, frente a las distopías que construyen otros. Imaginemos estas utopías y otras, caminemos hacia ellas.

REFERENCIAS

Azam, A. y Perlroth, N. (2017). "'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México". *New York Times*. Disponible en https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Dans, E. (2021). *Populismo y redes sociales*. Disponible en https://www.enriquedans.com/2021/06/populismo-y-redes-sociales.html

Lado B. (2017). *Promotores del impuesto al refresco, espiados con malware gubernamental*. Disponible en https://ladobe.com.mx/2017/02/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-malware-gubernamental/

Louvet, S. (2019). *Gran Hermano: la vigilancia mundial*. Francia: Arte France & Capa Presse. Documental disponible en https://archive.org/details/vigilancia-mundial-documental

Red en Defensa de los Derechos Digitales (R3D). (2017). *Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México*. Disponible en https://r3d.mx/2017/06/19/gobierno-espia

Sursiendo. (2015). *Razones para habitar internet*. Disponible en: https://sursiendo.org/2015/02/razones-para-habitar-internet/

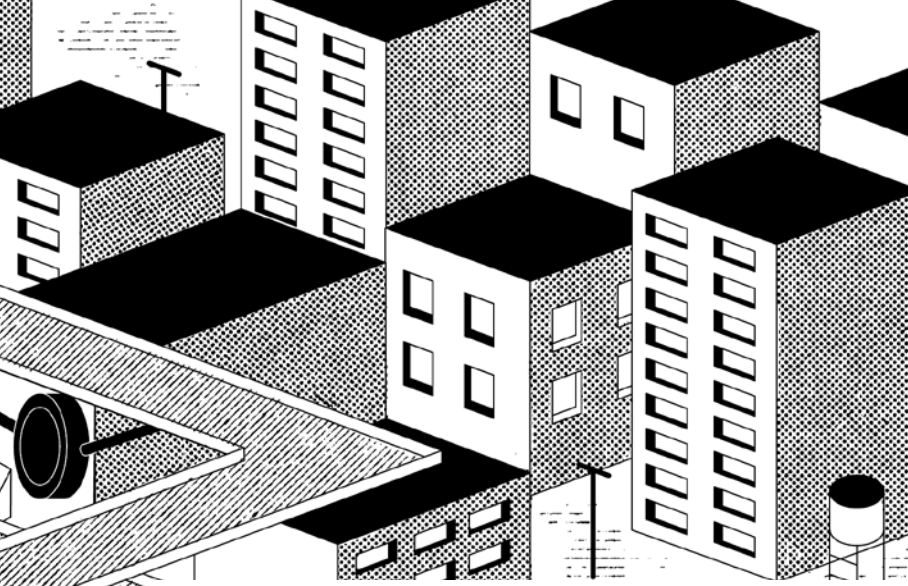
Sursiendo. (2019). *Informe Investigación sobre seguridad digital con organizaciones sociales de Chiapas*. Disponible en https://sursiendo.org/2019/01/informe-investigacion-sobre-seguridad-digital-con-organizaciones-sociales-de-chiapas/

Sursiendo. (2019). ¿Territorio internet? Espacios, afectividades y comunidades. Disponible en https://sursiendo.org/2019/03/territorio-internet-espacios-afectividades-y-comunidades/

Sursiendo. (2019). *Resumen vigilancia digital en México*. Disponible en https://sursiendo.org/2019/05/vigilancia-digital-en-mexico/

Sursiendo. (2021). *Imaginar un principio feminista para internet que ponga en el centro la justicia ambiental*. Disponible en https://sursiendo.org/2021/06/imaginar-un-principio-feminista-para-internet-que-ponga-en-el-centro-la-justicia-ambiental/

Teknokultura. (2014). *Revista de Cultura Digital y Movimientos Sociales*. Vol. 11. *Núm. 2. Dedicado a* "Vigilancia global y formas de resistencia". Disponible en: https://revistas.ucm.es/index.php/TEKN/issue/view/2712



Las calles son nuestras: la violencia de la vigilancia en el espacio público contra las mujeres

GRECIA MACÍAS

Grecia es egresada de la Facultad de Derecho de la Universidad Panamericana. Realiza investigaciones para la incidencia y el litigio estratégico sobre la intersección de derechos humanos y tecnología. Ha colaborado en la Suprema Corte de Justicia de la Nación y el Consejo de la Judicatura Federal. Apasionada en temas de libertad de expresión, privacidad, moderación de contenidos y desigualdad de algoritmos. Es aficionada a la tecnología y fiel creyente en su capacidad para disminuir la brecha de la desigualdad.

ANTES DE MUDARME A la capital a estudiar, viví por 10 años en uno de los estados más peligrosos para ser mujer: el Estado de México. Mi pubertad estuvo marcada por la violencia en el sexenio de la guerra contra el narcotráfico. La primera balacera que presencié fue en una excursión de la primaria, tuve compañeras secuestradas en las inmediaciones de la escuela y vecinas que salieron a un mandado a plena luz del día y después aparecieron en bolsas de basura. Evidentemente, en esas situaciones extremas de violencia, como mujer era muy complicado hacer propio el espacio público, pues la experiencia nos decía a las demás y a mí que un desliz era la diferencia entre graduarse de preparatoria o acabar en una ficha de desaparecida.

No fue hasta las primeras marchas a las que asistí en la Ciudad de México que entendí la libertad de apropiarse de las banquetas, los monumentos e incluso de los baches para expresarme en contra del gobierno, de la inseguridad, de la justicia que no llegaba.

Llevo dos años trabajando como abogada en R3D: Red en Defensa de los Derechos Digitales. R3D es una organización de la sociedad civil dedicada a la defensa de derechos humanos y su intersección con la tecnología. Desde hace casi dos años, he participado en diversas pláticas e impartido talleres sobre violencia digital donde he expuesto las distintas caras que tiene la vio-

lencia contra las mujeres[24] a través de medios digitales. Una de las preguntas más comunes ocurre cuando saco a tema que la vigilancia es una forma de violencia digital contra la mujer. Es una confusión común pues lamentablemente tanto el gobierno como agentes privados han normalizado la observación constante de todes nosotres.

La violencia implica ocupar el espacio de las mujeres sin su consentimiento. Implica obstruir canales de expresión, así como remover el carácter privado de sus rutas diarias para mantener el control sobre ellas. Precisamente este texto se dedicará a responder esta pregunta con base en lo que he aprendido como mujer feminista defensora de derechos humanos en el entorno digital. En especial, me enfocaré en cómo el discurso de la vigilancia que he escuchado de gobernantes en México es una expresión del mandato de masculinidad que resulta en violencia desproporcionada contra las mujeres.

"SI TE ESPÍA, NO TE AMA"

En 2015, *Association for Progressive Communications* definió la violencia digital como "actos

[24] El uso del concepto "mujer" en este texto incluye a todas las mujeres transgénero, cisgénero y todas las personas que se identifiquen como mujer, no importando su condición social, etnia, raza, grado educativo o profesión.

de violencia de género cometidos instigados o agravados, en parte o totalmente, por el uso de las Tecnologías de la Información y la Comunicación (TIC), plataformas de redes sociales y correo electrónico; y causan daño psicológico y emocional, refuerzan los prejuicios, dañan la reputación, causan pérdidas económicas y plantean barreras a la participación en la vida pública y pueden conducir a formas de violencia sexual y otras formas de violencia física"[25].

Esta es la definición con la que he enmarcado las discusiones que he facilitado sobre violencia digital contra la mujer[26]. Larga pero comprensiva en las formas en las que los medios digitales reproducen violencia de género. "Lo digital también es real", dice normalmente la segunda diapositiva de la presentación que proyecto en dichas conferencias. Esto es tanto para explicar cómo las consecuencias de esas violencias también se resienten en el espacio físico, pero también cómo se reproducen las actitudes discriminatorias y violentas del espacio físico en el espacio digital. Para recalcar esta afirmación, tengo una diapositiva donde se lee en letras grandes y centradas:

---

[25] Association for Progressive Communications. (2015). *Technology-related violence against women. A briefing paper*.

[26] Ver: Artículo 19, R3D y Social TIC. (2017). *Gobierno Espía: vigilancia sistemática a periodistas y defensores de derechos humanos en México*.

"EN LA VIOLENCIA DIGITAL CONTRA LAS MUJERES SIEMPRE SE BUSCA PERPETUAR ROLES DE GÉNERO"

Por lo cual, insisto que la mejor herramienta para analizar y contrarrestar una violencia es nombrarla. Así, el siguiente paso en dichas pláticas siempre es identificar, analizar y conocer las distintas formas en las que puede manifestarse la violencia digital.

La difusión de contenido sexual sin consentimiento es una de las violencias digitales que se identifican más rápidamente, mas no es la única. Existen accesos no autorizados, amenazas por medios digitales, desprestigio, acoso, extorsión, afectaciones a los canales de expresión, suplantación y robo de identidad, manipulación de la información, vigilancia, acecho, entre otras[27]. Luchadoras y APC hicieron un gran trabajo recolectando 15 tipos distintos en los que ocurre violencia digital. Normalmente, esto resuena mucho en las mujeres que me acompañan en esos espacios. Entonces empieza el círculo de catarsis donde cada quien cuenta sus experiencias: "Mi ex subió una nude mía sin mi consentimiento".

[27] Luchadoras. (2017). *La violencia en línea contra las mujeres en México*.

“Me amenazaron en Twitter”. “Alguien hackeó mi cuenta de Facebook y ahora me está extorsionando”. Hablamos y nos acuerpamos mientras cada quién estaba contando sus vivencias, entonces una de las participantes que no había hablado antes pidió la palabra:

“No sé si esto cuente como violencia digital”, empezó, “pero había una cuenta que me mandaba fotos mías en plena calle”. La participante, que llamaremos Lorena para proteger su identidad, contó cómo la cuenta anónima de Instagram mandó la primera foto después de haber ido a una marcha del 8 de marzo. La foto la había tomado alguien más en las calles y la había etiquetado en redes sociales. Luego, el agresor seguiría mandando más fotos de Lorena caminando en la plaza o afuera de la universidad con sus amigas. “Me reenvió una foto mía en la marcha donde me etiquetaron. Luego siguió tomando fotos mías en la escuela, en la plaza o en la calle. No era nada sexual, estaba en lugares públicos, no me pedía nada a cambio, pero me hacía sentir muy insegura”, nos contó.

Esta no era la primera vez que escuchaba el caso de una mujer que había sido afectada por este tipo de violencias. Mujeres periodistas y defensoras de derechos humanos han sido víctimas de estas agresiones realizadas por el gobierno mexicano. Así sucedió en el sonado caso de #GobiernoEspía donde el software de vigilancia Pegasus fue usado en contra de mujeres incómodas al gobierno a través de mensajes ame-

nazantes. Sí, eso también es violencia digital, se llama monitoreo y acecho. El informe de Luchadoras y APC lo define como: "La vigilancia constante a las prácticas, la vida cotidiana de una persona o de información (ya sea pública o privada), independientemente de si la persona involucrada se da cuenta o no de la acción en su contra. *Ya sea que la persona se dé cuenta o no de que está siendo acechada*[28]".

Unos minutos antes habíamos hablado sobre los distintos tipos de violencia en los que incluimos el acecho y la vigilancia, lamentablemente, no es la primera vez que se piensa que la injerencia en nuestra vida privada "no es realmente violencia". Francamente, es una reacción normal debido a la expansión y la normalización de distintos tipos de vigilancia tanto realizada por actores privados como por los mismos gobiernos. Esto sucede muchas veces por el desconocimiento del funcionamiento y el alcance de las tecnologías de vigilancia. El desconocimiento es propiciado por gobiernos y agentes privados para crear una caja negra hacia dicha tecnología, por lo cual es importante tener una noción básica sobre qué implica la vigilancia y los alcances que tienen ese tipo de tecnología en especial, un medio de violencia que tiene efectos desproporcionados sobre mujeres.

[28] Ídem. p. 21.

"EL ESTADO NO TE CUIDA, TE VIGILA"

La vigilancia masiva usa sistemas que recolectan, analizan y generan información de un número indefinido de personas. Esto se realiza por agentes privados o agentes públicos, no obstante, con las tecnologías actuales de vigilancia tanto empresas privadas como gobiernos pueden recolectar todo tipo de información de nuestras vidas, incluso las más confidenciales. El objetivo principal de la vigilancia es permitirle a quien la ejerce, ya sea desde el ámbito público o desde el privado, la producción de conocimiento sobre las personas vigiladas[29]. A través de la tecnología de vigilancia se busca obtener un cúmulo masivo de información sobre la vida de las personas para después categorizarlas en ciertos rubros que permiten ejercer un control sobre las y los ciudadanos.

Existen distintos tipos de tecnologías y metodologías para realizar tareas de vigilancia, ya sea a través de medios ocultos como intervención de comunicaciones o geolocalización encubierta, o semiocultos, como lo son las cámaras de vigilancia con tecnologías de reconocimiento facial. Lucía Santanella[30] los clasifica como panóptico, el

[29] Natansohn, G. y Goldsman, F. (2018). "Violencia de género expandida: vigilancia y privacidad en red". *Revista Fronteiras – estudos midiáticos*.

[30] Santaella, L. (2010). "As ambivalências das mídias móveis e locativas". En: Beiguelman; G., La

que se realiza en espacios circunscritos; escópico, la ubicuidad de las cámaras de vigilancia, con o sin reconocimiento facial; y de rastreamiento, mismo que nace en el espacio digital y se manifesta tanto con monitoreo de fuentes abiertas, así como con malware de espionaje que invade los dispositivos de una persona.

La crisis de seguridad lleva permeando la vida de todas las personas en México desde hace más de 15 años. Lamentablemente, el Estado mexicano, en distintos sexenios, ha abusado de los argumentos en favor de la seguridad pública y los peligros del crimen organizado para utilizar herramientas de vigilancia y afectar los derechos de las personas mexicanas. Si bien la vigilancia estatal masiva afecta a todas las personas, existe un impacto desproporcionado en los grupos en situación de vulnerabilidad. Mientras que el discurso del gobierno mexicano señala que estas herramientas de vigilancia son medidas necesarias para combatir el crimen organizado, realmente son utilizadas en contra de periodistas, enemigos políticos, personas defensoras de derechos humanos y, en específico, mujeres de grupos feministas.

Poco a poco, han invadido más espacios de resistencia y recientemente han vigilado uno de los más esenciales: la calle. La calle es el lugar donde llevamos a cabo nuestro proyecto de vida con

---

ferla, J. (org.). *Nomadismos Tecnológicos*. São Paulo: Ed. Senac. p. 133-149.

una rutina diaria, pero también es el espacio público de protesta. Por lo cual, es preciso distinguir entre la calle como espacio cívico y espacio para desarrollar nuestro proyecto de vida donde también tenemos una expectativa de privacidad. Para fines prácticos, quisiera enfocarme en explicar el funcionamiento de la tecnología de reconocimiento facial y el uso de IMSI catchers. Estas dos herramientas tecnológicas que he investigado en mi trabajo para entender lo invasivas que son estas estrategias de la vigilancia en el espacio público.

RECONOCIMIENTO FACIAL

El reconocimiento facial es una tecnología de concordancia digital respecto al marco facial. Esta tecnología recoge la imagen del rostro, la divide y la reduce en partes que la hagan identificable[31]. Básicamente, el rostro de cada una de nosotras es como una huella digital. La distancia de nuestros ojos, el tamaño de nuestra nariz o la posición de nuestros labios se vuelven un mapa que se transforma en código para identificarnos de manera fehaciente[32].

[31] Harvard. (2007). "In the Face of Danger: Facial Recognition and the Limits of Privacy Law". *Harvard Law Review*. Vol. 120. No 7.

[32] Ver: Kirill, L. (2013). "The Rise of A New Type of Surveillance for Which the Law Wasn't Ready". *Columbia Science & Technology Law Review*. Vol. 15. No 1.

La comparación entre los rostros en vivo y la plantilla del rostro contenida en una base de datos que permite el funcionamiento de un sistema de reconocimiento facial se compone por distintos procesos algorítmicos[33]. Para que esta comparación se logre, primero el sistema tiene que reconocer en las fotos o videos en vivo el área donde se encuentra un rostro. Después el sistema tiene que adecuar y alinear el rostro detectado para compararlo con otros marcos faciales contenidos en una base de datos. Esta comparación arroja porcentajes de similitud entre el rostro en vivo (el cual se quiere reconocer) y los rostros contenidos en la base de datos. La tecnología de reconocimiento facial es falible. En los sistemas de reconocimiento facial se pueden actualizar errores como falsos positivos o falsos negativos. Cabe aclarar que la ocurrencia de estos dos tipos de errores no puede ser eliminada por completo y que la reducción de un tipo de error significa el aumento de la ocurrencia del otro tipo de error.

El software de reconocimiento facial se ostenta la mayoría de las veces como una tecnología neutra que no toma en consideración categorías como género o color de piel. No obstante, la evidencia del uso de esta tecnología ha demostrado lo contrario. En primer lugar, está documentado que existe una tendencia de poca o nula repre-

[33] Li, S. Z., Jain, A. K., et al. (2011). "Handbook of Face Recognition". *Springer*. p. 4.

sentación de personas racializadas en las bases de datos utilizadas en el entrenamiento de los algoritmos de reconocimiento facial[34]. Incluso con la utilización de bases de datos más balanceadas en el entrenamiento de algoritmos, es más difícil para los sistemas reconocer los tonos de piel más oscuros[35]. Por ejemplo, en el caso de tecnología con reconocimiento facial, se ha investigado que la concepción binaria de la sexualidad provoca que cuerpos transgénero se vean poco representados, a comparación de rostros y cuerpos cisgénero, en la base de datos que alimenta el software de reconocimiento facial[36]

[34] Buolamwini, J. y Gebru, T. (2018). "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". *Conference on Fairness, Accountability, and Transparency*. Disponible en http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[35] Klare, B. F., Burge, M. J., Klontz, J. C., Vorder Bruegge, R. W. y Jain, A. K. (2012). "Face Recognition Performance: Role of Demographic Information". En *IEEE Transactions on Information Forensics and Security*. Vol. 7. No. 6. p. 1789-1801. Doi: 10.1109/TIFS.2012.2214212. Disponible en https://ieeexplore.ieee.org/document/6327355

[36] Cfr. Keyes, O. (2018). "The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition". *Proceedings of the ACM on Human-Computer Interaction*. Vol. 2. No CSCW. EUA: University of Washington. Disponible en https://ironholds.org/resources/papers/agr_paper.pdf#page=19&zoom=100,0,710

Esta situación pone en estado de indefensión a todas aquellas personas transgénero y personas no binarias que pasen frente a cámaras de reconocimiento facial[37]. Lo anterior debido a que la tasa de error en la que pueden incurrir es más alta, por lo que puede que se le considere como una persona sospechosa en alguna investigación. Por lo tanto, desde un punto de vista interseccional, uno de los grupos a quienes más afecta este tipo de herramientas son a las mujeres transgénero racializadas. Esto también las pone en una situación de riesgo agravado pues se ha documentado que las personas transgénero o no binarias son más susceptibles a ser víctimas de violencia y detenciones arbitrarias por parte de la policía[38].

Los mecanismos de vigilancia no son ajenos al contexto mexicano. El 2 de abril de 2019 el gobernador del Estado de Coahuila Miguel Riquelme anunció[39] el Sistema de Video Inteligencia

---

[37] Gault, M. (2019). "Facial Recognition Software Regularly Misgenders Trans People". *Vice*. Disponible en https://www.vice.com/en_us/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people

[38] Stotzer, R. L. (2014). "Law enforcement and criminal justice personnel interactions with transgender people in the United States: A literature review". *Aggression and Violent Behavior*. Vol. 19. No 3. p. 263–277. Doi: 10.1016/j.avb.2014.04.012

[39] Fernández, H. (2019). "Compran cámaras con reconocimiento facial en Coahuila". *El Universal*. https://www.eluniversal.com.mx/estados/preparan-

para la Seguridad, por el cual instalaron 1,281 cámaras de vigilancia con capacidad de reconocimiento facial en las 11 ciudades más grandes del Estado. El discurso de vigilancia y seguridad pública es constantemente repetido al promocionar estas iniciativas. No obstante, han reservado información esencial para saber el funcionamiento de dichas cámaras y analizar la tasa de error en la que pueden incurrir. A pesar de todas estas problemáticas, el gobernador de Coahuila anunció con orgullo que estas cámaras ya habían logrado la aprehensión de "delincuentes". También en Aguascalientes instalaron cámaras de vigilancia con tecnología de reconocimiento facial. No se han transparentado tampoco metodologías, especificaciones o tasas de error, pero, a pesar de eso, se han puesto en operación y supuestamente ya han "arrojado resultados positivos"[40].

camaras-de-vigilancia-con-reconocimiento-facial-en-coahuila

[40] Ayuntamiento del municipio de Aguascalientes. (2019). "Nuevas cámaras arrojan resultados positivos". *Boletín no 1161*. Disponible en https://www.ags.gob.mx/cont.aspx?p=6253

IMSI CATCHERS
O STINGRAYS

Son torres falsas de telefonía que recolectan[41] datos de todos los teléfonos en su rango de alcance de manera masiva e indiscriminada, tales como números de identificación de la tarjeta SIM (IMSI) y del dispositivo (IMEI), proveedor de telefonía celular, ubicación, llamadas y mensajes de texto. Los IMSI catchers tienen la capacidad de interceptar la conexión entre una red celular auténtica y los teléfonos, recolectando información sin el consentimiento o conocimiento de las personas o del proveedor del servicio de telefonía.

En 2020, investigaciones realizadas por Poder[42] y South Lighthouse[43] encontraron que estas antenas están instaladas en los principales lugares donde se encuentran oficinas de gobierno, cuarteles militares, también donde ocurren las

[41] R3D. (2020). "Las #Golondrinasenelalambre del gobierno federal: torres falsas de telefonía para recolectar la información de personas". *R3D*. Disponible en https://r3d.mx/2020/06/03/las-golondrinasenelalambre-del-gobierno-federal-torres-falsas-de-telefonia-para-recolectar-informacion-de-personas/

[42] Balderas, R. (2020). "Fake Antenna, el espionaje a celulares que pasó de EPN a AMLO". *Poder*. Disponible en https://poderlatam.org/2020/05/fake-antenna-el-espionaje-a-celulares-que-paso-de-epn-a-amlo/

[43] FADE Project. *México*. Disponible en https://fadeproject.org/?project=mexico-df-es&lang=es

protestas ciudadanas y hay grupos grandes de periodistas y defensores de derechos humanos.

Esto ocurre un año después de que el presidente Andrés Manuel López Obrador declaró que, a comparación de su predecesor Enrique Peña Nieto, "ya no había golondrinas en el alambre"[44], refiriéndose a que su gobierno ya no usaba estos mecanismos invasivos de vigilancia.

LA VIOLENCIA DE LA VIGILANCIA

Muchas de las violencias contra las mujeres se basan en el elemento esencial de control y dominación sobre sus cuerpos. Rita Laura Segato establece que el mandato de masculinidad se revela como un acto disciplinador vengador contra una mujer[45]. Segato señala que este mandato se expresa como un acto moralizador contra las mujeres. Este acto consiste en castigar y retirar la vitalidad a una mujer percibida como aquella que desacata y abandona la posición que le fue destinada en el sistema de estatus de la moral

[44] Morales, A. y Zavala, M. (2018). "En el gobierno ya no hay golondrinas en el alambre". *El Universal*. Disponible en https://www.eluniversal.com.mx/nacion/seguridad/en-el-gobierno-ya-no-hay-golondrinas-en-el-alambre-amlo

[45] Segato, L. R. (2008). "La estructura de Género y el mandato de violación". *Las estructuras elementales de la violencia*. p. 21-42.

tradicional. Este sistema de estatus, explica la autora, se basa en que los hombres cisgénero extraigan el tributo de obediencia de las mujeres. Por lo cual, la célula violenta se manifiesta al retirarle cualquier tipo de poder y subordinar por cualquier medio posible a las mujeres[46].

Esta misma violencia se manifiesta en la vigilancia y en su modalidad como violencia digital. La vigilancia afecta la vida de las personas, pero incide de manera particular y desproporcionada en la vida de las mujeres. Esta violencia afecta el derecho a la privacidad de las mujeres, pues se les observa sin consentimiento mientras que hacen uso del espacio público de manera privada.

También afecta el derecho a la libertad de expresión al usar esta información para inhibir a las mujeres de tomar las calles en modo de protesta y expresar su disidencia. Este tipo de violencia se manifiesta en el plano individual, como el caso de Lorena, o en interacciones uno a uno, pero también en el plano estructural. El plano estructural se manifiesta especialmente cuando el Estado se avoca a vigilar y almacenar la recolección masiva de la información de las mujeres como una forma de control para asegurarse que las mujeres no desobedezcan la norma patriarcal de sumisión.

[46] Ídem. "Las estructuras elementales de la violencia: contrato y estatus en la etiología de la violencia". p. 131-134.

Lamentablemente, este tipo de violencia se normaliza por el discurso de seguridad que propicia el Estado. En especial, este discurso se intensifica cuando se banaliza el derecho a la privacidad como una comodidad de las cuales las personas y, especialmente, las mujeres pueden prescindir.

LA HABITACIÓN PROPIA NO ES UN PRIVILEGIO, ES UN DERECHO

La privacidad no es un lujo. Es un derecho humano que nos faculta no sólo en la parte negativa, evitar las injerencias ajenas en nuestra esfera privada, también exige acciones positivas para que se propicie un espacio de creación, reflexión y formación de nuestra esencia como personas. La privacidad no tiene definiciones exhaustivas y varía dependiendo de la persona. "La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás"[47], sentenció la Corte Interamericana de Derechos Humanos.

Estas nociones sobre la privacidad y su importancia eran entendidas por Virginia Woolf a la perfección. "Una mujer debe tener dinero y una habitación propia si va a escribir ficción", declara en su famoso ensayo *Una habitación propia*. Es

[47] Corte Interamericana de Derechos Humanos. "Atala Riffo y Niñas vs Chile". Serie C. No. 239.

necesario tener un lugar propio donde podamos ensayar, probar y formular ideas sin que la mirada ajena nos escrutine. Lamentablemente, este sistema de opresiones coloniales, patriarcales, racistas y coloniales pretende imponer que el derecho a un espacio propio con uno mismo es un lujo sólo del hombre blanco cisgénero. Y esto, al final, es también incorporado a las dinámicas de vigilancia masiva que realiza el Estado patriarcal en el que vivimos. El Estado patriarcal necesita saber cada uno de los movimientos de las, les y los sujetos que pone en situación de vulnerabilidad para ejercer su poder. No obstante, la transparencia se pide de "abajo hacia arriba", pero no de "arriba hacia abajo".

Aquí es donde se empieza a notar uno de los primeros efectos desproporcionados de la vigilancia sobre las mujeres. El patriarcado es nervioso, no permite que las mujeres, sus objetos de control, escapen de su espacio de vigilancia. Entonces, el sistema patriarcal obstaculiza tanto que las mujeres tengan su espacio privado para desarrollar sus ideas, como tampoco permite que hagan uso del espacio público para desobedecer la norma de subordinación que les impuso. Los espacios "públicos" tienen una dimensión política o cívica y una dimensión privada que son vitales para el desarrollo de nuestro plan de vida y para el ejercicio de nuestras libertades civiles.

A primera vista, puede sonar contradictorio el término de privacidad en lo público, pero es algo que todes hemos estado haciendo a lo largo de

nuestras vidas. Como lo ha señalado incluso nuestra Suprema Corte de Justicia de la Nación[48], cada quién tiene una noción de lo privado distinta a los demás. Por lo cual, cabe distinguir la calle como espacio de protesta y la calle como lugar en el que vemos a nuestras amistades, realizamos nuestro trabajo, llevamos una rutina y, básicamente, vivimos nuestras vidas, sin que necesariamente busquemos que cada uno de estos pasos sean conocidos por todo el público en general, y mucho menos observados por las autoridades gubernamentales.

De nuestras rutinas diarias se desprende mucha de nuestra información privada, ideologías políticas, religiosas, nuestros grupos sociales, nuestra orientación sexual e incluso detalles íntimos de nuestra vida sentimental. Las tecnologías de vigilancia pública, como los IMSI catchers o cámaras con herramientas de reconocimiento facial, obstaculizan este uso del espacio público como parte de la esfera privada. Ya que recopilan datos de nuestra privacidad sin nuestro consentimiento con el fin de establecer un perfil y categorizar nuestras vidas para ejercer control sobre ellas.

Lamentablemente, se ha querido imponer la idea patriarcal de que los espacios públicos son "prestados" para las mujeres. Estas narrativas

[48] SCJN. Primera Sala. Amparo directo en revisión 2044/2008. Aprobado por mayoría de votos en sesión del 17 de junio de 2009.

invisibilizan este tipo de violencias, como pasó en el caso de Lorena, y disuaden a las mujeres de hacer propio el espacio público, o de siquiera tener la tranquilidad de caminar por las calles sin mirar por arriba del hombro.

Por eso la frase de Woolf me parece ideal para hablar de la importancia de la privacidad. La habitación propia es un espacio de libertad, así como también lo es tener independencia económica. Estas dos herramientas juntas llevan al acto de disidencia y a ocupar espacios en el mundo, o como ella lo refleja en su ensayo: "escribir ficción", actividad por la cual se juzgaba a las mujeres en su época. No obstante, la metáfora de la habitación propia no debe entenderse únicamente como un espacio privado en nuestra casa, sino también la facultad tanto de tener una esfera privada en espacios públicos como de apropiarse del espacio cívico.

La privacidad es esencial para ejercer el derecho a la libertad de expresión y faculta los derechos de reunión y asociación pacífica. El derecho a la privacidad, en especial cuando se habla desde el anonimato, nos ofrece un espacio seguro. Sin este lugar seguro sería muy complicado expresar ideas sin temor a represalias, generar comunidad o denunciar agresiones. La denuncia sin privacidad genera un efecto intimidatorio ante las represalias, esto lo ha reconocido la Relatoría de Libertad de Expresión de la CIDH[49] al

[49] Informe del Relator Especial sobre la promoción

resaltar la importancia de la protección al anonimato, pues su restricción provoca un efecto intimidatorio en las víctimas de violencia y abuso.

Lo preocupante es que los mecanismos de vigilancia usados por gobiernos locales y federales en el espacio público están empezando a amenazar nuestra libertad para protestar sin detrimento a nuestra dignidad humana y la libertad de hacer uso de las calles para desarrollar nuestra vida cotidiana.

LAS CALLES TAMBIÉN SON NUESTRAS

La otra cara de la moneda se actualiza cuando la calle se usa como espacio cívico. La calle como espacio de expresión y disidencia. La calle, aquel espacio donde han buscado invisibilizar a las mujeres y a muchas otras personas en situación de vulnerabilidad. La protesta feminista viene a romper y desobedecer los mandatos patriarcales. Hacernos presentes en las calles es la peor pesadilla del mandato de masculinidad, pues implica que no pueden seguir cobrando ese tributo de sumisión en el cual lamentablemente han basado toda su noción errónea de lo que "significa ser hombre".

y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40. 17 de abril de 2013.

La vigilancia en el espacio público busca inhibir esta desobediencia y así, mediante actos intimidatorios y supervisión constante, se manifiesta la violencia. El Comité de Derechos Humanos reconoce el efecto inhibidor de estos mecanismos, por lo que advierte que la recolección masiva de datos personales por parte de las autoridades no debe resultar en una supresión de derechos o crear un efecto inhibidor para ejercer el derecho a la protesta[50].

Esto también ha sido retomado por la Comisión Interamericana de Derechos Humanos. La Comisión señala con preocupación que la criminalización de la protesta deriva en la "realización de actividades de espionaje, seguimiento, infiltración y toda una serie de actividades de inteligencia encubierta realizada sobre manifestantes, referentes, líderes, abogados, defensores de derechos humanos". La Comisión describe que la mayoría de las actividades de vigilancia encubierta son desproporcionadas y excesivas, y que "constituyen una práctica discriminatoria contra movimientos sociales por el hecho de criticar algún aspecto de la política pública".

Desgraciadamente, distintos actores gubernamentales ya han usado la vigilancia para inhibir y criminalizar la protesta feminista. Asesoré un caso preocupante en Aguascalientes, donde el 8

[50] Comité de Derechos Humanos. Observación General no. 37. Artículo 21: derecho a la reunión pacífica. 27 de julio de 2020, C/20/27.

de marzo de 2021 se congregaron varias colectivas feministas para marchar en el centro de la ciudad. Lamentablemente, fueron recibidas por cuerpos policiacos que identificaron a varias con nombre y apellido, a pesar de no haber hecho ninguna referencia a esto en ninguna de sus redes digitales. Una de las activistas me cuenta su preocupación por ser objeto de vigilancia, "hubo represión policial, quiero meter una solicitud de cancelación de datos personales porque no sé cómo obtuvieron mi información".

Lo mismo pasó en el caso de un grupo de jóvenes feministas que fueron a marchar a la Ciudad de México el 8 de marzo de 2020, a quienes les abrieron carpetas de investigación[51] por supuestos daños a la propiedad. La Fiscalía de la Ciudad de México declaró que habían obtenido esta información derivada del monitoreo de fuentes abiertas, en especial Facebook. No obstante, ya iniciadas las carpetas de investigación, la fiscalía requirió a este grupo de mujeres feministas para que realizaran una "concordancia de marco facial".

La asesora jurídica de una de las víctimas me contactó para preguntarme por esto. Estaban confundidas porque habían ido a la marcha con el rostro cubierto para proteger su identidad y

[51] Arteto, I. (2020). "Fiscalía de la CDMX abre investigación contra 13 jóvenes feministas". *Animal político*. Disponible en https://www.animalpolitico.com/2020/11/fiscalia-cdmx-abre-investigacion-contra-13-jovenes-feministas/

tampoco habían puesto en los perfiles públicos de sus redes sociales que iban a estar ahí. "¿Con qué se supone que van a comparar sus rostros?". Todas se negaron a realizar dicha concordancia y preguntaron por qué no había registros de ese supuesto dato de prueba en la carpeta de investigación. La Fiscalía de la Ciudad de México simplemente retiró su solicitud. Hasta hoy, junio de 2021, la Ciudad de México sigue teniendo la información respecto al uso de tecnología de reconocimiento facial como reservada, así como sigue abierta la investigación en contra de aquellas 13 jóvenes activistas.

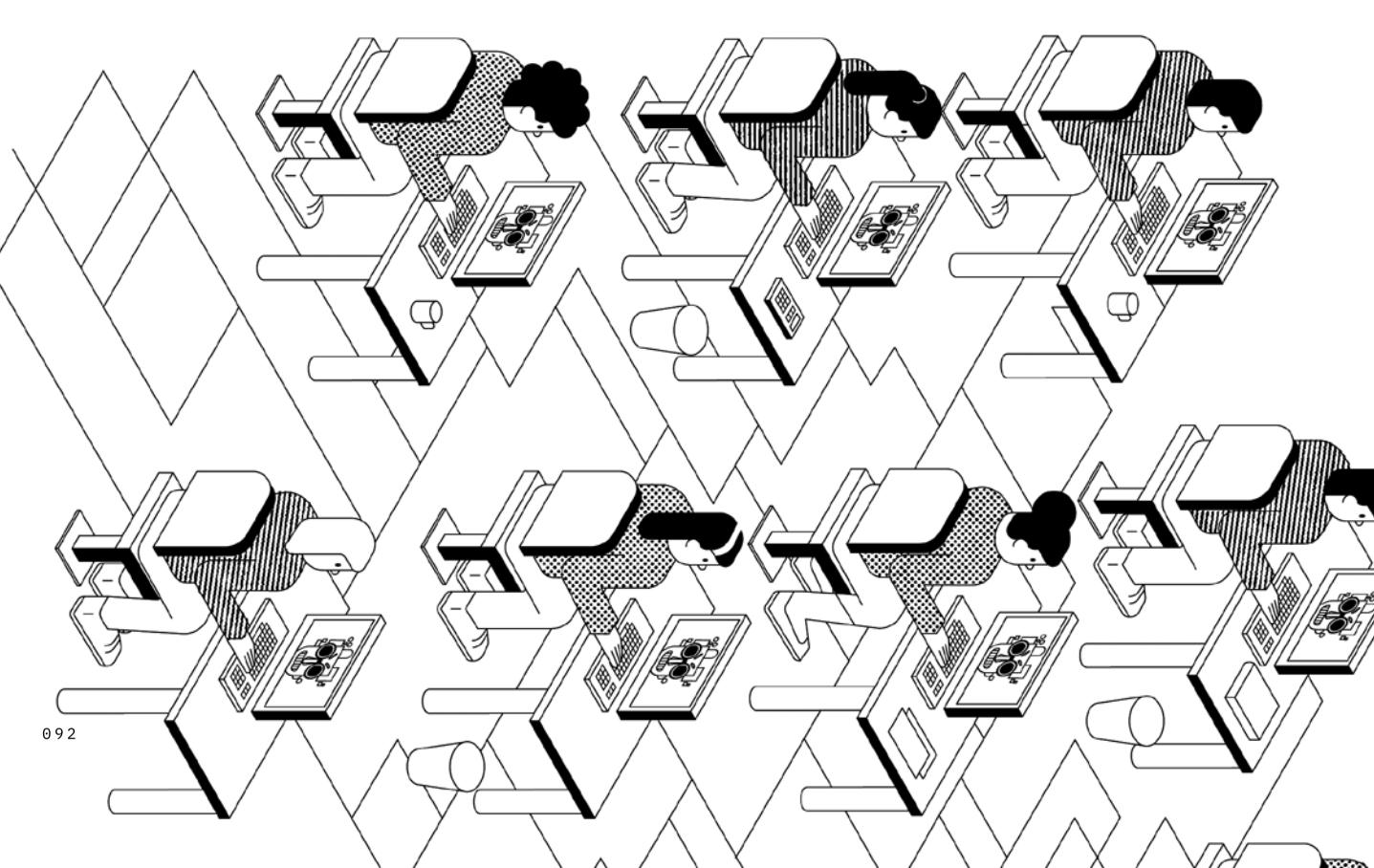
"EL ESTADO NO NOS CUIDA, NOS CUIDAN LAS AMIGAS"

No ha pasado mucho tiempo desde que experimenté la libertad de apropiarme de mi espacio cívico. Llevo seis años en la capital del país y he salido más veces a caminar sola en la calle que todo el tiempo que viví en el Estado de México. No ha pasado mucho tiempo desde que pude expresar mi enojo en las calles por la apatía del gobierno ante las 10 mujeres que asesinan a diario. No obstante, entiendo que la protesta no solamente puede ocurrir el 8 de marzo caminando del Monumento a la Revolución al Zócalo. La protesta ocurre todos los días. Sucede en actos de resistencia como la red de ternura radical que tengo con mis amigas, ocurre al ponerme una falda y tomar el

metro, cuando camino sola en la calle después de salir del trabajo, en compartir experiencias con otras mujeres y en el abrazo de mi madre.

A lo largo de la historia, las mujeres ocupando espacios públicos han sido merecedoras de actos que van desde fruncidas de ceño hasta penas de cárcel. Y aun así hemos desobedecido los estándares patriarcales que buscan que la participación de la mujer se limite al espacio doméstico. La vigilancia masiva en espacios públicos es un síntoma del patriarcado nervioso e inseguro. Es una forma de violencia porque genera un efecto discriminatorio y hostil contra las mujeres que desafían los estereotipos de género. Esto sucede desde el momento en el que nos observan, categorizan y supervisan sin nuestro consentimiento.

Es importante identificar este tipo de violencia en nuestra vida cotidiana para enfrentarla. Las calles, los parques, las banquetas y monumentos son nuestros. El Estado no nos está cuidando, nos está vigilando para después castigarnos en cuanto rompamos la norma patriarcal. Debemos compartir y socializar este tipo de conocimientos para todas nuestras hermanas de lucha que existen y resisten todos los días, cosas tan simples como no tomar fotos sin consentimiento de otras manifestantes o practicar los buenos hábitos de seguridad cuando estamos en una protesta pública. Porque si el Estado no nos protege, la resistencia se encuentra en los cuidados y la ternura que generamos entre nosotras.



Control social a través de la mordaza a internet

MARTHA A. TUDÓN M.

Martha es defensora de derechos humanos, con expertise en construcción de políticas públicas participativas y procesos de incidencia hacia la verdad, memoria y justicia. Su experiencia laboral incluye consultoría de riesgo político e investigación en materia de seguridad pública, el Sistema de Justicia Penal y violaciones a derechos humanos. Actualmente es Coordinadora de Derechos Digitales en ARTICLE 19, Oficina para México y Centroamérica, donde implementa investigaciones y procesos de incidencia política y mediática en defensa de la libertad de expresión e información en el entorno digital.

LAS TECNOLOGÍAS DE la Información y Comunicación (TIC), incluida la internet, han hecho posible que las personas reinventemos y aumentemos el poder que tenemos como ciudadanía. Más que tratarse de cables y fierros, internet se traduce a esa infraestructura que nos permite tener acceso a la cultura, ciencia y conocimiento a través de un sinnúmero de contenidos disponibles para su reproducción, vista e intercambio. Sobre todo, internet se refiere a nosotras como sociedades de la información y creadoras de contenido esparcidas alrededor del planeta, que utilizamos la red para captar y distribuir ideas más allá de nuestras fronteras.

En México es innegable que esta herramienta nos ha permitido expandir nuestros horizontes más allá del nivel personal. Incluso, "salir" del país nunca ha sido tan fácil. Virtualmente podemos visitar y nutrirnos de lo que pasa en otros rincones del mundo: podemos observar y contrastar nuestra realidad con la de otras personas y otros gobiernos, podemos mirar hacia afuera y repensar lo que deseamos hacia adentro.

La capacidad inaudita para que las personas actuemos conforme a lo que percibimos a través y con el uso de las TIC se ha traducido en una revolución democrática en nuestro país. Internet ha potencializado nuestro actuar colectivo y comunitario cuando el contexto lo ha demandado. Por ejemplo, hoy más que nunca —por el riesgo sanitario ocasionado por el virus COVID-19— las protestas en espacios públicos se han traslada-

do mayoritariamente a los entornos digitales, donde con hashtags y el retumbe de tendencias exigimos justicia y recuperamos juntas y juntos la memoria de lo que acontece y nos importa como sociedad.

Este uso ciudadano de las TIC ha incluso abonado a aumentar la transparencia y la rendición de cuentas por parte de las autoridades. Los hechos de abuso estatal, corrupción y violaciones de derechos humanos son innegables cuando son registrados, documentados y difundidos por la ciudadanía, periodistas y medios de comunicación digitales a través de las redes sociales o por transmisiones especiales.

En ese sentido, internet se ha vuelto tan relevante para ejercer los derechos políticos, culturales y sociales que la propia Constitución Política de los Estados Unidos Mexicanos reconocen a su acceso como un derecho en sí mismo[52]. Además, regionalmente —en el ámbito del Sistema Interamericano de Derechos Humanos— los estándares para su acceso y uso han evolucionado hasta demandar el cumplimiento de determinadas pautas para garantizar que internet sea siempre libre, abierta e incluyente. Sobre todo, se ha insistido en que la red debe estar lejos de intromisiones e intervenciones ilegítimas por

[52] Gobierno de México. (2013). *En México, el acceso a internet es un derecho constitucional*. Disponible en https://www.gob.mx/gobmx/articulos/en-mexico-el-acceso-a-internet-es-un-derecho-constitucional

parte de los Estados, a quienes tantas bondades de las TIC en la democracia pueden resultarles particularmente molestas y quieran diluirlas a toda costa[53].

De forma complementaria, la Organización de las Naciones Unidas ha establecido que los derechos humanos (a la libertad de expresión e información, a la privacidad, a la protesta, entre otros) deben ser igualmente protegidos, respetados y garantizados cuando estos se ejerzan en el entorno digital y no sólo en el ecosistema físico.[54] Más recientemente, el Comité de Derechos Humanos ha establecido específicamente que los Estados no deben bloquear u obstaculizar —directa o indirectamente— la conectividad a internet y no deben censurar los contenidos digitales[55], ya que dicho control digital puede

[53] Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos. (2017). *Estándares para una internet libre, abierta e incluyente*. Párrafo 6. p. 13. Disponible en http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

[54] Consejo de Derechos Humanos de la Organización de las Naciones Unidas. (2012). "Promoción, protección y disfrute de los derechos humanos en Internet". A/HRC/20/L.13. Disponible en https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

[55] Comité de Derechos Humanos de la Organización de las Naciones Unidas. (2020). "Observación general núm. 37 (2020), relativa al derecho de reunión pacífica (Artículo 21)". CCPR/C/GC/37. Disponible en https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsrdB0H1l59

considerarse como una búsqueda de control ciudadano y una supresión de las libertades que son pilares de la democracia.

No obstante, el empoderamiento ciudadano propulsado a través de las TIC no ha pasado desapercibido por parte de los poderes fácticos y políticos de nuestro país. A pesar de los diversos ordenamientos jurídicos nacionales, regionales e internacionales que reafirman la necesidad de proteger los derechos humanos ejercidos en el entorno digital y salvaguardar a la propia internet, el Estado mexicano ha reaccionado a este empoderamiento con agresiones y un discurso institucional que estigmatiza a las personas que se informan y movilizan a través de las tecnologías. Más consistentemente, también ha decidido intentar establecer una mordaza a internet como instrumento habilitador de la democracia del siglo XXI, mientras simultáneamente ha emprendido una estrategia de desinformar y deslegitimar a quienes defienden a internet y los derechos digitales[56].

79OVGGB%2bWPAXj3%2bho0P51AAHSqSubYW2%2fRWvqeXcmwcJPCLnvmaZpSJFN4i2MgSnq7H0QmP4hTgADGwACs%2f4pF06q8I9WCRbyJ

[56] El término “derechos digitales” hace referencia a los derechos humanos que se ejercen con y a través del uso de las TIC.

AVERSIÓN Y FOBIAS DEL ESTADO HACIA LAS TIC

Las generaciones que ocupan distintos puestos de poder político corresponden mayoritariamente a quienes vivieron su juventud en tiempos análogos. Son esas que crecieron con la radio y la televisión como únicas fuentes de información y con los monopolios que las controlaban, así como con el priismo[57] que se coludía con la industria de telecomunicaciones para controlar el discurso público y difundir su propaganda[58]. Los tiempos que esas generaciones conocieron son distintos a los actuales: no porque ya no existan los monopolios ni los pactos entre los grandes conglomerados empresariales y los personajes políticos, sino porque la sociedad ya no es un grupo pasivo en la arena de las tecnologías.

La evolución de las TIC ha traído consigo una nueva manera de experimentar las telecomunicaciones. La radio y la televisión son instrumentos invaluables que fueron y han sido imprescin-

[57] Haciendo referencia a los años transcurridos entre 1929 hasta 2000, en los que el Partido Revolucionario Institucional (PRI) gobernó en México.

[58] Valdés Vega, M. E. (2016). "Reforma a telecomunicaciones y radiodifusión en México: la perspectiva de la Asociación Mexicana del Derecho a la Información". *Tla-melaua*. Volumen 9. No. 39. Puebla. Disponible en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-69162016000100188

dibles para informarnos. No obstante, estas tecnologías se caracterizan por ser unidireccionales: existe una persona emisora que va compartiendo mensajes y una audiencia que los consume, y no existe una respuesta o reacción en sentido contrario por parte de quienes los ven o escuchan. Tampoco la radio o la televisión permiten que captemos fácilmente los contenidos que hayan sido creados más allá de nuestras fronteras nacionales. Esas son las grandes diferencias entre ellas e internet.

Internet, a diferencia de la radio y la televisión, no es fácil de controlar. Como se detalló con anterioridad, internet se constituye a partir de las sociedades de la información que utilizamos estas herramientas para crear y difundir contenidos, no sólo para allegarnos de ellos. La red de redes está creada en sí misma por el infinito intercambio de ideas e interacciones entre un sinnúmero de personas que actúan como emisoras y receptoras al mismo tiempo, y dichas personas se ubican dentro y fuera del territorio mexicano.

La naturaleza multidireccional de internet la constituye como una herramienta que se ha vuelto imprescindible para la participación en la vida sociopolítica de México. Quienes cuentan con conexión a la red viven la internet como una plataforma que les permite ejercer otros derechos humanos, tales como el acceso a la información, la libertad de expresión, la libertad de reunión, la educación, la protesta y la salud. So-

bre todo, permite participar activamente en la democracia de nuestro país.

En ese sentido, ni tantos derechos ni tanta democracia han hecho mucha gracia a las generaciones de tiempos análogos —ni a las generaciones más jóvenes que les toman de ejemplo—; a esas que actualmente están en el poder y que les convendría una sociedad desinformada, desarticulada y desorganizada, nutrida únicamente con una narrativa oficialista —verdadera o no.

Más aún, la aversión de quienes nos gobiernan hacia la internet va más allá del poder que esta tecnología ha brindado a la población. En realidad, temen también del poder que han concentrado las plataformas digitales para decidir qué contenidos pueden estar disponibles a través y con el uso de las TIC. Es perceptible que en lugar de someter o coludirse con estas empresas —como los gobiernos anteriores lo hicieron tanto tiempo con la radio y la televisión—, el gobierno actual ve en ellas a actores que no cederán fácilmente ante sus presiones y que, de hecho, concentran más capacidades y recursos que otros poderes fácticos.

A manera de ejemplificar lo anterior, es importante considerar el caso de Estados Unidos. Dejó de ser sorpresa que su exmandatario, Donald Trump, utilizara sus redes sociales cotidianamente como un arma para alterar el ciclo informativo que hablaba sobre él y su gobierno. Durante su administración dispersó mensajes que buscaron distraer y deslindarse de responsabili-

dades por sus decisiones y acciones. Sin embargo, sí fue sorpresa cuando a él, quien en su momento pudo coloquialmente considerarse como el hombre más poderoso del mundo, Facebook, Instagram y Twitter le suspendieron sus cuentas de redes sociales por las expresiones que llevaron a la violencia desatada en el Capitolio[59]. Si al presidente de la nación más poderosa del mundo lograron detenerlo en sus formas de actuar contrarias a principios y valores democráticos, ¿qué límites no les pondrían a las demás personas gobernantes de lugares que no son potencias mundiales?

El temor que provoca esta situación tiene algo de creíble. Las preocupaciones relacionadas al gran poderío que las empresas privadas han consolidado para colocar restricciones a los contenidos en línea, bloqueos y suspensiones de cuentas, basadas en decisiones arbitrarias de quienes trabajan en las plataformas digitales —incluyendo de sus direcciones ejecutivas o CEO— son legítimas. También es comprensible la crítica a que muchas de estas empresas operan como gatekeepers o "porteras" de la información, ya que sólo a través de someterse a sus términos y condiciones de uso es que las personas

[59] Romano, N. y Bucksbaum, S. (2021). "Donald Trump suspended from Twitter, banned from Facebook and Instagram 'indefinitely' following Capitol riots". *Entertainment Weekly*. Disponible en https://ew.com/celebrity/donald-trump-banned-facebook-instagram/

tenemos acceso a ciertos contenidos que se difunden y distribuyen a través de sus canales.

Lo que no es legítimo ni comprensible son las acciones contrarias a los derechos humanos que se han emprendido por diversos gobiernos, incluido el mexicano, para responder a esas preocupaciones. Se ha buscado no sólo abatir el poder de las empresas, sino destruir a internet como la conocemos. La intención ha sido clara: lo que realmente desean es controlar a internet y, en consecuencia, a la información que fluye y se difunde por este medio. Peor aún, en México, los personajes políticos intentan aplicar las mismas mordazas y candados que les colocaron a la radio y la televisión en los tiempos de antaño, lo cual resultaría catastrófico para una sociedad que ya depende de las libertades y oportunidades que internet nos ha ofrecido.

EL USO DEL PODER LEGISLATIVO PARA OBSTACULIZAR EL EJERCICIO DE DERECHOS

La aversión y la fobia hacia las tecnologías y las empresas que forman parte de internet ha derivado en que el gobierno y sus alianzas recurran al uso excesivo del poder legislativo para interferir en el flujo informativo y con las libertades en la red. Lo anterior no es menor, implica que se estén utilizando todas las artimañas estatales para conquistar un espacio cívico internacional

que las personas usuarias de las TIC hemos tardado tantos años en construir.

Tan sólo en 2020, 15 iniciativas legislativas se presentaron ante el Congreso federal o los estatales en detrimento de la internet y los derechos digitales[60]. De estas, aunque sólo ocho se aprobaron y publicaron, la característica que asemeja a todas es que se presentaron a pesar de ser inconstitucionales y contrarias a estándares regionales e internacionales de derechos humanos. Algunas iniciativas buscaron crear nuevos delitos en los marcos jurídicos que rigen a la sociedad[61], sin siquiera describir qué criterios se tomarían en cuenta para determinar cuándo cierta conducta se consideraría o no como un acto criminal. Estas son fallas en la manera en que se escriben las leyes. Lo que ocasionan es que "todo sea delito" y "nada sea delito" al mismo tiempo, y que más bien se apliquen los castigos a conveniencia de quién está siendo acusada o quién está acusando[62]. Más aún, la falta de claridad sobre lo que constituye o no un delito propi-

[60] ARTICLE 19. (2021). *Distorsión: el discurso contra la realidad*. p. 174. Disponible en https://articulo19.org/wp-content/uploads/2021/03/Book-1_ARTICLE-19_2021_V02_en-baja_.pdf

[61] Por ejemplo, para castigar a lo que sea que se defina como "desinformación", "discurso de odio" o a todo aquello que se considere como violencia digital de género o ciberdelitos. También se intentó penalizar a quienes osaran en denunciar y presionar a las autoridades. Ibíd. p. 174.

[62] Ibídem.

cia que las personas que navegamos en internet no sepamos cómo actuar y, por miedo a ser sancionadas, nos autocensuremos.

Otras iniciativas buscaron obligar a las plataformas digitales a censurar o borrar contenidos en sus espacios, incluyendo aquellos que son de interés público sobre acciones del poder político, sobre hechos relevantes que ocurren en el país, críticas al gobierno y muestras de disidencia y descontento ciudadano[63]. Resulta lógico que el sólo hecho de exigir a las empresas privadas que censuren contenidos tiene un efecto devastador en la libertad de expresión en internet. Además, también afecta al combate a la impunidad, la lucha por la verdad, memoria y justicia, y al ejercicio efectivo de la participación política, ya que elimina todo rastro de información que nos ayude a conocer lo que está pasando en el país y a movilizarnos para luchar a favor o en contra de determinada situación.

Otras ocurrencias legislativas quisieron obligar a periodistas y medios de comunicación —que difunden contenidos en línea— a borrar toda información de una persona que se nombraba en sus publicaciones cuando esta así lo solicitara, lo que hubiera beneficiado enormemente a personas servidoras públicas, retiradas o en funciones, que encontraran desfavorable la cobertura mediática que se les ha dado —por ser corruptas o violadoras de derechos humanos,

[63] Ibídem.

por ejemplo— y quisieran esconderla de la vista de la ciudadanía[64]. También se quiso obligar a estos actores a que identificaran, con nombre completo, a quiénes escribían determinada pieza periodística[65]. Ambas situaciones hubieren sido un atentado directo al derecho humano a la libertad de expresión e información, al habilitar la censura y la persecución directa de periodistas, en un país donde cada 13 horas se registra una nueva agresión contra la prensa[66].

Hubo otras iniciativas que quisieron interferir en el mercado económico del entorno digital[67]. El poder legislativo ha buscado, en diversas ocasiones, obligar a las plataformas digitales —Netflix, portales de animé, canales de cocina— a que ofrezcan producciones mexicanas en sus catálogos con porcentajes determinados. En 2020 intentó establecerse que un 30% de los catálogos de contenidos de las plataformas contuviera producciones nacionales, mientras que en 2021 se buscó establecer que fuera el 15%. La imposición arbitraria de cualquier porcentaje implicaría una carga regulatoria que no hace sentido para plataformas digitales que no buscan comprar contenidos a las televisoras mexicanas. De hecho, ello ocasionaría que muchas de estas empresas terminen por inhabilitar el acceso a

64 Ibíd. p. 174-175.
65 Ibíd. p. 175.
66 Ibíd. p. 128.
67 Ibíd. p. 175.

sus servicios desde México o a retirar contenidos producidos en el extranjero de sus catálogos, todo con el fin de dar con el porcentaje requerido. Así, de una u otra forma, la reducción en la oferta de contenidos mermaría el derecho a la libertad de expresión y a la cultura de las y los usuarios. Además, al imponer cuotas de contenidos con porcentajes, cuando en internet no hay escasez, sino abundancia de ellos, sólo se termina favoreciendo a la industria de televisión mexicana —como poder fáctico y económico—, no a las y los mexicanos.

En otros temas igual de catastróficos, hubo iniciativas legislativas que quisieron debilitar las competencias y atribuciones de entes estatales que actúan como contrapesos al poder ejecutivo federal sobre decisiones que impactan al entorno digital y al uso de las TIC. Este es el caso de la iniciativa de reforma constitucional que se promovió para extinguir al Instituto Federal de Telecomunicaciones y convertirlo en un órgano político no especializado al servicio del presidente[68].

En contraste con lo anterior, otras iniciativas quisieron (y algunas lograron) otorgar facultades extraordinarias a diversas autoridades para que estas puedan solicitar a las plataformas digitales que eliminen contenidos de internet. Incluso hubo aquellas que intentaron que estas mismas autoridades tuvieran el poder de ordenar el bloqueo de páginas completas y servicios en línea.

[68] Ibídem.

Estas acciones arbitrarias, al no estar sometidas a procesos judiciales que evalúen si determinada eliminación o bloqueo son medidas necesarias, legítimas y proporcionales, constituyen medidas descaradas de censura[69].

Dado el recuento de lo aquí expuesto, "todas las iniciativas presentadas —la mitad de las cuales se han aprobado— se configuran como artilugios legales que, al prosperar, atentan contra la participación, expresión e información en línea, y terminan por convertirse en una mordaza a internet"[70]. Esto es una creciente presión del Estado sobre el espacio digital y sobre los derechos que las y los mexicanos ejercemos en este ámbito. Al final, lo que se ha buscado es reducir el espacio cívico en línea para quienes buscamos expresar nuestras críticas, organizarnos y protestar[71]. Desafortunadamente, esta tendencia que se comenzaba a esbozar desde el primer año de la actual administración se confirmó en 2020 y se percibe que continuará para 2021.

---

[69] Ibídem.

[70] Ibíd. p. 177.

[71] ARTICLE 19. (2020). *Disonancia: voces en disputa*. p. 168. Disponible en https://disonancia.articulo19.org/wp-content/uploads/2020/07/DISONANCIA-INF-A19-2019-PDF-WEB.pdf

EL GOLPETEO DE LA NARRATIVA ESTATAL PARA DESPRESTIGIAR Y DESINFORMAR

Usar el aparato legislativo para amedrentar derechos y libertades es una forma escurridiza de atentar contra la democracia. Sin embargo, existen otras manifestaciones directas de violencia digital en México por parte del Estado, en donde lo palpable y tácito del discurso antiderechos del presidente se ha actualizado en nuevas formas de agredir a periodistas y medios de comunicación, ahora, a través de las TIC.

La alternancia partidista de México en 2018 no vino acompañada de un cambio en la forma de gobernar, es decir, de cambiar la *vieja escuela* de buscar controlar y desactivar —a como dé lugar— todo ejercicio de disidencia y crítica al poder. Evidencia de ello ha sido el discurso tan claro del presidente Andrés Manuel López Obrador al describir a periodistas y medios de comunicación mexicanos que reportan sobre su administración. Lo anterior ha consistido en que el presidente señale[72] como "fantoches", "conservadores", "neoliberales", "hipócritas", "doble cara" o "prensa fifí" a todo aquel que provea coberturas periodísticas que no resulten gratas para él.

Más importante aún es mencionar que este discurso no se repite únicamente por políticas y políticos que lo encuentran conveniente para

[72] Op. cit. ARTICLE 19. Distorsión (...). p. 128.

desacreditar a la prensa libre que les estorba; sino que también se replica entre la ferviente masa de personas seguidoras que repiten, incuestionablemente, los dichos del presidente a través de las redes sociales. Así, "la narrativa imperante es la del rechazo a cualquier forma de cuestionamiento o crítica. Las redes sociodigitales se inundan de ruido y las cuentas participantes en estas tendencias construyen una barrera que no permite un debate que respete el disenso. Este clima contribuye a la vulnerabilidad de los periodistas"[73].

Un caso muy emblemático ha sido el del periódico *Reforma*. Desde 2019 el presidente ha insistido en que este medio es un adversario de su gobierno. A consecuencia de esa insistencia los hashtags #NarcoReforma[74] y #ReformaTodoLoDeforma[75] han sido tendencias que se popularizaron desde entonces y han continuado esporádicamente hasta la fecha.

Más recientemente, a partir de septiembre de 2020, el poder ejecutivo federal se ha empeñado

[73] Signa_Lab. (2019). *"Ustedes cumplen con su trabajo": Andrés Manuel López Obrador*. ITESO Universidad Jesuita de Guadalajara. Disponible en https://signalab.mx/2019/11/25/prensaprostituida/

[74] Op. cit. ARTICLE 19. *Disonancia:* (…). p. 130.

[75] Signa_Lab. (2019). *Democracia, libertad de expresión y esfera digital. Análisis de tendencias y topologías en Twitter. El caso de la #RedAMLOVE*. ITESO Universidad Jesuita de Guadalajara. Disponible en https://signalab.iteso.mx/informes/informe_redamlove.html#footnote-03

en difundir la narrativa de que la prensa mexicana nunca ha atacado tanto a un presidente como a él, ya que asegura que alrededor del 66% de las notas y columnas de opinión están en contra de los proyectos de su administración y de su gobierno[76]. Además de desinformar a la sociedad con estos dichos y supuestos datos que carecen de evidencia probatoria y fundamento, el gobierno aprovecha las acusaciones para nombrar —con nombre y apellido— a quienes se refiere como "adversarios". Producto de su campaña de estigmatización y desinformación es que se han alebrestado los ataques de ciertos sectores de la población y de otras personas servidoras públicas hacia el gremio periodístico[77].

Este tipo de ataques a quienes se dedican a la labor informativa tienen dos consecuencias naturales. En primer lugar, cualquier ataque masivo, aunque digital, tiene como secuela el generar una sensación de inseguridad o miedo en la vida de una persona, "porque los sentimientos no se producen en la esfera digital, se producen en la vida real, y eso tiene un efecto en la vida cotidiana"[78]. De esta manera puede generar silenciamiento y autocensura. En segundo lugar, la

[76] Redacción Animal político. (2020). "AMLO analiza a la prensa: el 66% de las columnas son contra el proyecto de la 4T, dice". *Animal político*. Disponible en https://www.animalpolitico.com/2020/09/amlo-analiza-prensa-columnistas-contra-proyecto-4t/

[77] Op. cit. ARTICLE 19. *Distorsión* (...). p. 127.

[78] Op. cit. ARTICLE 19. *Distorsión* (...). p. 185.

política de ataque digital hacia periodistas y medios de comunicación, al ir construyendo la imagen de la prensa como personajes despreciables y enemigos de la democracia, apuesta porque cualquier acción represiva o de uso desproporcionado del aparato público en contra de la prensa sea cada vez más tolerada socialmente, en tanto se configure como una acción para constreñir a estos actores.

Como si esto fuera poco, más indignantes resultan los casos de asedio directo a periodistas y medios de comunicación a través de los recursos que pagamos las y los mexicanos con nuestros impuestos, como lo es el caso del uso político de la Agencia de Noticias del Estado (NOTIMEX) —una institución de gobierno— para coordinar agresiones contra la prensa. En mayo de 2020, Aristegui Noticias, Signa_Lab del Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO) y ARTICLE 19 hicieron pública información y testimonios que demostraban que Sanjuana Martínez, directora de NOTIMEX, junto con otras personas directivas de la agencia, ordenaron acciones coordinadas en Twitter para acosar y agredir a personas periodistas que consideraban enemigas del gobierno del presidente López Obrador[79]. Básicamente, la directiva de la agen-

[79] ARTICLE 19. (2020). *Directiva de Notimex ataca periodistas y organiza campañas de desprestigio en redes sociales*. Disponible en https://articulo19.org/directiva-de-notimex-ataca-periodistas-y-organiza-campanas-de-desprestigio-en-redes-sociales/

cia coaccionó e intimidó a su personal para diseñar y ejecutar campañas de desprestigio, descrédito y daño reputacional en contra de periodistas[80], "lo que es más grave aún si consideramos que estos ataques podrían enmarcarse en una estrategia más amplia para controlar y manipular el diálogo en las redes (sociales)"[81].

Lo acontecido en el caso NOTIMEX es el claro ejemplo de lo que jamás debería pasar en un Estado democrático. Ordenar, accionar y utilizar recursos materiales, humanos y financieros para difundir desinformación sobre la vida privada de periodistas y socavar su credibilidad a través de las TIC, y coartar con ello el ejercicio de su libertad de expresión, va en contra de todo principio democrático, incluso en contra del ordenamiento jurídico mexicano y del derecho internacional en materia de derechos humanos.

Los efectos de todos estos ataques no sólo son dañinos para quienes enfrentan el golpeteo digital por parte del Estado o por parte del sector de la población que no se da cuenta de que este le utiliza para amedrentar a quien le expone. Como ya se ha mencionado, las TIC han ampliado nuestras capacidades como ciudadanía para

[80] ARTICLE 19. (2020). *La guerra está en Twitter: evidencia confirma tácticas de la dirección de Notimex para atacar periodistas*. Disponible en https://articulo19.org/la-guerra-esta-en-twitter-evidencia-confirma-tacticas-de-la-direccion-de-notimex-para-atacar-periodistas/

[81] Op. cit. ARTICLE 19. *Disonancia:* (…). p. 144.

tener acceso a información que nos importa e interesa. Sin embargo, lo cierto es que muchas veces esto es posible gracias a la información que proviene, precisamente, de personas periodistas y medios de comunicación. Por lo tanto, si estos actores deciden replegarse y autocensurarse en su trabajo por los ataques que están enfrentando a través de las plataformas digitales, entonces la ciudadanía también sufre al ver deteriorada su fuente primordial de información.

Así, el asedio al periodismo y al acceso a la información periodística ha encontrado un cauce sostenido a través y con el uso de las tecnologías, ya que la violencia estatal, primero, desinforma y polariza a la opinión pública. Segundo, acciona a su arsenal institucional o a un segmento de la población para atacar y desprestigiar digitalmente a quienes les son incómodos al poder por exhibirles, criticarles y exigirles rendición de cuentas.

ATACAR AL MENSAJERO PARA DESVIAR LA ATENCIÓN DEL MENSAJE

En su conferencia de prensa del 31 de marzo de 2021, el presidente López Obrador aprovechó la investidura presidencial para descalificar el trabajo de ARTICLE 19, al insinuar que los fondos con los que la organización subsiste la hacen parte de un complot conservador y adversario

que está en contra de su gobierno. Menos de dos meses más tarde, el 7 y 13 de mayo, el presidente volvió a recurrir a la desinformación para atacar la labor que realiza esta y otras organizaciones que, frente a una clara inacción, indolencia y abuso del Estado, documentan, denuncian y acompañan a víctimas de violaciones a derechos humanos[82].

El movimiento de derechos humanos en México —así como en otros países con historias dolorosas de casos de desapariciones forzadas, tortura, ejecuciones extrajudiciales, privación ilegal de la libertad, etcétera— se financia a través de donantes, embajadas y financiadoras de otros países precisamente para no tener ataduras o confabulaciones con los gobiernos locales que vigila. La autonomía e independencia financiera que ello le confiere hacen de las organizaciones de la sociedad civil actores políticos relevantes en el proceso de democratización de México y en la denuncia permanente de violaciones y omisiones cometidas por el Estado, independientemente de quién ocupe los puestos de poder.

"El trabajo de defensa de los derechos humanos es una causa legítima y esencial para socie-

[82] ARTICLE 19. (2021). *Presidente de México recurre a la distorsión y guarda silencio sobre la violencia contra la prensa*. Disponible en https://articulo19.org/presidente-de-mexico-recurre-a-la-distorsion-y-guarda-silencio-sobre-la-violencia-contra-la-prensa/

dades democráticas"[83]. Por el contrario, la criminalización y estigmatización desde el Estado para acosar a quienes luchan por las personas y sus derechos son estrategias autoritarias que desinforman, intimidan y buscan callar a quienes denuncian la violencia e injusticia en nuestro país. En ese sentido, la insistencia en deslegitimar a ARTICLE 19, organización que defiende a periodistas del asedio del poder y procura el acceso de la ciudadanía a información pública y a TIC libres de censura debe leerse a la luz del contexto. Los contrapesos y el escrutinio público no son oportunos para gobiernos con tintes autoritarios y que dependen de su omnipotencia impune para controlar a la población.

Atacar al mensajero sólo busca desviar la atención del mensaje. La narrativa violenta que promueve el poder ejecutivo federal, y que se replica en otros actores políticos, es un mecanismo que busca desviar la atención de su incapacidad y falta de voluntad para responder a las dignas demandas de la sociedad. Los hechos nos muestran que los esfuerzos por diluir la voz de quienes respaldan causas legítimas, entre ellas la búsqueda del ejercicio efectivo a la libertad de expresión en línea, se han recrudecido en esta administración. Y en realidad eso no es lo más grave, sino que atacar a quienes defienden las libertades y derechos de la ciudadanía es necesariamente un ataque hacia la ciudadanía en sí misma.

[83] Ibídem.

LA DEFENSA DE INTERNET COMO ESPACIO CÍVICO

Los retos para la defensa de los derechos digitales en este país están relacionados con la determinación por parte del poder político de intentar controlar y desalentar el flujo informativo en internet. En paralelo, con recurrir al desprestigio hacia la prensa y las personas defensoras de derechos humanos, a la desinformación para defender las agresiones en su contra, y a expresiones de violencias directas hacia quienes resultan incómodos al régimen.

Enfrentar con dignidad y resiliencia a las agresiones, la omisión, la impunidad, la falta de interés y la falta de conocimiento de las autoridades es un camino de largo aliento. Ante este panorama tan desalentador, la contranarrativa que contrasta y reta el discurso estatal —que busca vulnerar derechos y personas— ha comprobado ser la mejor táctica de resistencia. Los datos, los hechos y la evidencia, documentados y difundidos a través de las cámaras, notas informativas y redes sociales de la ciudadanía, activistas y prensa han logrado fungir como una pared que resiste a la desinformación y ataques del poder político que usa los recursos públicos para librarse del escrutinio y cuestionamiento.

Frente a un Estado que busca desdibujar los derechos humanos en el entorno digital, considerándolos como un lujo y un peligro, y no como componentes de la democracia de nuestra épo-

ca, es responsabilidad de quienes radicamos en México el hacernos conscientes de este acecho generalizado hacia nuestros derechos y libertades. Un país democrático es aquel donde todas las personas pueden expresarse con libertad, seguridad e igualdad, al mismo tiempo en que pueden ejercer su derecho a la información, tanto en el entorno físico como digital. Sólo de este modo la sociedad puede llegar a tomar decisiones informadas, de tal forma que logren vivir a plenitud todos los derechos individuales y colectivos.

Lamentablemente todo lo aquí reseñado pone en evidencia la tendencia de violencia digital gubernamental y de control ciudadano que pone en riesgo lo anterior. La propagación de legislaciones restrictivas para el uso y acceso de internet y los derechos digitales, al mismo tiempo en que se incendia a la población mediante campañas de desinformación contra periodistas, medios de comunicación y personas defensoras de derechos humanos, es aún más nociva porque se da en un país tan sediento de verdad, memoria y justicia.

"Los Estados deben regirse bajo principios de garantía, protección, promoción, acceso y seguridad ante el uso de las TIC"[84]. En ese sentido, bienvenido sea el ejercicio de reconocer y acep-

[84] ARTICLE 19. (2021). *#LibertadNoDisponible: Censura y remoción de contenido en México*. p. 14. Disponible en https://articulo19.org/wp-content/uploads/2021/02/LIBERTAD-NO-DISPONIBLE-single-page.pdf

tar las violencias que sufrimos y de las que —inadvertidamente—, por comernos el cuento de quienes nos gobiernan, hemos llegado a reproducir. Sea esta una reflexión que nos indigne y nos mueva a la acción y a la defensa de internet y los derechos humanos, sabiendo que merecemos mucho más de lo que se nos ha devengado.

0120

La censura y la criminalización en el periodismo digital y feminista

ANAIZ ZAMORA

Anaiz es periodista feminista y activista con formación universitaria en psicología y ciencias de la comunicación. Es cofundadora de Luchadoras MX, un proyecto que marcó el inicio del periodismo digital feminista en México. Su trabajo se ha centrado en la documentación, investigación y seguimiento a la violencia de género, el feminicidio, la salud y la academia. Cuenta con un amplio acervo de publicaciones en formatos de texto, audio y video sobre feminicidio; materiales realizados desde la perspectiva de género. Su trabajo periodístico ha sido reconocido por la Suprema Corte de Justicia de la Nación. Actualmente realiza el ejercicio de periodismo multimedia "Cartografías del cuidado" enfocado en mapear las tareas de cuidado que sostienen la vida.

DESDE HACE DOS DÉCADAS hay una advertencia constante para quienes decidimos trabajar en medios de comunicación: "México es uno de los países más peligrosos para ejercer el periodismo", una afirmación que se puede leer en informes e investigaciones de organizaciones, que se repite en columnas de opinión y reportajes, una oración que acompaña marchas y manifestaciones; pero la frase carece de sentido hasta que se siente en el cuerpo, en el estómago, en la mandíbula. Se vive cuando dejas de escribir porque no te puedes concentrar, se entiende cuando estás "tronada" por todas las lágrimas que tuviste que aguantar durante las entrevistas, las coberturas y los regresos a casa.

"México es uno de los países más peligrosos..." no sólo se cuenta por los lamentables asesinatos de periodistas, y que suman 138 del año 2000 a la fecha, de acuerdo con el registro de Article 19[85]. También se refiere al miedo de pensar que "alguien" sabe mucho de ti. Ese peligro incluye las fotografías, insultos y amenazas que llegan a tu cuenta de Twitter, o a la cuenta del medio independiente —y muy pequeño— en el que trabajas; abarca las ocasiones en las que fuiste señalada de "vándala", "criminal", y hasta

[85] ARTICLE 19. (2021). *Periodistas asesinados/as en México, en relación con su labor informativa*. Disponible en https://articulo19.org/periodistasasesinados/

los bajos salarios, carencia de servicios médicos, ahorros y seguridad social[86].

"...para ejercer el periodismo", leer la frase también es recordar las coberturas que pudieron terminar de maneras lamentables, los riesgos que pasaron casi desapercibidos, pero que no debían existir. Entender esa oración también es cuestionar las decisiones que tomas: cuál solicitud de amistad aceptas y cuál no, dejas que tus amigas suban a redes sociales la fotografía que se tomaron contigo o les pides que no te etiqueten, publicas ese tweet o te reservas tu opinión. La libertad de expresión en México está en crisis, los efectos —pero también muchas formas de resistencia— pueden percibirse en las vidas de las mujeres.

"SÍ SABEMOS QUIÉN ERES"

La vigilancia es silenciosa. Es una estrategia que pasa desapercibida hasta que simplemente te das cuenta. Me di cuenta de esa realidad en mi tercer año de periodista cuando respondí una llamada en la redacción. Me buscaba alguien que me saludó con mi nombre completo y hablándome como si fuéramos grandes amigas. Me buscaban para ofrecerme una entrevista con la di-

[86] SinEmbargo MX. (2020). "Periodismo en México: informar para vivir, morir por informar". *OpenDemocracy*. Disponible en https://www.opendemocracy.net/es/periodismo-en-mexico-informar-para-vivir-morir-por-informar/

rectora de cierta institución, aseguraban que la nota que se acababa de publicar y en la que se mencionaba a la dependencia "tenía muchas imprecisiones", y que "esa nota estaba poniendo en riesgo los empleos de algunas personas".

El reportaje en cuestión documentaba lo complicado que es denunciar el acoso sexual y hacer uso de los programas que están diseñados para acompañar a las víctimas durante esos procesos. Lo escribí desde la rabia y la frustración, pero lo investigué y documenté desde la experiencia y acompañamiento de la jefa de información. Antes de llegar a la redacción, un tipo aprovechó el semáforo para apretarme las nalgas. Para ese momento, yo ya había leído toda la Ley de Acceso de las Mujeres a una Vida Libre de Violencia, el Código Penal y entrevistado a varias especialistas en violencia de género. Sabía que eso era una agresión y que podía denunciarlo, decidí hacerlo y el acompañamiento que me dio la abogada del programa fue una lista de razones por la que mi denuncia no iba a proceder y una explicación de lo complicado, tardado y costoso que iba a ser un proceso así por un delito que no iba a proceder porque "la nalgada no me había dejado un moretón".

Yo estaba segura de que no existían tales imprecisiones, la nota partía de una experiencia personal, había consultado las leyes y reglamentos de la institución, buscado datos, verificado esos datos, encontrado otros testimonios y hasta solicitado una entrevista que me negaron.

Acepté ir al encuentro con la directora de la institución y antes de dar mi nombre en la entrada, alguien ya me estaba esperando. "Sí sabemos quién eres, te vemos en todas las conferencias". El encuentro incluyó un recorrido por todas las notas que iban firmadas con mi nombre y en las que se mencionaba a la institución y un recorrido por los presupuestos, memorándums y oficios que acreditaban el programa que en mi caso no había funcionado.

Experiencias similares se siguen repitiendo, cuando pongo mi nombre en el listado de asistencia de una institución, cuando investigo un tema y un funcionario "muy amable" decide responderme de manera directa a mi correo, ¿cómo saben a qué extensión marcarme?, ¿cómo saben mi nombre completo?, ¿cómo saben cómo luzco?, ¿cómo encontraron mi correo? La vigilancia es silenciosa, pero muy efectiva.

Mis experiencias no son graves, no han pasado de servidores públicos que deciden saludarme o seguirme en Twitter. Estoy casi segura de que es parte del monitoreo de prensa de las dependencias y, al mismo tiempo, es resultado de mi huella digital, esa que he logrado disminuir, pero no erradicar. A diferencia de lo que nos enseñan en las escuelas tradicionales sobre periodistas que tienen fuentes anónimas a las que ven en un lugar oscuro y que hacen su trabajo con una libreta y una máquina de escribir, ahora mucho del periodismo de investigación lo hacemos detrás de una pantalla. Horas y horas de redactar y enviar

solicitudes de información, de buscar ese dictamen que está escondido en una página web nada amigable, de buscar los perfiles de los que están en el poder, usamos las tecnologías a favor de la libertad de prensa.

La vigilancia, hasta ahora, se ha transformado en miedo y asombro. Con el tiempo modificó mi comportamiento, mis decisiones y hasta mi forma de relacionarme. En #GobiernoEspia[87], R3D: Red en Defensa de los Derechos Digitales, junto con ARTICLE 19, oficina para México y Centroamérica, y SocialTIC, documentaron al menos 88 intentos de infección con el malware Pegasus en contra de periodistas y defensores de derechos humanos en México, una estrategia de vigilancia sistemática bastante costosa y altamente especializada, pero no es la única.

Ser periodista no es ser una figura pública (o al menos no debería serlo), pero es ser un nombre conocido. Nuestra identidad está al alcance de una búsqueda en Google y otras plataformas. Los detalles de tu vida privada no importan en el ejercicio de tu profesión, tampoco la forma en la que vistes o te ves, pero la vigilancia revela esos detalles que luego son sacados de contexto y son utilizados para la burla o el desprestigio. Estamos frente a un panóptico digital —así lo expli-

[87] ARTICLE 19. (2017). *Gobierno espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.* Disponible en https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

ca Alejandro Miranda— que pone nuestra privacidad e intimidad en juego.

Documentar la violencia de género y la poca acción de las instituciones de justicia ante las agresiones es uno de mis compromisos como periodista, pero al mismo tiempo es un acto político de nombrar y reconocer las violencias y agresiones que también me han atravesado el cuerpo, que le han cambiado la vida a amigas y a las mujeres de mi familia, es un acto de reivindicación de esas experiencias para nombrarlas desde otro lugar. Mi intención es hacer un periodismo más feminista, un periodismo que contribuya a la construcción de espacios seguros para las mujeres.

Enterarme del seguimiento minucioso que hacen de ese tipo de publicaciones no detuvo esa labor, pero, en un país en donde el 97%[88] de los casos de agresiones contra periodistas quedan en la impunidad, también aprendí que tenía que ser cuidadosa con todo lo que escribía, desactivar la geolocalización para no revelar los lugares en los que estaba y de alguna manera aminorar el riesgo en el que pueden estar las personas más cercanas a mí. Debo confesar que al principio esos cuidados rayaban en la paranoia.

[88] Trujillo, N. (2021). "El sexenio en el que los periodistas repetíamos: 'Nos van a matar'". *Pie de página*. Disponible en https://piedepagina.mx/el-sexenio-en-el-que-los-periodistas-repetiamos-nos-van-a-matar/

Si buscas la palabra censura en internet aparecen imágenes de seres oscuros y extraños que le tapan la boca a una persona, y aunque cualquier agresión es un intento por censurar la libertad de expresión, generalmente pensamos la censura de esa manera, asociándola a un agente de poder que decide sobre alguien más. Las historias de cómo se definía la línea editorial[89] de periódicos desde la presidencia durante los gobiernos priistas no se esconden en ningún sitio, pero en la época del periodismo digital, las formas de censura se han diversificado.

Es claro que los viejos métodos siguen funcionando: amenazas directas a los editores, compra de historias a modo, acusaciones de difamación y la negación de recursos de publicidad a los medios “incómodos”, pero nuevos agentes y nuevos medios se suman a la ecuación. Las políticas de moderación de contenidos en plataformas digitales y la solicitud de remoción de contenidos son una nueva forma de censura que utiliza menos recursos y esfuerzos. De acuerdo con Article 19, la remoción de contenidos se origina a través de tres vías: la primera, mediante solicitudes de

[89] Sánchez Parra, S. A. y Gil Pérez, A. P. (2018). *El día de la libertad de prensa en México como medio de control del gobierno sobre la prensa, 1951-1969.* Colombia: Universidad Autónoma de Bucaramanga. Disponible en https://www.redalyc.org/jatsRepo/110/11058502012/html/index.html

remoción de contenidos a las plataformas digitales, realizadas por parte del Estado o por actores privados. La segunda, mediante la comunicación directa de actores públicos y privados con periodistas o medios periodísticos, para exigir la eliminación de contenidos en sus sitios web o páginas de redes sociales. La tercera, mediante la ejecución de los términos de servicio o normas comunitarias de las plataformas digitales. Todas las vías se han hecho presentes cuando de una investigación sobre el derecho de las mujeres a decidir sobre su cuerpo se trata.

Hay temas que siempre ocupan los reflectores de las denuncias de censura: corrupción, narcotráfico, lavado de dinero, mafias empresariales, desvíos de recursos, contar esos relatos es tarea ardua de los periodistas, la valentía y la destreza para hacerlo merece un reconocimiento de pie, pero hay otros temas necesarios que también son censurados. Los cuerpos, la sexualidad, el placer y las decisiones de las mujeres siempre han resultado incómodas cuando se narran desde la autonomía y la voz de sus protagonistas. La sexualización del torso desnudo se permite en todas partes pues ahí el cuerpo está al servicio de alguien más, pero cuando los senos son parte de un ejercicio de protesta o reivindicación son censurados por algoritmos e inmediatamente removidos de las plataformas. Cuando se realiza un periodismo feminista, los cuerpos, sus reivindicaciones, sus curvas y sus capacidades son parte

esencial de las historias, muchas de ellas no pueden compartirse libremente.

Solemos hablar de Salud Sexual y Reproductiva, pero en esa frase se encuentran dos grandes campos que son ampliamente censurados en las redacciones, plataformas y otros espacios. Hablar sobre la capacidad reproductiva de las mujeres es una tarea aún más compleja. La primera vez que propuse una nota sobre las investigaciones que se realizan —evidentemente por mujeres— sobre las propiedades de la sangre menstrual y de cómo las industrias farmacéuticas se aprovechan del desconocimiento que tenemos de nuestros procesos naturales, para negarme el espacio, el editor simplemente me preguntó: "¿Y cuál es la nota?". Mi poca experiencia en el tema me impidió defenderlo. Insistí de manera personal en la investigación, pregunté a más mujeres cuáles eran sus experiencias con la sangre menstrual, qué tipo de dolores experimentaban, cómo les había ido en su visita al ginecólogo e incluso si podían identificar el color y olor de esa sangre, redacté la historia y la presenté, la respuesta fue: "Esa nota no va".

De nueva cuenta la experiencia no resultó en una agresión que me pusiera directamente en riesgo. Los insultos vinieron años después, cuando logré publicar la nota en un medio muy pequeño y abiertamente feminista, el texto se acompañó con una imagen de una copa menstrual usada. Durante ese día las notificaciones de la noticia se llenaron de insultos sobre lo asquerosa que era

mi historia, lo "feas" que eran las feminazis y de mensajes que pedían "hablar con el hombre a cargo", la publicación fue denunciada por personas que se sentían incómodas con ella. Facebook removió el contenido hasta que compañeras ciberfeministas nos acompañaron en el proceso.

Esa pequeña revista feminista se enfrentó a varios bloqueos de Facebook y dos ataques DDoS[90] que impidieron el acceso a los contenidos por completo. La falta de recursos económicos, técnicos y humanos terminó venciendo y el medio no existe más. De alguna manera, todos sus contenidos fueron censurados. En el informe *Violencia en Línea Contra Mujeres en México*[91], Luchadoras, Social TIC y APC hacen un llamado a reconocer las expresiones discriminatorias, así como la expulsión y el derribo de espacios de expresión como una forma de violencia relacionada con las tecnologías.

Pensar en la diversificación de las formas de censura a través de lo que permite la tecnología y el internet, también pasa por pensar las posibi-

[90] Un ataque DDoS ocurre cuando se provoca una denegación de servicio distribuida. Esto quiere decir que, de forma descentralizada se satura una página o servicio de internet, para evitar que otras personas puedan ingresar; menguando el acceso a la información y estableciendo una censura temporal del sitio afectado.

[91] Zamora, A. (2017). *La violencia en línea contra las mujeres en México*. México: Luchadoras. Disponible en https://luchadoras.mx/informe-onu/

lidades que estas herramientas le dan al periodismo. Ya no escribimos para el papel, para las planas impresas, las y los periodistas hemos inventado, rescatado y encontrado nuevas formas de narrar historias. Hay medios que ahora sólo piensan sus historias en formatos digitales, pero ¿cómo hablar de derechos reproductivos para estas audiencias cuando Instagram también censura de manera inmediata las fotografías de partos, flujos vaginales y del cérvix? "La censura algorítmica replica la mirada masculina, occidental y moralizante en línea", nos dice Ixchel García[92].

Sobre parteras, su organización, la forma en la que cuidan los conocimientos ancestrales y resisten ante procedimientos médicos que violentan los cuerpos y experiencias femeninas aún tengo entregas pendientes. Documentar sus historias no es sencillo, pues pertenecen al mundo privado, pero hacerlas públicas es enfrentarse a la censura de Facebook y de quienes consideran que es irresponsable ir a una partera cuando se puede acudir a un hospital.

En una investigación[93] realizada por la UNESCO

[92] García, I. (2021). "Cuerpxs desnudxs que asustan a los algoritmos". *Internet_feminista.* Disponible en https://luchadoras.mx/internetfeminista/2021/03/23/cuerpxs-desnudxs-que-asustan-a-los-algoritmos/

[93] Posetti, J., Aboulez, N., Bontcheva, K., et al. (2021). *Violencia en línea contra las mujeres periodistas: Instantánea mundial de la incidencia y las repercusiones.* UNESCO. Disponible en https://

y el Centro Internacional para Periodistas sobre violencia en línea contra mujeres periodistas, se da cuenta de que una de las respuestas más frecuentes ante las agresiones digitales "es la autocensura en medios sociales". El hecho de que la decisión sobre lo que resolvemos contar o callar sea de nosotras mismas, genera niveles más altos de ansiedad. Puesto que nuestro objetivo es sacar del ámbito privado los temas que nos parecen urgentes, es una decisión que pesa y que genera frustración. Historias sobre feminicidio, desaparición o defensa de los territorios dejan de contarse.

En reuniones con compañeras periodistas es común escuchar que deciden guardar su opinión sobre ciertos temas ante el inminente riesgo de enfrentarse a una ola de mensajes que van a cuestionar su credibilidad, sus fuentes y hasta su nivel de conocimientos sobre un tema en el que son expertas. También es común escuchar que han optado por prácticas de cuidado digital que incluyen el evitar compartir los lugares que les gusta visitar, las fotografías de las fiestas familiares o de las reuniones entre amigas. El internet es el nuevo espacio público que por momentos decidimos abandonar. Cada vez que el miedo, el temor y hasta el cansancio de enfrentarme a todos los que van a insultarme o burlarse de mí me lleva a decidir no publicar un tweet o una nota

www.icfj.org/sites/default/files/2021-03/Online%20Violence%20Against%20Women%20Journalists%20Global%20Snapshot%20Spanish.pdf

entiendo por qué decimos que la libertad de expresión está en crisis. Como periodista he aprendido a no callar, como feminista estoy convencida de que "calladita no me veo más bonita".

"ELLAS SON LAS VÁNDALAS"

Me identifico como periodista feminista, nunca como experta o especialista en la materia, no me atrevo a teorizar sobre las apuestas políticas, pero hay una fecha que yo marcaría como el inicio de una nueva etapa en los movimientos: el 24 de abril de 2016. No fue mi primera marcha, ni mi primera manifestación. Ya había caminado junto a madres de víctimas de feminicidio, junto a madres en búsqueda de sus hijos e hijas, junto a mujeres que denunciaban la violencia política y laboral, y ya tenía varias notas publicadas sobre el 8 de marzo o el 25 de noviembre; pero esa fue la primera vez que vi la Avenida Reforma llena de mujeres y jóvenes convencidas de reclamar el espacio público, la primera vez que una marcha comenzó en el Estado de México, la primera vez que realmente se formó una marea violeta.

La cobertura de ese acontecimiento histórico se hizo desde el corazón, la rabia y la memoria. Tomábamos las fotografías y las compartíamos de manera directa en redes, no nos dimos cuenta de todas las que habían sido censuradas porque se mostraban pezones o eran ilustraciones de vaginas hasta días después, cuando la emo-

ción se asentó e hicimos el recuento de lo ganado, pero también de los riesgos que ahora enfrentábamos, las activistas, defensoras y periodistas estábamos siendo identificadas y señaladas en internet, nuestras identidades digitales, que hasta ese momento parecían anónimas, fueron localizadas y en los grupos de trolls se organizaban ataques masivos, fotografías de perros asesinados, de pistolas y de balas comenzaron a llegar a nuestras cuentas. Habíamos dejado claro que no íbamos a permitir una agresión más y al patriarcado no le gustó.

El #24A fue la primera movilización en donde las mujeres se reconocían abiertamente feministas, sólo fue el primer rugido. La violencia y las violaciones a derechos humanos, pero sobre todo la impunidad y la inacción estatal no han cesado. Dar cobertura a las movilizaciones y manifestaciones feministas es cada vez más cuestionado. Las que salimos a las calles, y a las redes, sabemos que valen más las vidas que los monumentos, que el glitter no es adorno, es un recurso desesperado por decir: "¡Basta ya!".

Si tocan a una, respondemos todas, ese es el sueño, pero los agresores buscan a la responsable, a la que —según ellos— organizó las manifestaciones y le "ordenó a las otras" que "hicieran desmanes". El periodismo feminista acompaña las decisiones de las otras y también busca ser una herramienta de información para que esas elecciones se lleven a cabo con seguridad y sin riesgos. Esa fue mi apuesta como editora y re-

portera durante las movilizaciones que se organizaron en la Ciudad de México para denunciar que la policía, en lugar de cuidar, agrede a las víctimas, pero todo se salió de control en medio de esa cacería de brujas en la era digital. Ya existía una amenaza. Se iban a presentar cargos penales contra quienes habían provocado daños a la Fiscalía de Justicia de la Ciudad de México, era posible identificarlas a través de los videos que circulaban en redes sociales. La advertencia avivó más la rabia y la marea violeta fue convocada para reunirse en la Glorieta de Insurgentes. Antes de que se reunieran, desde el medio en el que estaba habíamos publicado información sobre cómo salir a las calles de forma segura.

Bastaron unos cuantos retweets señalándonos como las organizadoras de la manifestación para que la viralización hiciera el resto en cuestión de minutos. Cada post se respondía por dos bandos. El primero integrado por quienes no salieron a las calles y agradecían la fuerza de quienes estaban presentes, el segundo conformado por todas las personas indignadas que no dudaban en decir "esas son las vándalas que organizaron todo". En los más de 3,200 mensajes que recibimos en cuestión de horas había acusaciones serias, de transgredir el orden público, provocar incendios, dañar los monumentos históricos y "no respetar el patrimonio histórico". Los mensajes que nos acusaban de vándalas también venían acompañados de insultos y en algunos de ellos se pedía que un régimen como el de

Gustavo Díaz Ordaz —responsable de ordenar el asesinato de estudiantes durante las manifestaciones de 1968— volviera a "poner orden".

No fue la primera vez que las redes del medio se llenaron de insultos y amenazas. Cada publicación que mencionara la palabra aborto recibía sus respectivos mensajes llenos de oraciones que pedían por "la salvación del alma de las asesinas de bebés" y versículos de la Biblia, pero sí fue la oleada de criminalización más fuerte y que se acrecentó a cada minuto. Si bien no fueron presentados cargos penales, como suele ocurrir en los casos en donde el aparato de justicia se usa en contra de quienes resultan incómodos, responsabilizarnos de alguna manera por las manifestaciones que se estaban llevando a cabo nos demandó tomar un descanso y buscar un lugar seguro para desahogarnos y sanar los efectos del ataque.

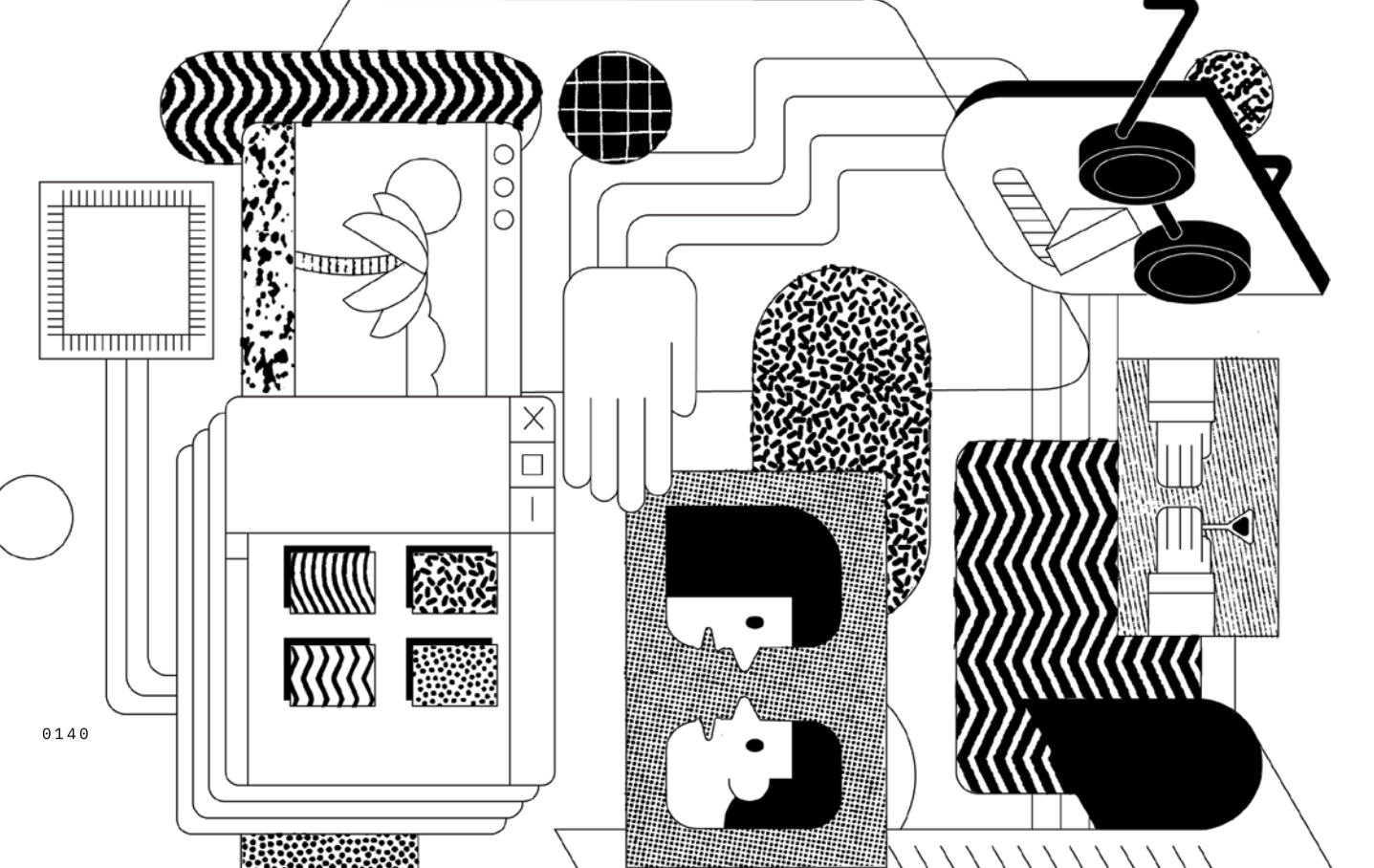
"LAS REDES SALVAN VIDAS"

Como lo he mencionado en múltiples ocasiones a lo largo de este texto, los momentos de riesgo, las experiencias de violencia, censura y criminalización no han puesto en riesgo mi vida o mi integridad física, sin embargo, sí han tenido un impacto en mi estabilidad emocional y mi salud mental. Las coberturas cansan y entristecen, pero las agresiones desgastan. Mis tiempos de concentración son menores, las ganas de estar

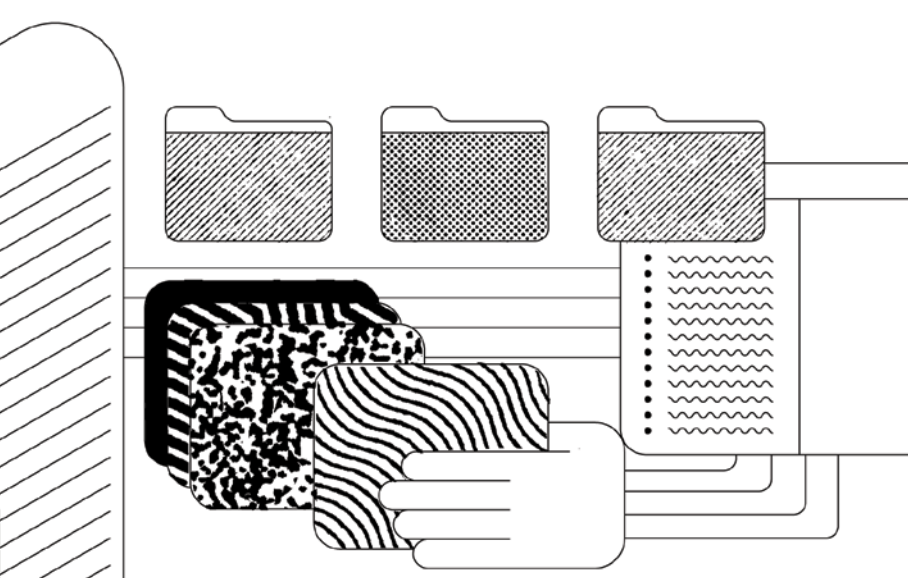
en internet durante esos momentos desaparecen por completo, los dolores de cabeza o de estómago aparecen de manera constante. Identifico mi historia en la de otras compañeras que deciden darse un tiempo en los medios, renunciar a sus trabajos y escribir historias más espaciadas, en las que llevan un registro de todas las tristezas del día y en las que buscan recetas y suplementos para evitar el insomnio.

Estoy próxima a cumplir 10 años en el periodismo, desde que inicié y, hasta ahora, el principal medio de distribución de mis reportajes y notas ha sido el espacio digital. Las tecnologías me han permitido acceder y profundizar en muchas de las investigaciones que realizo, profesionalizarme y adquirir nuevos conocimientos. No busco renunciar a ellas. En este tiempo las agresiones y los ataques han estado presentes, pero también las amigas, las compañeras y las aliadas.

No fue hasta que llegué a espacios convocados por ciberfeministas que entendí que podíamos hablar de cuidados digitales y no de seguridad digital; que los talleres para aprender estrategias de protección no tenían que ser un espacio de miedo y paranoia, y podían ser un espacio de escucha activa y dudas compartidas. También fue hasta que llegué a reconocer y nombrar que el periodismo que hago tiene una apuesta política que comencé a sanar las violencias, hay conversaciones urgentes que nos debemos entre periodistas, pero que estamos comenzando desde distintos espacios.



0140



Apuntes de la lucha por la cultura libre y acceso al conocimiento en México

IRENE SORIA GUZMÁN

Irene Soria es doctoranda en Estudios feministas, académica, diseñadora gráfica y activista de software y cultura libre. Actualmente es la representante líder de México en el Consejo Global de la Red Creative Commons. Comenzó a usar software libre en el 2009 y, desde entonces, sólo usa tecnologías y recursos abiertos para su ejercicio como diseñadora gráfica y profesora. Se ha desempeñado como tallerista, facilitadora, profesora, ponente y conferencista en México y en el extranjero. Sus temas de interés van y vienen sobre feminismo, tecnología, cultura libre, seguridad digital, software libre, cultura hacker, programación y educación.

"ES QUE NO SABEN LEER la ley", decían las personas abogadas que defendieron las reformas a la Ley Federal de Derecho de Autor en México (LFDA), para referirse despectivamente al grupo de activistas que manifestamos nuestra inconformidad a dichas reformas a través de la campaña "Ni censura ni candados" en julio de 2020.

Aunque las reformas se aprobaron, y un mes después se decretó su inconstitucionalidad, la acción reabrió un debate necesario en torno a los modelos tradicionales de derecho de autor y sus implicaciones en el acceso a la cultura, así como la problematización de los candados digitales que operan sobre todo en la esfera tecnológica, pero que subyacen a la conformación de las sociedades humanas actuales. El enfrentamiento de algunas posturas en torno a estos temas aborda las tensiones que subyacen en la compartición a partir del uso masivo de internet, más específicamente, en la difusión de música, imágenes, libros en pdf, artículos de investigación y, en general, de todo objeto cultural digital.

Estas tensiones, en el terreno del acceso a la cultura y la generación de conocimiento, podrían esbozarse, por un lado, a) el acceso libre al conocimiento; y por el otro, b) las restricciones de propiedad intelectual y derecho de autor. Por su parte, el grupo de personas que defienden el derecho de acceso libre al conocimiento, y que lo colocan en la esfera de los bienes comunes, apelan a que estos deben de ser públicos y gratuitos —más aún, si dicho conocimiento se "genera" a

partir de financiamiento del erario—. Se trata de activistas del conocimiento libre y abierto, quienes creen que encerrar los objetos culturales detrás de cuotas de pago elevadas o a través de candados digitales que impiden la copia y la compartición, sólo frena el avance de las artes y las ciencias, y, por lo tanto, del bienestar social.

Por otro lado, hay quienes sostienen lo contrario, que el pago de cuotas o la implementación de limitaciones a la copia, o el ensanchamiento de las leyes de protección de derecho de autor, ayudan a incentivar la creación cultural y a cubrir el trabajo de personas creativas. Pugnan por que los principios de "propiedad privada" se apliquen al conocimiento y la cultura y, por lo tanto, se pague para tener acceso a ellos.

DEFENSA DE LA PROPIEDAD INTELECTUAL Y LOS CANDADOS DIGITALES PARA LA RESTRICCIÓN

Para ejemplificar brevemente las implicaciones de ciertos candados digitales que se justifican a través de los argumentos en defensa de la propiedad intelectual, y que se vieron legitimados en una de dichas reformas de la LFDA, propongo remontar un escenario cercano partiendo de algunas metáforas.

Imaginemos que nuestra librería local decide cerrar el negocio debido a la pandemia y que recogerá los libros que ya nos vendió, devolviéndo-

nos el costo que pagamos por ellos. Imaginemos también que el personal de esa librería tiene acceso a nuestra casa, se dirige a nuestros libreros, busca los libros que nos vendió y se los lleva, dejando en nuestra mesa de centro el monto que habíamos pagado por ellos. En caso de que esos libros tengan algunas notas o marca que hayamos dejado como camino de nuestro conocimiento, el negocio nos compensará con 25 dólares más del costo del libro, pero eso sí, habrá que olvidarnos de nuestras anotaciones[94]. Si bien, no todas las analogías del entorno offline pueden ser válidas para entender algunos fenómenos, el ejemplo anterior nos ayuda a explicar la magnitud de un problema que, por desgracia, no es nuevo, ya que esta metáfora nos ayuda a evidenciar algo que ha sucedido en la esfera virtual en múltiples ocasiones y que pocas veces dimensionamos.

En julio de 2019, Microsoft cerró su tienda de libros en línea y dejó de tener disponibles sus volúmenes electrónicos. Aunque las personas que adquirieron un ebook de la Microsoft Store obtuvieron el reembolso completo por sus compras, no tuvieron acceso a ninguno de los ejemplares, incluso los que fueron descargados de manera gratuita, ya que fueron borrados de todos los dispositivos electrónicos en los que alguna vez

[94] Microsoft. (2019). *Books in Microsoft Store: FAQ*. Disponible en https://support.microsoft.com/en-us/help/4497396/books-in-microsoft-store-faq

se leyeron. Esta acción, naturalizada en los entornos mercantiles digitales, supone una invasión a la privacidad, evidenciando con ello el nivel de control y acceso que tienen las grandes corporaciones a los dispositivos de las personas.

Desde sus orígenes, Microsoft Store, así como muchos otros servicios de consumo de canciones, películas, fotografías o videos representados en ceros y unos y distribuidas por grandes empresas, cuentan con mecanismos que controlan la copia, reproducción o visualización de archivos. A estos mecanismos se les conoce bajo el rubro DRM, cuyas siglas en inglés significan Digital Rights Management (Gestión de Derechos Digitales). El DRM es, en resumen, cualquier estrategia puesta en marcha por las compañías que empaquetan contenido digital para controlar la distribución de obras culturales. Impiden, por ejemplo, que estas se compartan en otros dispositivos no asociados a los de la persona que lo compró. Es precisamente lo que te impide pasar a otra persona la canción que compraste en iTunes, o grabar en un CD tu lista de reproducción de Spotify para regalarlo a alguien cercano —como solíamos hacer en el siglo pasado con los cassettes o los discos compactos.

A pesar de que no existe una norma en la industria para los DRM, este se implementa generalmente a través de algoritmos que conforman el software en los dispositivos. Dicho software emplea códigos incrustados en la mayoría de los contenidos digitales, ¡y también en el hardware!

Lo que quiere decir que los reproductores de mp3, celulares, discos duros, lectores de blueray y hasta los adaptadores de Mac que se conectan a proyectores, incluyen mecanismos DRM de fábrica. La activista argentina, Beatriz Busaniche, afirma que estos algoritmos "deniegan o autorizan de manera inapelable el acceso a la obra de acuerdo a las condiciones que pueden ser cambiadas unilateralmente por el proveedor de la obra con total independencia de lo que dicte el marco jurídico[95]. Un libro con DRM no puede compartirse ni mucho menos ser copiado, limitando así su distribución a quien pueda comprar el permiso de leerlo; asimismo, permite borrarlo de los dispositivos, incluso sin que las personas usuarias lo sepan. El caso de Microsoft en el 2019 no es de ninguna manera el primero: 10 años antes, en el 2009, Amazon borró de los Kindle el libro *1984* de George Orwell[96] y, en 2005, Sony instaló un software espía en miles de computadoras a través de los DRM incrustados en algunos CD de música[97].

---

[95] Busaniche, B. (2007). "Tecnologías de restricción: los sistemas DRM". *Monopolios Artificiales sobre Bienes Intangibles.* Argentina: Vía Libre.

[96] El País. (2009). "Amazon retira dos obras de Orwell de los Kindle de sus clientes". *El País*. Disponible en https://elpais.com/tecnologia/2009/07/20/actualidad/1248080461_850215.html

[97] Ver: https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

Debido a que el DRM atenta contra los derechos digitales, varias personas hemos cuestionado severamente su implementación en el entorno digital. Puesto que estos mecanismos dificultan la accesibilidad a las obras generadas con y a partir de recursos digitales con licencias restrictivas, estas impiden la adaptabilidad a múltiples formatos y, en consecuencia, obstaculizan el acceso al conocimiento y la preservación digital con el paso del tiempo.

Para quienes somos activistas en favor de la libre circulación de las obras digitales, el DRM no "protege" los objetos culturales, sino que limita y restringe su circulación en beneficio de los intereses de unas pocas personas, quienes son dueñas de las empresas que median la distribución. Por esto es que nos referimos al DRM como Digital Restriction Management (Gestión de Restricciones Digitales), y nos oponemos categóricamente a su implementación. Por poner un ejemplo: ¿te has preguntado cómo se puede acceder hoy en día a una película producida en los dos miles? Es muy probable que lo hagamos a través de servicios de terceros, pero no siempre se encuentran en repositorios públicos, no hay copias físicas suficientes y, literalmente, hay que pagar un derecho para verla una vez, restando la posibilidad de almacenarla o preservarla —al menos de manera legal—, como hicieran las antiguas filmotecas con el celuloide. Parafraseando al abogado estadounidense Lawrence Lessig: resulta cada vez más fácil ac-

ceder a una obra del siglo XVII, que a una obra digital del siglo XXI.

Actualmente, existen diversos mecanismos que buscan eludir los DRM, pero que son considerados ilegales ya en la reforma de la LFDA en México, pues se les asocia a la piratería y se les considera una amenaza a los derechos de autor. Sin embargo, antes de criminalizar o sancionar estas acciones, habría que ampliar la reflexión a múltiples esferas y difundir el análisis desde diversos enfoques, ya que "el DRM sirve para limitar la copia, bajo el argumento de frenar la piratería y proteger al creador. La realidad es que este mecanismo rara vez funciona y, cuando lo hace, es de manera restrictiva"[98].

Es por ello que campañas como Defective by Design de la Free Software Fundation, o algunas más de la Electronic Frontier Foundation, llevan varios años en la lucha por las libertades digitales. La esperanza de que las nuevas generaciones frenen o al menos cuestionen el uso de DRM —aun después de 14 años de escándalos y de su amplia proliferación— está en la información, pues como diría uno de los ejecutivos de Disney en el 2005: "Si los consumidores llegaran a saber que hay un DRM, qué es y cómo funciona, ya habremos fallado"[99].

---

[98] Flores, P. (2013). "DRM: el intento por regular el derecho a copiar". *QORE*. Disponible en https://www.qore.com/articulos/5193/DRM-el-intento-por-regular-el-derecho-a-copiar#sthash.505Zbyab.dpuf

[99] "If consumers even know there's a DRM, what it

HERRAMIENTAS PRIVATIVAS Y ACCESO AL KNOW-HOW

Sin embargo, el DRM no es la única restricción técnica para el acceso a la cultura, también lo es la manera en la que concebimos el uso de herramientas tecnológicas para la creación de contenidos, y cómo permea en la enseñanza en centros educativos, perpetuando el uso de tecnologías privativas en áreas creativas. Para explicar esta problemática, propongo nuevamente, un ejercicio imaginativo:

Imaginemos que pretendemos ingresar a una de las mejores escuelas de fotografía en el país y que uno de los requisitos para ello, dice: "En esta escuela sólo usamos herramientas de calidad, y lo más utilizado en el mercado, por lo que para todas las tareas es necesario y requisito indispensable contar con la línea de productos Nikon en cámaras y lentes"[100].

---

is, and how it works, we've already failed". Declaración de Peter Lee, Disney Executive en entrevista con *The Economist* en 2005. Contenido que, por cierto, está protegido por un mecanismo DRM: https://www.economist.com/special-report/2005/09/01/science-fiction

[100] Ejemplo que ofrece Lila Pagola en la Presentación de la charla en las IV Jornadas de Reflexión, Investigación y Gestión del Diseño en la Escuela Spilimbergo, y en las Jornadas de Conocimiento Libre de la Universidad de Villa María. Septiembre 2010. Disponible en http://www.nomade.org.ar/sitio/?p=308

De existir esta especificación en alguna escuela, seguramente nos preguntaríamos: ¿por qué este centro educativo se limita al uso de una sola marca de cámaras y lentes?, ¿por qué Nikon? Si yo tengo Canon, ¿tengo que comprar una Nikon? Por muy ridícula e improbable que parezca la suposición, esto es lo que sucede en la gran mayoría de la enseñanza en áreas creativas en México. Si bien no tienen como requisito el uso de una sola marca de cámara fotográfica, sí supeditan sus clases de herramientas digitales al uso de sólo un tipo de programa[101], una sola y única marca, y con ello, muy probablemente, una sola manera de resolver digitalmente sus requerimientos de producción, una única forma de "hacer" y resolver problemas.

Estos programas restringen y privan de varias libertades a las personas usuarias y es conveniente problematizar su uso. Por ejemplo, los programas que corren en las computadoras de las universidades públicas suelen ser ilegales, pues se tratan de copias no autorizadas, y, a la larga, se fomenta que el estudiantado adquiriera software "pirata"[102], pues comprar una licencia

[101] En el caso de la enseñanza de Diseño Gráfico, por ejemplo, el uso exclusivo de Photoshop, Illustrator y toda la suite de Adobe, como única herramienta posible para la creación visual digital.

[102] Prefiero el uso del término "copia no autorizada", en lugar del criminalizado término de "piratería", y aunque comparto la idea de que "los piratas sólo están en los barcos", también reconozco

de la suite completa de programas para la edición de videos, gráficos y audio es prácticamente inalcanzable para el alumnado de universidades públicas —aunque también para las privadas—. Con la pandemia del coronavirus en el 2020-2021, la problemática se acentuó, pues no había manera de acceder a las versiones pagadas de los programas si no era a través de las computadoras de los planteles o algunas (pocas) licencias para el uso personal. Vale la pena preguntarse, ¿qué implicaciones tiene para el acceso al conocimiento y la información la creencia constante del uso de una única herramienta tecnológica más usada en el mercado?

Aunado a esto, muchas de las versiones de los softwares comerciales precisan cada vez más requerimientos de hardware y, con ello, la necesidad de cambiar de computadora por una más reciente, más poderosa y, claro, más cara. Todas estas —y más— prácticas que parecen "normales", en realidad son condicionadas y obligadas por una compañía transnacional de la cual somos público cautivo, convirtiendo a algunos sectores creativos de México en "esclavos de la innovación tecnológica". Como siempre, estas problemáticas afectan mucho más a las poblaciones históricamente vulnerables, a poblaciones en el margen o precarizadas, ya que amplía aún más la brecha digital y les aleja de la posibi-

---

la apropiación de algunos colectivos de este término a manera de manifiesto político.

lidad de acceso a la cultura, al conocimiento y a la creación de contenidos asistidos por un equipo de cómputo. De igual forma, el código fuente, o lo que algunas personas llaman "la receta de cocina" de esos programas es cerrado, es un secreto y nuevamente funciona bajo esquemas de propiedad intelectual, por lo que priva el conocimiento de formas de "saber-hacer", ya que no sabemos cómo está hecho o cómo funciona el software que usamos —desde las apps en el celular, hasta los sistemas operativos que vienen instalados "de fábrica" en los equipos de cómputo.

Estas y muchas otras implicaciones del software de patente han hecho que un grupo de personas opten por llamarle software privativo para referirse a un software que "priva" libertades y ofrece ciertas limitaciones. Algunos de esos grupos, a los que personalmente me adscribo, han decidido crear y optar por el camino del software libre, el cual permite no sólo que las y los usuarios conozcan las líneas de código con el que se ha hecho el programa, sino que sea copiado, distribuido y mejorado sin restricción ni problema alguno, convirtiéndose así en una alternativa viable al software privativo. Personalmente, desde el 2009, he usado exclusivamente software libre para mi trabajo como diseñadora, comprobando que es una alternativa viable. Desde el 2012, decidí enseñarlo en las asignaturas prácticas en las materias de comunicación que imparto, poniéndome como planteamiento político no enseñar software privativo y buscar

con ello que el estudiantado conozca otras formas de "saber-hacer".

ACTITUD COPYLEFT

Uno de los pilares del movimiento de software libre es la apertura del conocimiento en tanto que promueve la apertura del código fuente de programación, y con ello, el know-how de nuestros programas de cómputo. El dilema ético de la propiedad intelectual, y el cuestionamiento de la concepción de autoría, que se aleja de la noción de "dueño/a" se ha puesto al día con términos y usos documentados en el terreno de la creación.

Las académicas argentinas, Lila Pagola y, años después, Bianca Racioppe han llamado actitud copyleft al conjunto de ideas, formulaciones y puesta en práctica de diversas formas de compartición. Se refiere a la motivación de diversos generadores de objetos culturales a compartir sus producciones, a ponerlas a disposición del público para ser modificadas, distribuidas y forjar con ello las bases del movimiento de Cultura Libre. La actitud copyleft está basada en la reflexión de las múltiples transformaciones de las herramientas tecnológicas en relación con los "saber-hacer", que a su vez se contraponen a las reglas establecidas y a los imaginarios hegemónicos. De esta forma, el flujo de objetos culturales en la era digital permite cuestionar ciertas relaciones de poder-saber y, con ello, los refe-

rentes de lo que significa ser autor-autora, qué es la obra y qué es el proceso creativo[103].

Cuando un autor o autora toma conciencia de lo anterior, es probable que también comience a optar por los licenciamientos abiertos, es decir, que libere su obra a través de licencias permisivas basadas en el copyleft, permitiendo con ello que la obra pueda compartirse e incluso modificarse con el pleno permiso de quien la generó y, por lo tanto, facilitar el intercambio de conocimientos. Cabe señalar que el término copyleft es un juego de palabras que busca anteponerse al copyright, que se propone como una forma de darle la vuelta a "todos los derechos reservados" y a la restricción de la copia que implica el copyright, para pasar al derecho de copia y reinterpretación, propias de la génesis de la creatividad.

Para algunas personas, los licenciamientos permisivos, la cultura libre y la actitud copyleft, resultan utópicos, irreales, carentes de algunos ejes o limitante en otros, sin embargo, la propuesta es cuestionar los paradigmas establecidos que damos por hecho y que se han probado insuficientes en la era digital. Quizá valga la pena abrir camino hacia una nueva actitud que podría traernos más beneficios que limitantes a la sociedad en su conjunto.

[103] Racioppe, B. (2016). "Autor y creación: significados en disputa en la actitud copyleft". *Razón y palabra.* Vol. 20. No 95. Ecuador: Universidad de los Hemisferios.

Ahora bien, la actitud copyleft tiene sus orígenes en el hacktivismo (hacker + activismo) que, a su vez, proviene de la cultura hacker. En este tema, las personas hacker se preguntan: ¿de quién es el conocimiento?, ¿este debe ser reconocido como valioso sólo cuando viene de sujetos autorizados por su función en la estructura económica? En la búsqueda de una sociedad justa, para el hacktivismo, la lucha del conocimiento de nuestra época se equipara a la de la tierra o a la del capital, es decir, una lucha entre propietarios, que defienden o amplían su reivindicación de la propiedad privada, y entre los desposeídos, que luchan por ampliar o defender la propiedad pública. Así pues, si los agricultores luchan contra el despojo de la tierra, los obreros contra el despojo de su mano de obra, las y los hackers lucharán por socializar los flujos de información y del conocimiento[104]. Es por ello que algunas personas hacktivistas ven en las empresas tecnológicas una amenaza a las herramientas inmediatas de producción, en tanto que el poder del mercado se apropia de la información y del aprendizaje libre, fruto de una red de conocimiento; generando una especie de escasez artificial, a partir de la acumulación de información. Este poder del mercado influye incluso en las definiciones que el Estado hace sobre la represen-

[104] Wark, M. (2006). *Un manifiesto hacker*. Barcelona: Alpha Decay.

tación de la propiedad en lo digital[105], desencadenando en el endurecimiento de leyes restrictivas de propiedad intelectual, que van en detrimento del bien común.

LIBERA TU OBRA

Una opción que resulta ser útil para llevar a la práctica la actitud copyleft y compartir nuestra obra o tomar obras de otras personas, sin que esto represente un acto ilegal —pues nos habrá dado el permiso de uso—, así como seguir otorgando el crédito a quien tiene la autoría, y que preserva el corazón del hacktivismo, son las licencias Creative Commons.

Las licencias Creative Commons (CC) son una iniciativa del abogado estadounidense Lawrence Lessig, que están inspiradas en la licencia GPL (General Public Licence) del Software Libre y, a su vez, en el copyleft que pretende darle una vuelta al concepto de copyright, es decir, el artista protege algunos derechos —como el de su autoría, por ejemplo— y libera algunos otros, como la posibilidad de que otros copien, distribuyan, modifiquen o hagan uso comercial de su obra. Estas licencias nos ofrecen múltiples beneficios, como la posibilidad de que nuestra obra sea mucho más difundida y nuestra autoría, respetada.

[105] Ídem. p. 96.

Hay seis tipos de licencias Creative Commons, que van desde la más permisiva —pueden hacer lo que quieran con tu obra, siempre y cuando te otorguen el crédito— hasta la más restrictiva —que no lucren con tu obra, que no hagan obras derivadas y que te den el crédito—. Algunas de las variantes de estas licencias, como la última mencionada, no son propiamente licencias copyleft. Vale la pena señalar que las licencias Creative Commons son sólo unas de tantas opciones —quizá de las más conocidas— para llevar a la práctica esta actitud copyleft. Sin embargo, existen otras aún más específicas que apelan a la compartición siempre y cuando no sea con fines corporativos y capitalistas, como es el caso de la Licencia de Producción entre Pares, una propuesta de otro tipo de licenciamiento conocido como copyfarleft.

LAS SEIS LICENCIAS CREATIVE COMMONS[106]

CC: BY	**Licencia de reconocimiento (BY)**
	Es la más abierta; en esta licencia sólo hay que darle crédito al autor de la obra. Quien usa la obra puede copiarla, difundirla, modificarla, hacer obras derivadas y hasta hacer uso comercial de ella. En las seis licencias Creative Commons es obligatoria la atribución de autoría.
CC: BY - SA	**Licencia de reconocimiento (BY) – Compartir igual (SA)**
	Esta licencia permite hacer todo lo mencionado en la anterior, pero si creamos una obra derivada debemos liberarla con la misma licencia (es decir, no se puede registrar bajo copyright). Esta es usada por Wikipedia.
CC: BY - ND	**Licencia de reconocimiento (BY) – Sin obra derivada (ND)**
	Esta licencia permite la redistribución comercial o no comercial, siempre y cuando no se modifique la obra, es decir, si usamos el trabajo del autor no podemos hacerle ningún cambio ni obra derivada.

[106] Todo este subtítulo es autoría de José Flores. Disponible en https://www.qore.com/articulos/9801/Licencias-Creative-Commons-para-principiantes

CC: BY - NC	**Licencia de reconocimiento (BY) – No comercial (NC)**
	Esta licencia permite que una persona distribuya, modifique o cree una obra derivada a partir de la obra protegida, siempre y cuando no se utilice con fines comerciales. Las obras derivadas no están obligadas a usar la misma licencia.
CC: BY – NC – SA	**Licencia de reconocimiento (BY) – No comercial (NC) – Compartir igual (SA)**
	Al igual que la licencia anterior, permite que una obra sea distribuida o modificada sin uso comercial, siempre y cuando el trabajo derivado también sea licenciado en condiciones idénticas.
CC: BY – NC – ND	**Licencia de reconocimiento (BY) – No comercial (NC) – No derivado (ND)**
	La licencia más restrictiva de todas. Permite que otros descarguen y distribuyan la obra, pero sin modificaciones ni uso comercial.

HACKEAR AL SISTEMA

En muchas ocasiones he usado el término hackear como una metáfora para referirme a la necesidad de modificar el sistema desde adentro, conocer cómo funciona un mecanismo para luego irrumpir en él y mejorarlo para un bien común. Considero que los hacks a los modelos restrictivos de propiedad intelectual, accionados desde el derecho de autor, son precisamente los movimientos de acceso abierto. El software libre, el

copyleft, la ciencia abierta, los recursos educativos abiertos, la cultura libre, el hacktivismo, la cultura hacker, sostienen que tanto la ciencia, la cultura y, en general, el conocimiento manifestado a través de cualquier objeto cultural, fueron creados por gente parada "sobre hombros de gigantes". Gracias a que las personas que nos antecedieron compartieron sus saberes, hoy quienes creamos, los hemos heredado.

Hay quienes creemos que el objetivo de la compartición en tiempos de internet no es solamente que funcione de manera ininterrumpida, sino también de manera legal en todo el mundo. Esto sólo será posible en la medida en la que las sociedades nos cuestionemos la incompatibilidad del espíritu comunitario del conocimiento con la propiedad intelectual de la economía capitalista, que ha resultado ser "la sangre del sector privado"[107]; cuando la justicia social y el beneficio comunitario se ponderen por encima del beneficio individual.

Más allá de mirar esto como una utopía, aprendamos de las iniciativas de jóvenes activistas de la cultura libre, tanto en nuestro país, como en otras partes del mundo. Por ejemplo: Aaron Swartz, quién cuestionó el abuso detrás de los grandes repositorios privados, como JSTOR, y quien se suicidó en 2013 después de múltiples presiones políticas debido a acusaciones legales

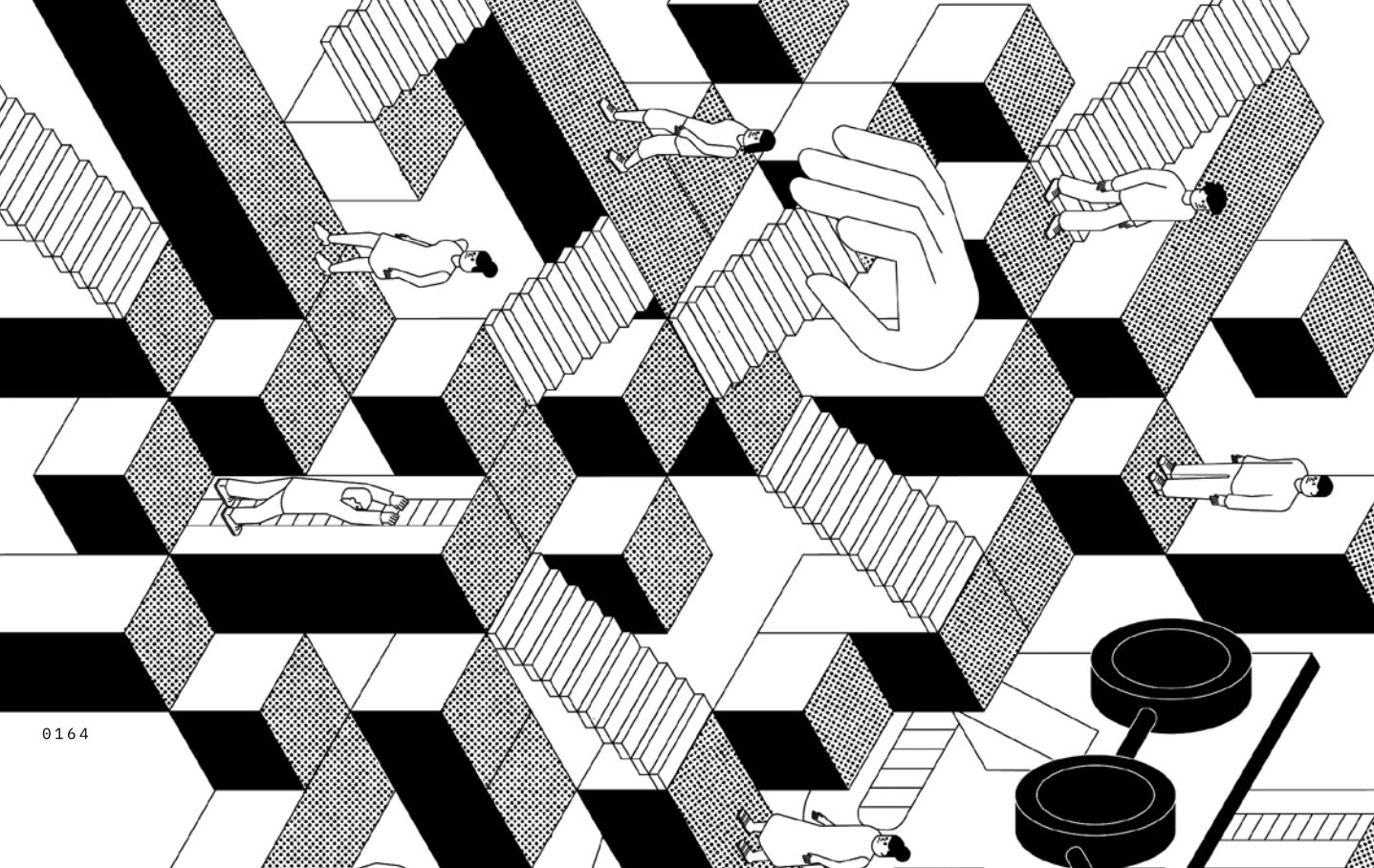
[107] Según palabras de Albert Bourla, director ejecutivo de Pfizer.

en su contra en Estados Unidos; o Alexandra Elbakyan, desarrolladora del portal más grande para acceder a artículos académicos de forma libre y gratuita, Sci-Hub, y que le ha costado diversas demandas millonarias de repositorios privados como Elvieser, lo cual le impide entrar en territorio estadounidense.

En el caso de México, han existido múltiples iniciativas y movimientos ciberactivistas en los últimos años que, desde diversas trincheras, defienden, promueven y generan puentes de comunicación entre sociedad civil, sector educativo, Estado y empresas, para que la actitud copyleft y la cultura libre dejen de verse como una práctica ilegal, y se entiendan como una práctica legítima de acceso al conocimiento. Algunas de estas personas son queridas, cercanas y hemos estado en la lucha por el conocimiento abierto desde hace algunos años, algunas de ellas —y seguramente olvidaré mencionar a muchas— son: Iván Martínez, Carmen Alcázar, Salvador Alcántar Morán, José Serralde, Gunnar Wolf, Sursiendo (jes y dom), La Pirateca, MIAU, Wikimedia México y toda su comunidad, Luis Álvarez, Red en Defensa de los Derechos Digitales y todo su equipo, la comunidad de EDUSOL, Creative Commons México, algunas comunidades de Software Libre en México y todas las personas que hicieron parte de diversas campañas mediáticas en redes sociodigitales en los últimos años, como #InternetNecesario, #NiCensuraNiCandados, #Salvemo-

sInternet, #NoAlaLeySopa y un largo, pero muy largo, etcétera.

Seguramente, existen muchas otras experiencias en favor de la cultura libre que no conocemos; personas que, desde sus trincheras y su ejercicio cotidiano, dentro y fuera de sus instituciones, accionan desde procesos que no han sido "tuiteados" o que no han recibido los reflectores. Todas ellas, las mediáticas y las que no tuvieron una debida difusión, representan golpes que erosionan y fisuran los viejos paradigmas, y poco a poco dan luz a una nueva forma de construir el conocimiento. Una nueva forma donde no sólo será necesario "leer las leyes" —muchas de ellas injustas— sino forjar, sentir y pensar "más allá de la ley" y con ello, dar forma a nuevos y mejores mundos posibles.



Tecnosolucionismo: obstrucción en el acceso a la justicia

ALEXANDRA ARGÜELLES

Alex Argüelles es tecnóloga, licenciada en comunicación, integrante de Ciberseguras y fundadora del Laboratorio de resiliencia digital comun.al. Desde 2013 colabora en iniciativas sobre derechos humanos y tecnologías en América Latina; realizando procesos de incidencia y análisis con énfasis en privacidad, género, accesibilidad e inclusión. Facilita talleres y provee acompañamiento en seguridad digital a periodistas, comunicadoras y activistas en la región desde un enfoque psicosocial, con aproximaciones para la justicia transformativa. Actualmente forma parte del programa de Tecnología y Sociedad de la Fundación Mozilla, abordando la violencia sociopolítica ejercida a través de las tecnologías en México.

CUANDO ENFRENTAMOS VIOLENCIA digital, lo primero que suele venir a la mente es qué hay que hacer para restablecer la seguridad de nuestros dispositivos o cuentas. Queremos recuperar el control de nuestra información e incluso identificar el origen del ataque o la violencia que estamos recibiendo. Una vez que tenemos algunas ideas sobre cómo accionar a partir de esto, buscamos mecanismos de reporte o denuncia, buscamos el acceso a la justicia frente las agresiones que vivimos, pero ¿qué significa justicia y cómo podemos acceder a ella?, ¿en qué términos —o los términos de quién— se define el acceso a la justicia?

La justicia tiene varios significados. Podemos pensarla como un bien común, como una condición indispensable para el desarrollo de las personas, como el conjunto de criterios que establecen los límites en las relaciones donde participamos (como individuos, como integrantes de la sociedad, como sujetos políticos, etcétera), a fin de que en estas relaciones diversas se respeten los derechos humanos y se establezcan condiciones que nos permitan ejercerlos de la manera más amplia posible. De acuerdo con las apuestas políticas de la justicia transformativa, podemos pensar la justicia como una respuesta a la violencia, al daño y al abuso que busca la restauración, la sanación y la transformación tanto de las personas involucradas como de sus entornos para prevenir la propagación de las violencias procurando la corresponsabilidad y la

resiliencia comunitarias. En teoría, el Estado —también en México— tiene entre sus funciones procurar la justicia por la autoridad que posee sobre su territorio y quienes lo habitan.

Volviendo al ejemplo de violencia digital, es interesante ver cómo en los últimos diez años se ha ido desarrollando un discurso incongruente en torno a las formas en las que el Estado provee respuestas o "justicia" a las situaciones en las que existen violencias propagadas a través de tecnologías, mientras refuerza el uso de tecnologías como una forma de consolidar las capacidades de control para mejorar la "seguridad" que nos ofrece. Entrecomillo justicia y seguridad porque estos conceptos han sido tan reducidos, desde la argumentación de los sesgos de quienes nos gobiernan, que terminan convirtiéndose en evidencia de la falta de habilidades para entender y atender la complejidad que los caracteriza.

En respuesta a la violencia digital, particularmente la violencia de género, se han creado dependencias especializadas en "ciberdelitos" e incluso se han incorporado reformas a leyes para amplificar los tipos penales que existen, a fin de que se contemplen algunas manifestaciones de las violencias que ocurren a través de las tecnologías. Como en muchos otros frentes en los que se defiende la dignidad en la búsqueda de justicia, la lucha por el reconocimiento de los efectos de las violencias digitales fue llevada por personas que anteriormente habían sido victimizadas por esas violencias y quienes fueron revictimiza-

das por el Estado, negándoles el acceso a la justicia: escudándose en la negligente carencia de perspectiva de género y la falta de herramientas necesarias para ser consecuentes con sus responsabilidades que —así como las violencias— también se trasladan a los entornos digitales. La toma de conciencia y el desarrollo de medidas para responder a la violencia de género que se manifiesta a través de las tecnologías en México es un logro de las personas que se organizaron para desarrollar y compartir habilidades con otras que estaban atravesando situaciones similares, como ha sido el caso de la activista Ana Baquedano; pero también es un logro de las personas que convocaron a otras por sus habilidades legales y comunitarias para incidir en el desarrollo de reformas legales promoviendo el reconocimiento de la gravedad de estas violencias, como fue el caso del Frente Nacional para la Sororidad y las Defensoras Digitales en sus diversos capítulos a lo largo del país.

Por otro lado, está la mirada más "industrial" de todo esto. En este campo no se habla tanto de violencia digital, sino más bien de "cibercrimen" o "ciberdelito". Y a lo que se refieren como cibercrimen puede ir desde la suplantación de identidad para realizar fraudes bancarios, hasta las presuntas violaciones a derechos de autor que, como hemos visto en varios casos, más allá de proteger los intereses de las personas creadoras o las industrias de propiedad intelectual, han sido usadas como un mecanismo ágil para la

censura y remoción de contenidos por parte del Estado. Aquí es donde los intereses del Estado y las diversas industrias que han incorporado las tecnologías digitales en sus entornos muchas veces coinciden, pero también entran en desacuerdo con el interés público y muchas veces terminan obstruyendo el ejercicio de los derechos humanos.

En ambos casos, cuando hablamos de violencia digital y cuando se habla de "cibercrimen", vemos cómo se han desarrollado respuestas para atender los daños que se contemplan en las normativas vigentes, sin embargo, cuando observamos el tratamiento que se da a los intereses de la sociedad civil frente a los intereses de las industrias o el Estado la diferencia es clara. El reconocimiento de la violencia digital y sus efectos ha sido parte de una lucha constante de la sociedad civil organizada (liderada por mujeres cis y trans e integrantes de la comunidad LGBTIQ+), que en ese reconocimiento de la gravedad que tiene la violencia digital —como continuación de la violencia machista, misógina, sexista que vivimos diariamente en los entornos físicos— ha exigido el acceso a la justicia que por muchos años fue negada. Sus matices, además, también se extienden a cuestiones en las que la libertad de expresión y la violencia contra periodistas, activistas y personas defensoras de derechos humanos en el país se intersecan con las brechas de desigualdad y el acceso a la información, la educación, la salud o la cultura; mientras

que el "cibercrimen" o los "ciberdelitos" han servido para retomar conversaciones en torno a medidas de persecución, intervención de dispositivos y vigilancia masiva, que consolidan las capacidades de control por parte del Estado bajo el pretexto de que en el uso de tecnologías cada vez más abusivas está la clave para protegernos de potenciales cibercriminales o ciberdelincuentes. Sobre este discurso, se ha señalado anteriormente que un Estado que presume que todas las personas que gobierna son potenciales delincuentes es un Estado que busca instaurar la criminalización como forma de gobierno, omitiendo la presunción de inocencia, apostando a la vigilancia y al castigo para controlar a quienes viven como sospechosas perpetuas, sin respuestas que transformen las situaciones de desigualdad, aborden los diversos contextos en su complejidad ni brinden acceso a la justicia.

El prefijo ciber, en el último caso, permite una nueva categoría de eufemismos que el Estado y sus representantes —en las distintas ramas del gobierno— han sabido instrumentalizar para vigilar, castigar, perseguir y criminalizar con herramientas tan potentes como sofisticadas... Monopolizando la "violencia legítima", también a través de las tecnologías. Estos eufemismos reclaman un poder especial cuando vemos cómo han sido utilizados en los discursos que han promovido estrategias de seguridad por parte del Estado que vienen acompañadas de la implementación de tecnologías que afectan directa-

mente derechos fundamentales, como el derecho a la privacidad o hasta la libertad de expresión y el acceso a la información.

Los despliegues de estas tecnologías, su instrumentalización con fines abusivos para la consolidación del poder y el desarrollo de legislaciones que se inclinan hacia el desarrollo de políticas públicas que centran su eficiencia en el uso de tecnologías son algunos ejemplos de cómo se manifiesta el tecnosolucionismo: una forma hipersesgada de abordar los problemas complejos, a fin de demostrar una correlación simplificada entre la implementación de algunas tecnologías y los efectos deseados para manejar situaciones que hasta ahora no han logrado ser resueltas por parte del Estado.

Podemos encontrar un ejemplo claro de esta ambivalente aproximación a la justicia en relación con las tecnologías en la consolidación del acceso a internet como derecho constitucional en México durante el 2013. El reconocimiento de este derecho tiene que ver con las posibilidades que brinda internet para amplificar el ejercicio de otros derechos, como son: el acceso a la información y la libertad de expresión, que, a su vez, son fundamentales para el desarrollo individual y social necesarios para que la democracia pueda manifestarse y ejercerse de forma plena.

Sin embargo, la misma reforma que llevó a que se estableciera este derecho en nuestro país venía con una serie de leyes secundarias en las que se establecían posibilidades que por un lado be-

neficiaban a los monopolios de telecomunicaciones, a través de la autorización del menoscabo de la neutralidad de la red —un principio fundamental para el acceso libre a la información sin discriminación por su origen, plataforma o formato en el flujo de internet— para beneficiar los intereses del mercado; mientras que por el otro, ofrecían vías para legitimar abusos de poder a través de las tecnologías por parte del Estado, como el bloqueo de servicios de telecomunicaciones o el seguimiento de la actividades digitales a través de tecnologías de geolocalización: en tiempo real y sin necesidad de aprobación judicial previa.

En abril de 2014 varias personas salimos a tomar las calles para manifestarnos en contra de estas leyes secundarias, exigiendo que se respetara la neutralidad de la red y nuestro derecho a la privacidad como garantías para el ejercicio de la libertad de expresión y el derecho de acceso a la información. En julio de ese año, se promulgó una nueva reforma a la Ley Federal de Telecomunicaciones y Radiodifusión que en su Artículo 145 establece que el Instituto Federal de Telecomunicaciones (un órgano constitucional autónomo creado un año antes para regular y supervisar tanto las redes como los servicios de telecomunicaciones y radiodifusión en el país) debía expedir una serie de lineamientos para asegurar la neutralidad de la red conforme a los principios de: libre elección, no discriminación, privacidad, transparencia e información, gestión

de tráfico, calidad y desarrollo sostenido de infraestructura. El Artículo 146 de esta ley también determina que: "Los concesionarios y los autorizados deberán prestar el servicio de acceso a internet respetando la capacidad, velocidad y calidad contratada por el usuario, con independencia del contenido, origen, destino, terminal o aplicación, así como de los servicios que se provean a través de internet, en cumplimiento con lo señalado en el artículo anterior".

Para enero de 2019, el IFT seguía sin expedir los lineamientos que permitirían salvaguardar la neutralidad de la red y los derechos que han sido afectados por la falta de mecanismos para resguardar la privacidad, el acceso a la información y la libertad de expresión. Frente a esto la Red en Defensa de los Derechos Digitales presentó un amparo para exigir al IFT el cumplimiento de su obligación de expedir estos lineamientos. Esta demanda de amparo favoreció a la sociedad civil y obligó al IFT a presentar los lineamientos pendientes a más tardar durante el segundo trimestre del año 2021. En diciembre de 2019 el IFT puso a consulta pública el anteproyecto de lineamientos para la gestión de tráfico y administración de la red, que según lo establecido por el mismo IFT tiene por objetivos:

i) Garantizar que el usuario final tenga libertad de decisión sobre los contenidos, aplicaciones y servicios a los que accederá, así como conocimiento de la

forma en que se gestiona su tráfico en la red.

ii) Otorgar certidumbre jurídica a la industria en materia de neutralidad de red, dando claridad sobre las políticas de gestión de tráfico y administración de red viables, así como respecto de las prácticas comerciales admisibles.

iii) Fomentar la innovación del sector mediante el uso de tecnologías más eficientes en el uso de las redes y en nuevas estrategias comerciales.

iv) Favorecer la disminución de la brecha digital, a través de ofertas comerciales alineadas con las políticas de gestión de tráfico y administración de red autorizadas por el instituto, con objetivos específicos.

v) Promover condiciones de competencia.

vi) Incentivar la inversión en redes para la provisión de internet fijo y móvil con mayor calidad y más cobertura.

Aunque a primera vista es claro que estos lineamientos comparten una visión afín a los intereses de la industria de telecomunicaciones y el desarrollo de esta, el documento en el que se presentaban estos lineamientos contaba una versión distinta a los objetivos mencionados anteriormente. El anteproyecto mostraba lineamientos que otorgaban al Estado la facultad de remover contenidos, aplicaciones y servicios de

internet, también permitía el monitoreo del tráfico de internet a través de la inspección profunda de paquetes, permitía la priorización pagada de contenidos en beneficio de los socios comerciales de las empresas proveedoras de acceso a internet (interfiriendo directamente con el acceso a la información e incluso afectando las posibilidades de competencia justa para productores de contenidos y servicios independientes, en completa incongruencia con la neutralidad de la red) y, además, omitía los contrapesos necesarios para asegurar la protección de la neutralidad de la red.

En respuesta a estos lineamientos que buscan favorecer los intereses de la industria menoscabando nuestros derechos, a través de la campaña #SalvemosInternet[108] se logró convocar a más de 150 mil personas en todo el país para que se sumaran a la participación en la consulta pública manifestando las preocupaciones que prevalecen desde 2014; ya que tanto en los objetivos del anteproyecto como en el documento que describe la propuesta de lineamientos se hace patente que el interés principal para el desarrollo de esta propuesta no era la defensa de la neutralidad de la red ni de nuestros derechos digitales, sino la búsqueda por privilegiar los inte-

[108] Argüelles, A. (2020). "#SalvemosInternet para proteger nuestra democracia". *Derechos Digitales*. Disponible en https://www.mnemozine.xyz/blog/salvemosinternet-para-proteger-nuestra-democracia

reses de las empresas y consolidar mecanismos de vigilancia y control para el Estado. Precisamente los mismos motivos por los cuales tomamos las calles hace siete años.

El reconocimiento del acceso a internet parece una victoria absoluta en la consolidación de los derechos humanos que se amplifican a través de las tecnologías —lo que solemos llamar derechos digitales—, pero también en este logro vemos cómo los intereses de los actores preponderantes —en este caso las empresas y el gobierno— entran en tensión con la amplificación de nuestros derechos. Para evitar perder el poder consolidado, vemos cómo estos actores preponderantes terminan desarrollando medidas opacas muchas veces ilegibles para quienes no manejamos lenguajes altamente técnicos o jurídicos, e incluso surge el desarrollo a puerta cerrada de políticas pública que son aprobadas rápidamente —sin consulta pública previa— para menguar nuestros derechos. Estas tensiones políticas entre los intereses de la sociedad civil y los intereses de las empresas o industrias —que muchas veces también participan en intercambios comerciales con el gobierno, dando pie a lucrativos negocios y corruptelas que lamentablemente no son novedad en nuestro contexto—, devienen en prácticas desleales en las que se restringe, o activamente se ignora, la participación de la sociedad civil en la toma de decisiones que terminan dando forma al "conjunto de criterios que establecen los límites de las relaciones

en las que participamos" que a su vez constituye el sistema de "justicia" que nos gobierna.

Si bien el acceso a internet y el acceso a las tecnologías —particularmente las tecnologías de información y comunicación o TIC— podrían ser clave para la amplificación del ejercicio de derechos, es claro que si sus implementaciones no ponen al centro el bienestar y la dignidad de las personas, estas tecnologías —y las políticas públicas que promueven su uso— terminarán siendo instrumentalizadas para consolidar el poder o perpetuar abusos que podrían disfrazarse bajo un discurso de progreso e innovación, a costa de los derechos de todas las personas, pero poniendo en riesgo especial a quienes han sido históricamente vulneradas y excluidas de estos "avances" por cuestiones de género, lengua, nivel socioeconómico u origen étnico. Un ejemplo claro de esto se puede contemplar actualmente, ante la profundización de la brecha educativa a raíz de las medidas de confinamiento que surgieron por la pandemia de COVID-19 y que llevaron a que la Secretaría de Educación Pública (SEP) apostara a trasladar la oferta educativa presencial a programas digitales.

Estudiantes de la Normal Rural de Mactumactzá, en Chiapas, vivieron y denunciaron las consecuencias de esta medida que, en su dependencia tecnológica, les excluyó del sistema educativo[109]. El 18 de mayo de 2021 se congre-

[109] _____. (2021). "Mactumactzá: derecho a la

garon en Chiapa de Corzo para exigir que se respetara su derecho a la educación y les permitieran acceder a la posibilidad de presentar el examen de ingreso al ciclo escolar de forma presencial, con cuadernillos de papel y pluma, en lugar de la vía digital; ya que a pesar de que el acceso a internet es un derecho en México, de acuerdo a la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares* (ENDUTIH) 2020 únicamente el 50.4% de las áreas rurales están conectadas a internet. Tanto la Normal Rural de Mactumactzá como sus estudiantes conforman la otra mitad de la población que sin acceso a internet no pudo beneficiarse de los programas tecnosolucionistas que implementó la SEP —a los que, además de lo que implica el costo de conectividad, habría que sumar la posibilidad de conseguir algún dispositivo funcional y accesible para aprovechar el acceso a internet.

Ese mismo día, en respuesta a sus demandas expresadas a través de la legítima protesta, el Estado desplegó a la policía militarizada para llevar a cabo la detención arbitraria de 95 estudiantes de comunidades rurales e indígenas, 74 estudiantes fueron liberadas el 24 de mayo, denunciando abuso de autoridad, uso excesivo

---

educación, acceso a internet y violencia estatal". *Animal político*. Disponible en https://www.animalpolitico.com/blog-invitado/mactumactza-derecho-a-la-educacion-acceso-a-internet-y-violencia-estatal/

de la fuerza y violencia sexual. Sus familiares, así como familiares de los estudiantes que seguían detenidos, continuaron recibiendo violencia por parte del Estado —resultando en lesiones y quemaduras de gas también en menores de edad y adultos mayores— hasta los primeros días de junio, cuando fueron liberados.

A la fecha no hay información disponible sobre las medidas de reparación ni el acceso a la justicia que ofrecerá el Estado a través del gobierno local para resarcir los daños y asegurar los derechos de alrededor 480 jóvenes que asisten a la Normal Rural de Mactumactzá y que, de acuerdo con el antropólogo y activista Abel Barrera Hernández, en su mayoría pertenecen a los pueblos Tzeltal, Tzolzil, Tojolabal, Zoque, Chol y Mam. En respuesta a las demandas del 18 de mayo, se anunció que el examen se llevará a cabo de manera presencial el 9 de junio a través de dispositivos conectados a internet que el gobierno local pondrá a disposición, imponiendo el uso de estas tecnologías —frente a la demanda específica del uso de cuadernillos y plumas— bajo el pretexto de las medidas sanitarias.

Aunque podríamos asumir que la intención de la Secretaría de Educación Pública era noble y a grandes rasgos práctica, es simplemente inaceptable que una Secretaría del Estado promueva medidas tan sesgadas y simplistas, sin el mínimo reparo en cómo estas podrían amplificar o agravar las brechas de acceso a derechos de las personas que enfrentan condiciones distin-

tas a las que podríamos asumir que están presentes en las grandes áreas urbanas del país. Sin embargo, este fenómeno que pretende usar las tecnologías como soluciones únicas y definitivas no se ha limitado al sector educativo, sino que ha propagado otros sectores como el cultural, el laboral, el económico, la salud y el ámbito de la seguridad pública.

Pensar las tecnologías de esa forma tan arbitraria demuestra el desconocimiento que existe sobre ellas y nos condena a vivir en una sociedad a la que se le niega la participación informada —y el consentimiento— respecto de las tecnologías que están siendo usadas para dar forma al futuro que habitaremos. Las tecnologías no son soluciones, las tecnologías son herramientas que pueden ayudarnos a encontrar las soluciones multidisciplinarias y flexibles que ameritan los problemas complejos en los contextos diversos que vivimos; sin embargo, si las tecnologías se implementan de forma sesgada y totalitaria —sin espacio a discusión, diálogo e incluso sin periodos de prueba— probablemente existan otros intereses para los cuales las tecnologías se vuelven instrumentos indispensables, como se ha visto en la consolidación de capacidades de control y vigilancia que se han extendido en los últimos años a lo largo de América Latina.

Además, las tecnologías vienen envueltas en sus propias complejidades, no están libres de conflicto y definitivamente no son neutrales. Cabe cuestionarnos quiénes desarrollan los dis-

positivos y plataformas que usamos, quién está detrás de los acuerdos comerciales que establecen el uso de un servicio sobre otro o incluso cuáles son las opciones de accesibilidad que existen para que estas tecnologías no únicamente lleguen, sino que puedan ser aprovechadas por personas con discapacidad o que únicamente hablan lenguas indígenas. Volviendo al caso de Mactumactzá, necesitamos conocer las necesidades de infraestructura que requieren las tecnologías para operar, así como también entender los impactos que estos despliegues tienen para nuestros entornos, tanto en el consumo de recursos naturales como en el medio ambiente. Por poner un par de ejemplos, pensemos en el impacto ambiental que tienen las granjas de servidores o los desechos digitales.

Algo que se suma a la gravedad respecto a la implementación de medidas tecnosolucionistas, particularmente las que se despliegan bajo el discurso de la supuesta "seguridad", tiene que ver con las obstrucciones que estas representan para los mecanismos de transparencia y rendición de cuentas. Antes de ir hacia las tecnologías más recientes y sofisticadas, en el ejercicio de preservación de la memoria, me gustaría recordar el caso del sitio 1DMX. En diciembre de 2012, tras la toma de poder de Enrique Peña Nieto, las agresiones físicas y detenciones arbitrarias de periodistas y personas que participaron en distintas protestas alrededor del país fueron ampliamente documentadas

por esfuerzos independientes que buscaban generar contrapesos a los cercos mediáticos establecidos por los medios de comunicación, que muchas veces terminaban cediendo a las presiones gubernamentales para presentar información sesgada o simplemente negar la cobertura a hechos en los que las violencias por parte del Estado y las violaciones graves a los derechos humanos eran evidentes. Así el 1dmx.org se convirtió en un repositorio abierto de evidencias de los abusos que habían surgido y de los cuales el gobierno en turno negaba rotundamente su existencia.

A un año de la creación del sitio, este fue dado de baja a través de la colaboración entre el gobierno de México y el gobierno de Estados Unidos. Poco después de que se inició un juicio de amparo que obligaba a la Secretaría de Gobernación y a la Comisión Nacional de Seguridad a brindar información sobre su participación en la remoción del sitio, estas instancias se negaron a cooperar en la investigación. Cabe mencionar que el comisionado a cargo de la Comisión Nacional de Seguridad, en aquel entonces, era también el responsable de los operativos que reprimieron tanto la protesta como las coberturas del 1 de diciembre de 2012. Tiempo después, GoDaddy —la empresa que alojaba el sitio— dijo que la solicitud de remoción había surgido del Centro Especializado en Respuesta Tecnológica (CERT), una dependencia de la Policía Federal de la Comisión Nacional de Seguridad.

Aunque probablemente este sea uno de los primeros casos mediáticos sobre la censura en internet habilitada por el Estado mexicano, definitivamente no cesaron ahí los intentos por consolidar otros mecanismos que surtieran estos efectos. Sin embargo, ahora los mecanismos de censura en internet se han ido sofisticando junto a los discursos con los que pretenden ser legitimados. Recientemente hemos visto cómo la censura ha avanzado a través de los acuerdos comerciales internacionales que incorporan medidas en beneficio de las industrias de propiedad intelectual y entretenimiento globales (como el Digital Millenium Copyright Act o DMCA), mientras menoscaban nuestros derechos; como se manifestó en la campaña #NiCensuraNiCandados[110], frente a las reformas que se hicieron a la Ley Federal del Derecho de Autor y el Código Penal Federal derivadas del Capítulo de Propiedad Intelectual del Tratado entre México, Estados Unidos y Canadá (TMEC). Por otro lado, incluso las "normas comunitarias" de las plataformas de redes sociodigitales más populares son usadas para remover contenidos afines a las protestas sociales, así como contenidos sobre salud sexual y reproductiva que permiten revertir los efectos

[110] _____. (2020). "¿Pero qué necesidad? Los derechos humanos NO son moneda de cambio". *Derechos Digitales*. Disponible en https://www.mnemozine.xyz/blog/2021/5/13/pero-qu-necesidad-los-derechos-humanos-no-son-moneda-de-cambio

de las políticas ultraconservadoras que nos han privado de esta información por generaciones.

Estas medidas, tan llenas de intermediación, dificultan que se pueda dar un seguimiento eficaz y claro que permita rastrear el origen de la censura; habilitando el abuso de estos mecanismos por la impunidad que permiten para quienes solicitan la remoción de contenidos a través de ellos, aun cuando los contenidos removidos sean de interés público. Esta instrumentación de las tecnologías, en un país con índices tan altos de violencia contra periodistas, activistas y personas defensoras de derechos humanos como México, constituye una mordaza para la libertad de expresión y un obstáculo para el acceso a la información que obstruye también el acceso a la justicia cuando se busca encontrar a quienes resultan responsables de esta censura digital.

Algo similar ocurre con los mecanismos de vigilancia e intervención de telecomunicaciones en nuestro país. Desde 2010, como refleja el resumen de vigilancia digital publicado por Sursiendo en 2019, han existido diversos casos donde las tecnologías se han usado para espiar a periodistas, activistas y personas defensoras de derechos humanos a través de la vulneración de su privacidad. Probablemente los casos que generaron más eco fueron los relacionados al informe #GobiernoEspía, publicado por la Red en Defensa de los Derechos Digitales (R3D) en 2017, en el que se evidencia la adquisición y el uso ilegal de herramientas de vigilancia por parte de las

autoridades mexicanas. Aunque frente a este caso se presentaron diversas medidas nacionales e internacionales para denunciar y condenar públicamente estas intervenciones abusivas, en años recientes hemos sabido de otros sistemas de vigilancia que han sido adquiridos por el Estado mexicano haciendo caso absolutamente omiso de las demandas que se han presentado por el uso abusivo e ilegal de estas tecnologías en años anteriores. En diciembre de 2020, a partir de una investigación realizada por Citizen Lab, se hizo de conocimiento público que México era el principal comprador de sistemas desarrollados para explotar vulnerabilidades en teléfonos celulares con el fin de acceder a llamadas, mensajes de texto y datos de localización. En abril de 2021, se reveló que la Fiscalía General de la República incumple con los controles judiciales al continuar adquiriendo servicios de geolocalización masiva e indiscriminada que ha utilizado desde 2018 sin haber solicitado autorización judicial. Estas actividades, constatadas por la Auditoría Superior de la Federación, se hicieron de conocimiento público a partir de un reportaje de Zorayda Gallegos publicado por *El País*[111]. Hasta

[111] Gallegos, Z. (2021). "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles". *El País*. Disponible en https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html

ahora, todas estas actividades ilegales que constituyen abusos de poder por parte del Estado y que violan directamente el derecho a la privacidad permanecen impunes o atrapadas en largos procesos de investigación que no han logrado brindar acceso a la justicia para quienes fueron víctimas de estas intervenciones.

En febrero de 2021, Madeleine Wattenbarger publicó un reportaje con el título "Donde funcionan las cámaras de vigilancia, pero la justicia no"[112] que —en un caso similar a lo que ocurre con los sistemas de espionaje digital— señala cómo en México, particularmente en la Ciudad de México, contamos con uno de los sistemas de videovigilancia más sofisticados del mundo que, a pesar de toda su potencia, no sirve para prevenir los delitos ni para procurar el acceso a la justicia. Los despliegues de cámaras de videovigilancia en el espacio público no son recientes, sin embargo, también se han ido sofisticando a pesar de que su uso se ha estado prohibiendo en varias ciudades alrededor del mundo porque al ser altamente invasivas estas tecnologías producen efectos inhibitorios en las personas, comprometiendo su libertad de tránsito y su privacidad. En Coahuila, un estado fronterizo al norte de México, en 2019, se inició la instalación de

[112] Wattenbarger, M. (2021). "Donde funcionan las cámaras de vigilancia pero la justicia no". *rest of world.* Disponible en https://restofworld.org/2021/donde-funcionan-las-camaras-de-vigilancia-pero-la-justicia-no/

cámaras de videovigilancia en el espacio público, que además poseen tecnologías de reconocimiento facial: tecnologías de vigilancia biométrica. En noviembre de 2020, una investigación publicada por Quinto Elemento Lab evidenció que incluso los protocolos internos establecidos por la fiscalía local para agregar imágenes a la base de datos de identificación habían sido descartados para responder a una petición de búsqueda realizada por el FBI, a fin de continuar la persecusión de dos estadounidenses que participaron en las protestas antirracistas tras el asesinato de George Floyd a manos de policías en Minneapolis. En México ni la persecución de activistas ni la siembra de evidencia para incriminarles son nuevas, tampoco lo es la colaboración con el gobierno estadounidense. Bajo la presunción de terrorismo, actualmente los sistemas de reconocimiento facial mexicanos participan en la persecusión de este par de activistas.

Las tecnologías de videovigilancia masiva en el espacio público, así como las tecnologías de vigilancia biométrica, también han sido denunciadas a nivel internacional por los efectos negativos que tienen sobre nuestros derechos, pero también porque han generado altas tasas de falsos positivos que criminalizan a personas que pertenecen a grupos que han sido históricamente vulnerados por cuestiones étnicas. A esta discriminación que se amplifica en los sesgos de estas tecnologías, se suma también la discriminación que se ha denunciado por parte

de integrantes de la comunidad trans, quienes terminan recibiendo revictimización por parte de estos sistemas que les niegan el reconocimiento de su identidad de género (aun cuando esta sea reconocida en documentos oficiales). A pesar de todo esto, a la fecha, los sistemas de videovigilancia y la vigilancia biométrica en el espacio público se siguen promoviendo por parte de las instancias tanto gubernamentales como encargadas de la seguridad nacional. De nuevo, descartando por completo las preocupaciones que desde la sociedad civil se han presentado respecto a la violencia que su uso representa para los derechos humanos y la falta de contrapesos o salvaguardas que efectivamente permitan que las personas estemos seguras, aun frente al uso de abusivo de estas tecnologías altamente invasivas y completamente inútiles —como expone el reportaje de Madeleine— para el acceso a la justicia.

La intención de consolidar bases de datos que nutran las tecnologías de identificación biométrica en nuestro país no termina ahí. En diciembre de 2020, la Cámara de Diputados aprobó la Ley General de Población que pretende garantizar el derecho a la identidad a través de una cédula de identidad digital que será operada y emitida por la Secretaría de Gobernación y, aunque no sustituirá otros documentos de identificación, servirá para consolidar otra base de datos altamente sensibles que estará en manos del Estado, pues esta cédula pretende incorporar datos

biométricos. Cuando hablamos de datos biométricos nos referimos a los marcos faciales, registros de iris, huellas digitales o hasta voz, pero también a cualquier dato sobre nuestro cuerpo que pueda ser recabado con el fin de hacernos identificables.

Algunas de las preocupaciones respecto a esta cédula tienen que ver con la falsa justicia que ofrece, ya que si bien se anuncia como una medida para "garantizar el derecho a la identidad", el uso de las tecnologías, por más sofisticadas o innovadoras que sean, no refleja realmente un compromiso por resolver la deuda pendiente que tiene el Estado con las poblaciones indígenas en el reconocimiento de su identidad e incluso —tomando de ejemplo lo ocurrido en la Normal Rural de Mactumactzá— resulta obvio deducir que esta medida podría amplificar las brechas relacionadas a la falta de rutas de acceso a la justicia o, en este caso, la falta de acceso al reconocimiento de la identidad por parte del Estado. Esto podría generar aún más obstrucciones para el reconocimiento de los derechos de estas poblaciones; pero también genera mucha desconfianza respecto a la consolidación de bases de datos tan sensibles como los datos biométricos, pues el gobierno mexicano ha demostrado en varias ocasiones no tener la capacidad para proteger bases de datos personales que han sido vulneradas, como han sido los casos del INAI en 2020 o el IMSS en 2021. En enero de 2021, Rodrigo Riquelme publicó desde *El Econo-*

mista[113] un resumen de las 12 vulneraciones a bases de datos más graves que se reportaron en 2020 por instituciones públicas y privadas en el país, que vale la pena tener en mente.

En un esfuerzo similar por consolidar bases de datos biométricos, que incluso podrían ser usadas para nutrir los algoritmos de identificación que permiten la operación de las cámaras de vigilancia con reconocimiento facial en el espacio público, en diciembre de 2020 se aprobó una iniciativa para crear el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) con la intención de que este registro pueda servir para reducir la extorsión telefónica en México. Esta iniciativa hace eco al RENAUT de 2011, registro que fue destruido un año después de su habilitación al demostrarse que no únicamente había resultado completamente inútil para reducir los índices de extorsión, sino que había permitido que se generaran casos de suplantación de identidad y desde su implementación la incidencia en extorsión había incrementado en más de 40% para el 2012. Si bien esta iniciativa nace, como muchas de las anteriores, como una respuesta para "mejorar la seguridad", en un contexto como el que enfrentamos ahora, ante una grave crisis económica tras la contingencia sanitaria por COVID-19,

[113] Riquelme, R. (2021). "2020, en 12 hackeos o incidentes de seguridad en México". *El Economista*. Disponible en https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

resulta completamente innecesario y desleal dirigir inversiones millonarias a este tipo de medidas que se ha demostrado que son inútiles.

La diferencia entre el PANAUT de 2020 y el RENAUT de 2011 es que el PANAUT busca sumar datos biométricos —aunque no ha quedado claro cuáles— a su registro. Algo que es muy importante mencionar aquí es que aunque esta medida se ofrece como una respuesta para mejorar la "seguridad", al no haber claridad sobre sus implicaciones tampoco existe la posibilidad de participar de manera informada, por lo que —de aprobarse esta medida— se nos negaría la posibilidad de otorgar o reservar el consentimiento sobre la captura de nuestros datos —también los biométricos— y además se contravendrían nuestros derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Lo anterior agrava el hecho de que en la participación coercitiva en este padrón también se supedita el derecho a la comunicación, ya que —en teoría— si no participamos en el PANAUT se nos restringiría la posibilidad de contratar una línea telefónica. Pensar que el crimen organizado no tiene formas para eludir estas medidas es completamente ingenuo e incluso necio frente a la evidencia que dejó la experiencia con el RENAUT, sin embargo, esto podría amplificar —nuevamente— las brechas que dificultan el acceso a las telecomunicaciones, obstruyendo tanto el ejercicio de derechos como el acceso a tecnologías que puedan servir como herramientas para avanzar en el acceso a la justicia.

Como fue el caso de las campañas #SalvemosInternet —o su antecesora #NoMásPoderAlPoder, en 2014— y #NiCensuraNiCandados, frente al PANAUT la sociedad civil se organizó en torno a la campaña #NoAlPadrón. Esta campaña además de generar información respecto a las implicaciones del padrón y generar conciencia en torno a los datos personas y la defensa de derechos digitales, también ofrecía rutas de participación política en las que, más allá de tomar las redes sociodigitales más populares para abrir espacios de diálogo sobre estos temas, se habilitó la posibilidad de generar demandas de amparo gratuitas a través de la plataforma https://noalpadron.mx. Este es un claro ejemplo de cómo las tecnologías pueden ser usadas incluso para fomentar el acceso a la justicia desde una perspectiva que incorpore la participación política diversa en la incidencia por la defensa de nuestros derechos.

Los ejemplos de las diferentes campañas, acciones e incluso las resistencias para generar incidencia en las políticas que afectan tanto positiva como negativamente el ejercicio de nuestros derechos a través de las tecnologías han sido fomentados a través del ejercicio de nuestros derechos digitales. Usamos las tecnologías como herramientas para compartir información, usamos las distintas plataformas para convocar y difundir recursos, nos comunicamos y generamos contrapesos a las narrativas hegemónicas para cuestionar los discursos que dicta el Estado.

Todas estas actividades que pasan por el acceso a la información, la libertad de expresión, el acceso a la cultura, el acceso a internet y, también, el derecho a la privacidad para resguardar nuestra identidad y proteger nuestros datos personales son formas en las que se manifiesta la construcción de la justicia que genera posibilidades de transformación frente a las brechas, desigualdades e imposiciones autoritarias que menoscaban nuestros derechos.

Para aprovechar las tecnologías como herramientas para el acceso a la justicia, volviendo a las preguntas con las que inicia este texto, es necesario conocer los alcances (y sesgos) que tienen y situarlas de forma que respondan a nuestras necesidades en un sentido amplio, que puedan abarcar la complejidad de nuestros contextos para evitar que las tecnologías se conviertan en barreras de discriminación. Para esto es importante romper con la engañosa noción de que las tecnologías son soluciones. Las soluciones fincadas en el compromiso social y el acceso a la justicia no pueden centrarse en la instrumentalización de herramientas, deben poner al centro la dignidad y el respeto a los derechos humanos para tejer, a partir de estas perspectivas, oportunidades creativas y locales, a fin de que se procuren entornos de innovación y desarrollo de tecnologías que respondan a nuestras necesidades específicas, sean accesibles y estén sujetas a mecanismos de transparencia —por parte de quienes las desarrollen y operen—, consenti-

miento y participación informada por parte de la población en general.

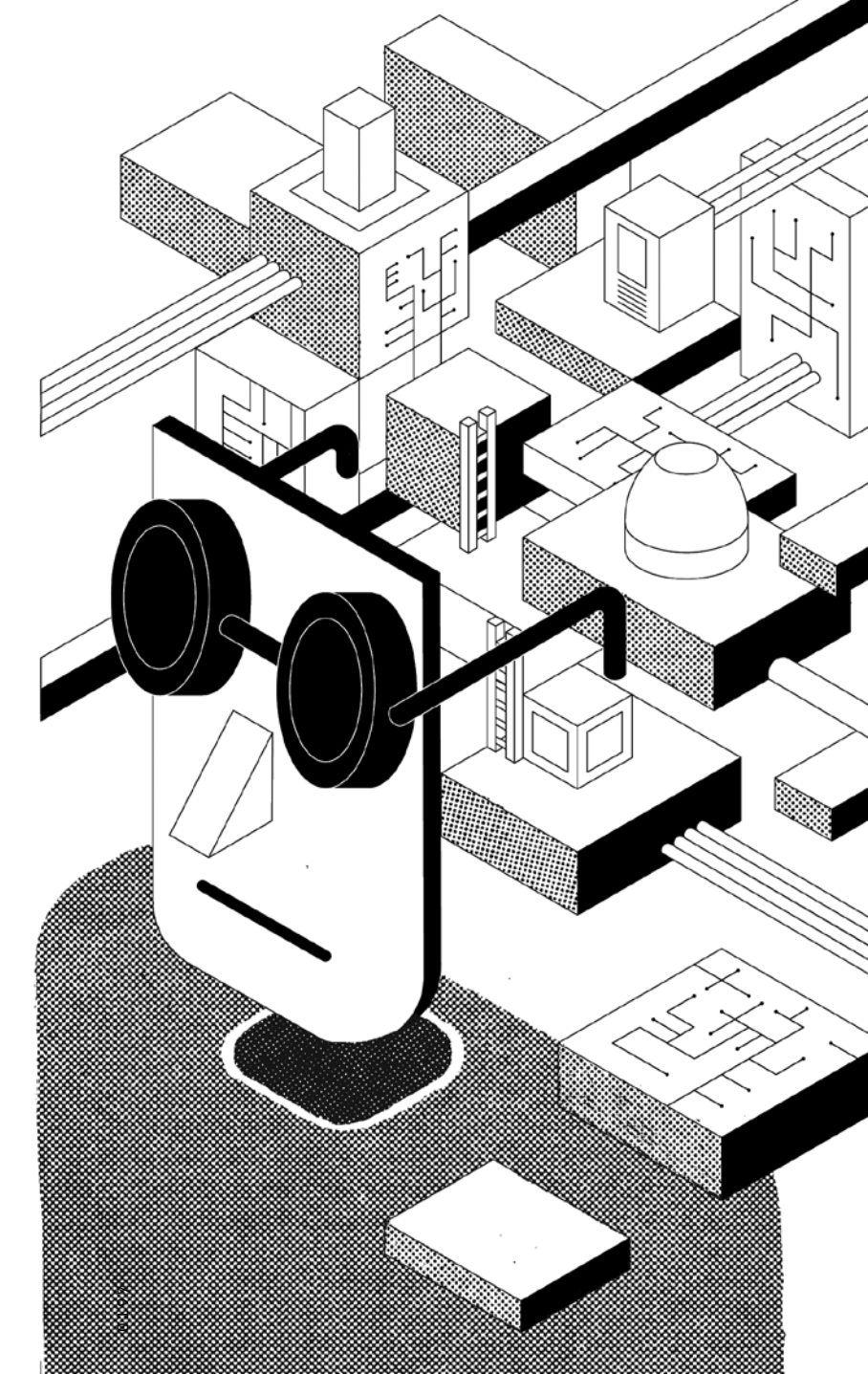
Parafraseando a Phi Requiem, consultor en seguridad digital para personas defensoras de derechos humanos: "Se usan tecnologías del futuro para resolver problemas del presente con legislaciones del pasado". El costo que estos sesgos tienen para el ejercicio de nuestros derechos se ve reflejado en la autonomía que poco a poco se nos ha ido menguando ante la implementación de despliegues de tecnologías que suelen reforzar las desigualdades y abusos de poder, abonando a la construcción de posibilidades que habiliten un futuro donde el autoritarismo podría encontrar una fuente inagotable de control en el uso de las tecnologías que actualmente se están desplegando en nuestro país bajo una falsa promesa de seguridad.

Si no podemos participar en la construcción de nuestro futuro, también se nos está negando el acceso a la justicia. Por esto es sumamente importante fomentar la participación, fomentar las posibilidades de incidencia para que, de manera informada y organizada, podamos romper la opacidad que rodea estos temas y evitemos que se sigan instaurando medidas tecnosolucionistas que nos tomará años revertir.

El terreno de lo político siempre está en disputa. No podemos permitir que esas disputas se sigan librando entre los mismos actores, entre los mismos poderes que se han consolidado a partir de la invisibilización y el silencio al que nos

relegan, los espacios que excluyen a la sociedad civil, con nuestras perspectivas múltiples y características diversas. Es importante informarnos, organizarnos e incidir para recuperar las posibilidades de construir el acceso a la justicia que queremos gozar en el futuro y que se nos ha negado en el presente.

Resguardemos la memoria, no olvidemos que las tecnologías son herramientas, no soluciones. Aprendamos sobre las que existen y están disponibles, desarrollemos tecnologías nuevas y hagámoslas accesibles. Rompamos las lógicas del progreso acelerado, detengámonos a imaginar e inventar los cimientos sobre los cuales queremos construir el futuro. Construyamos rutas accesibles para una justicia que transforme nuestro presente y nos permita acceder a futuros de posibilidades y no nos aten a un futuro distópico en el que tengamos que resignarnos a la impotencia y el miedo que instaura el autoritarismo que silencia el consenso y la participación. Aún estamos a tiempo de actuar, hagámoslo juntæs.



>> NO HAY JUSTICIA
SIN PARTICIPACIÓN
DIVERSA.

>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA
SIN CONSENTIMIENTO
INFORMADO.

>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA
SIN ACCESIBILIDAD.

>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA
SIN CONTRAPESOS
A LOS PODERES
PREPONDERANTES.

>> NO HAY JUSTICIA SIN TRANSPARENCIA.

>>>>>>>>>>>>>>>>>>

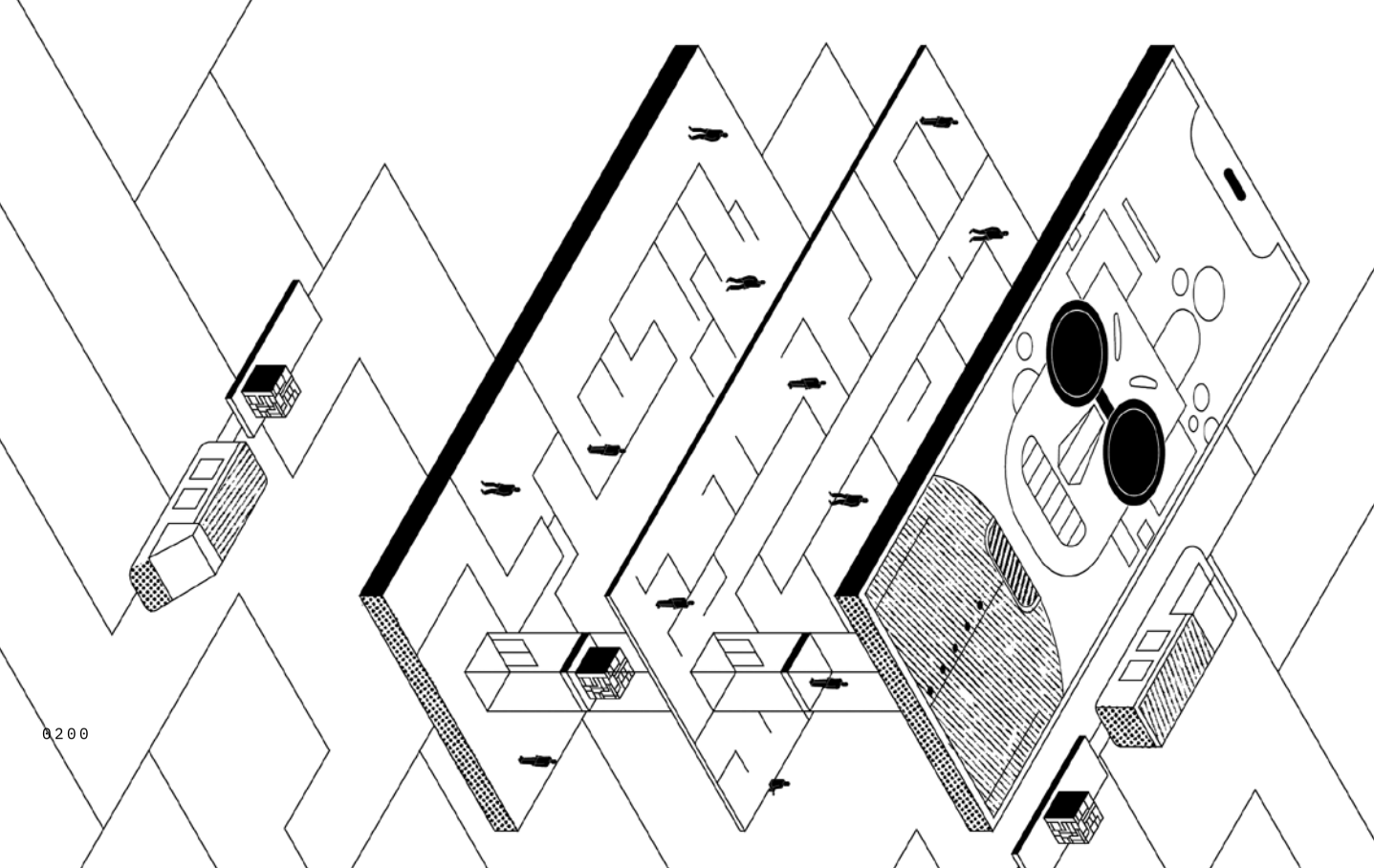
>> NO HAY JUSTICIA SIN RENDICIÓN DE CUENTAS.

>>>>>>>>>>>>>>>>>>

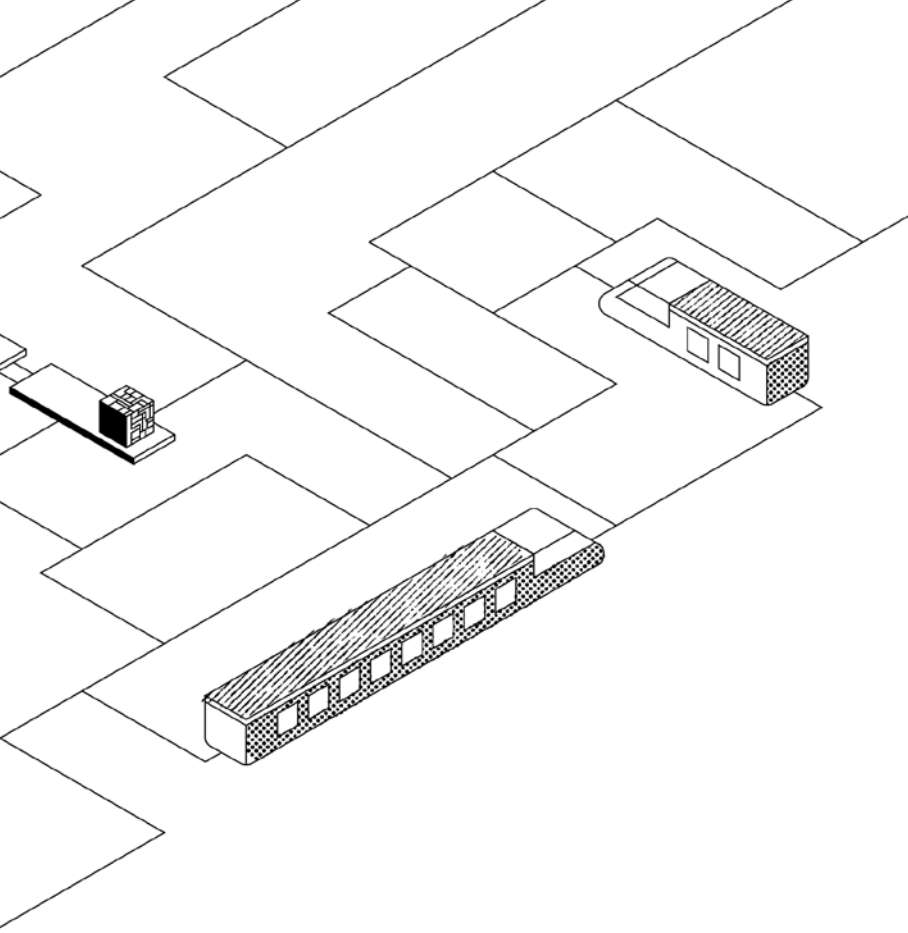
>> NO HAY JUSTICIA SIN MEMORIA.

>>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA SIN TRANSFORMACIÓN.



0200



[Este texto es un homenaje]

0202

Para más información sobre violencia digital en México, así como la versión digitalizada de este libro, eventos relacionados y recomendaciones actualizadas, visita nuestro sitio

- > **https://comun.al**

y ¡aprendamos juntæs!

ESTA EDICIÓN FUE IMPRESA EN LOS TALLERES DE XX, CIUDAD DE MÉXICO, EN EL MES DE OCTUBRE DE 2021. EL TIRO FUE DE 300 EJEMPLARES. LA EDICIÓN ESTUVO A CARGO DE GABRIELA ASTORGA, IVÁN CRUZ OSORIO, BENJAMÍN E. MORALES Y SANTIAGO SOLÍS.

DISEÑO: SANTIAGO SOLIÍS. CORRECIÓN DE ESTILO: ÓSCAR MUCIÑO

PARA SU COMPOSICIÓN TIPOGRÁFICA SE UTILIZARON LAS FUENTES: LORES 12 OT, DE ZUZANA LICKO E IBM PLEX DE MIKE ABBINK.

MÉXICO ES UN PAÍS MARCADO POR MÚLTIPLES DESIGUALDADES. Dichas desigualdades se traducen no sólo en una división entre quienes tienen y quienes no, sino también en el acceso a bienes y servicios, el pleno ejercicio de derechos básicos, el acceso a la justicia y, en última instancia, en diversas formas de violencia. En este contexto, las tecnologías se han convertido en un arma de doble filo: mientras funcionan como herramientas para garantizar derechos como la libertad de expresión, el acceso a la justicia y buscar caminos hacia la autonomía; son también aparatos de vigilancia, control y criminalización para quienes trabajan por una sociedad más justa. /////////////// Históricamente hemos desestimado la manera en la que el uso de las tecnologías afecta, tanto positiva como negativamente, la protección y garantía de los derechos humanos. Si bien ha contribuido a la amplificación de tareas de la sociedad civil organizada, también ha vulnerado la seguridad, privacidad e integridad de la ciudadanía, desde el acceso diferenciado a servicios y tecnologías hasta los abusos de poder cometidos por el Estado. /////////////// Las historias que conforman este libro son experiencias de resistencia y memorias compartidas sobre cómo la violencia digital y sociopolítica ha impactado a la sociedad civil organizada, pero también sobre los esfuerzos de resistencia, aprendizaje colectivo y creación de comunidades que siguen apostando y trabajando por un mundo más informado, más libre, más organizado, más justo. ///////////////

COMUN.AL
Laboratorio de resiliencia digital

10 MALPAÍS EDICIONES