revista Fronteiras – estudos midiáticos
20(3):378-389 setembro/dezembro 2018
Unisinos – doi: 10.4013/fem.2018.203.10

# Violencia de género expandida: vigilancia y privacidad en red

## Expanded gender violence: Surveillance and network privacy

Graciela Natansohn[1]
graciela71@gmail.com

Florencia Goldsman[1]
florcitag@gmail.com

**RESUMEN**
En este trabajo exponemos una reflexión que enlaza la violencia de género en entornos digitales, la vigilancia masiva, las discusiones sobre la privacidad y el derecho a la intimidad en internet. Analizamos cómo internet puede ser escenario de dos tipos de violencias: una, localizada en el plano de las interacciones (doxing, acoso, extorsión y amenazas, robo de identidad, alteración y publicación de fotos y videos sin consentimiento, entre otras). La otra, más invisible, está implícitaen la arquitectura de la red, pues al propiciar un sistemático y gigantesco sistema de rastreo y análisis de datos personales para alimentar el modelo de negocios de internet, se ha instaurado un potencial sistema de vigilancia que puede afectar los derechos de las mujeres, vía rastros digitales. Para sostener esto examinaremos las diversas nociones de vigilancia y privacidad (Bruno, 2013; Siri, 2015; Sparrow, 2014) y la legislación vigente, en función de comprender cómo afectan los derechos humanos de las mujeres en el ciberespacio.

**Palabras clave:** violencia de género, vigilancia y privacidad, internet.

**ABSTRACT**
In this paper, we present a reflection that links gender violence in digital environments, mass surveillance, discussions about privacy and the right to privacy on the internet. We analyze how the Internet can be the scene of two types of violence: one, located at the level of interactions (doxing, harassment, extortion and threats, identity theft, alteration and publication of photos and videos without consent, among others). The other, more invisible, is implicit in the architecture of the network, because, by promoting a systematic and gigantic system of tracking and analysis of personal data to feed the Internet business model, it has established a potential monitoring system that can affect the rights of women, via digital traces. To support this, we will examine the various notions of surveillance and privacy (Bruno, 2013; Siri, 2015; Sparrow, 2014) and current legislation in order to understand how they affect the human rights of women in cyberspace.

**Keyword:** gender violence, surveillance and privacy, Internet.

## Introducción

El objetivo de este trabajo es demostrar la relación entre la violencia de género en entornos digitales y el vigilantismo en internet - expresado en la recolección masiva de datos realizada por los gobiernos y corporaciones - que confronta el derecho a la privacidad y a la intimidad y vulnera aún más a grupos tradicionalmente vulnerables,

[1] Universidade Federal da Bahia. Rua Augusto Viana, s/n, Palácio da Reitoria, Canela, 40110-909, Salvador, BA, Brasil

como mujeres, LGBTI+ y grupos políticamente disidentes. Mostramos cómo internet puede ser escenario de dos tipos de violencias: una muy discutida, localizada en el plano de las interacciones, tal como el doxing[2], acoso, extorsión y amenazas, robo de identidad, publicación de fotos y videos sin consentimiento, entre otras. La otra, más invisible, está implícita en la arquitectura de la red pues al propiciar un sistemático y gigantesco sistema de rastreo y análisis de datos personales para alimentar el modelo de negocios de internet, se instaura un potencial sistema de vigilancia por parte del estado y de las corporaciones privadas que dominan los principales sitios de redes sociales, que puede afectar los derechos de las mujeres (cis o trans), vía rastros digitales.

El tema emergente del activismo feminista contra la violencia de género en Brasil ha sido el fenómeno del odio misógino ejercido mediante los dispositivos electrónicos con los que interactuamos - internet y dispositivos móviles conectados –, que colocan a las mujeres en una encrucijada: por un lado, se reclaman mayores puniciones a los *haters*, más leyes y más control sobre lo que sucede en internet. Por el otro, esos controles parecen caracterizarse más por restringir libertades – libertad de expresión, derecho al anonimato y protección de los datos personales – que por penalizar, efectivamente, a los criminales misóginos.

Primero, examinamos las diversas nociones de vigilancia y privacidad y analizamos el marco civil de internet en Brasil para comprender cómo son afectados los derechos humanos de las mujeres en el ciberespacio, tanto por las leyes como por la arquitectura contemporánea de internet.

Luego examinamos los tipos de violencias contra las mujeres en ambientes digitales y argumentamos que la expansión del uso del celular inteligente potencializa la vigilancia. Producto de la masificación del uso de internet vía smartphones (frente a la escasa extensión de banda larga para telefonía fija y datos, el celular es la única opción en muchos territorios del país) hay un mercado emergente de aplicaciones móviles en acelerado crecimiento, verdaderos "chupa-datos" asociados a las gigantes de internet (Google, Apple, Facebook, Amazon, Microsoft), cuyos términos y condiciones de uso exigen de los/as usuarios/as muchos más datos de lo estrictamente necesario para funcionar. En este mercado en franca expansión nos importa destacar las *apps* para *mobile* orientadas a las mujeres, que sirven para controlar sus ciclos vitales (menstruación, ovulación, etc.). Estos programas recogen datos íntimos en una escala nunca vista y no hacen público para qué esas informaciones pueden ser efectivamente utilizadas, y no dejan claro cuáles son sus posibles consecuencias sobre la salud individual y colectiva.

## Vigilancia como modelo de negocios y control político

Uno de los síntomas de nuestra época es el hecho de que estamos siendo observados todo el tiempo. En la actualidad el flujo de informaciones que circula en el ciberespacio resulta un núcleo privilegiado de monitoreo por parte de diferentes sectores y según diferentes propósitos, hacia toda la ciudadanía. Los fines son diferentes: comerciales, publicitarios, administrativos, por motivos de seguridad, afectivos, entre otros. Partiendo desde las diversas formas en que se manifiestan esas nuevas formas de la vigilancia vemos cómo las acciones y comunicaciones cotidianas en el ciberespacio se tornan cada vez más sujetas a colecta, registro, análisis y clasificación.

Por tal razón es necesario colocar de inmediato en el debate cuestiones sobre las implicaciones de estos dispositivos utilizados para la vigilancia, el control y la formación de saberes específicos. En especial aquellos que versan sobre deseos, inclinaciones, conductas y hábitos de individuos y de poblaciones. Es necesario discutir acerca de cómo, sobre las características de la corriente visible de los intercambios y las conversaciones sociales, se "constituye un inmenso, distribuido y polivalente sistema de rastreo y categorización de los datos personales que, a su vez, alimenta estrategias de publicidad, seguridad, desarrollo de servicios y aplicativos, dentro y fuera de estas plataformas", advierte Fernanda Bruno (2013, p. 9, traducción nuestra).

Podemos describir los principales aspectos de los procesos de vigilancia en las sociedades contemporáneas conformados a partir de elementos heterogéneos, constituyendo una red multifacetada, repleta de conflictos y ambigüedades. Bruno (2013) propone la noción de vigilancia distribuida como aporte para esta discusión, como una noción operatoria más que una definición acabada. Una vía de exploración, entendimiento y problematización que incluye una serie de tensiones en una red en la que

[2] Significa divulgación de datos personales como domicilio, revelación de datos financieros o teléfonos privados.

interactúan agentes humanos y no humanos. La vigilancia existe como una función potencial que está inscrita en el propio engranaje y arquitectura de esos dispositivos - en el caso de las redes digitales de comunicación como internet y muchas de sus plataformas. Estas, a su vez, contienen, en sus parámetros de funcionamiento regulares, sistemas de monitoreo de datos personales y control de flujos informacionales que responden a la lógica automatizada de programación que responde a través de protocolos. A su vez los sistemas de monitoreo son parte integrante de la eficiencia de esas plataformas, "que rastrean, archivan y analizan las informaciones disponibilizadas por los usuarios y comunidades de modo de optimizar sus servicios, tanto como las relaciones entre usuarios" (Bruno, 2013, p. 32, traducción nuestra). Como dice Sparrow (2014), cuando la comunicación es digital, la vigilancia se encuentra justo en su núcleo. En este contexto podemos clasificar, siguiendo a Sparrow, los principales agentes que ejercen acciones de vigilancia en el presente y que abarcan los ámbitos tantos públicos como privados con estrategias distintas, en dos tipos:

(a) Estrategia central de modelo de negocios: se manifiesta de diversas formas pero se relaciona con la recolección masiva de datos (minería de datos o *Big Data*) sin el consentimiento de usuarios/as, suscriptores/as a servicios como: apps, redes sociales, servicios de correo, servicios de repositorios de documentos en la "nube". En general se los denomina como "terceros implicados" (*third parties intermediaries*) y centran su estrategia de recolección a través del uso de *cookies* a través de las ventas en línea o del simple seguimiento de la navegación de cada usuario, rastreo de ISPs, respaldos de informaciones, servicios de telefonía, compañías de tarjetas de crédito y cualquier desarrollo de aplicaciones móviles.

(b) Estrategia central de seguridad de gobiernos a nivel global: afecta a todas/os los/as ciudadanas/os, pero en particular, a activistas, opositores/as y disidentes políticos.

A partir de la comprensión de que las tecnologías y plataformas que usamos cuentan por defecto con algoritmos de monitoreo de las informaciones y acciones de los individuos en el ciberespacio, queda claro su modelo de eficiencia (basta pensar en el modo de funcionamiento de cualquier motor de búsqueda). Sin embargo, afirmamos junto con Fernanda Bruno que el hecho de la vigilancia está presente como una posibilidad de la propia arquitectura de esos dispositivos no implica, con todo, que ella sea necesaria. Esto significa que el tener a la mano los datos de navegación, de uso de plataformas ("logueo") y hábitos de la vida virtual de la ciudadanía no debería implicar su sistematización, análisis y uso por fuera de nuestro conocimiento y consentimiento.

La vigilancia a la que nos estamos refiriendo tiene como misión permitirle a quien la ejerce, ya sea desde el ámbito público o desde el privado, la producción de conocimiento sobre los vigilados/as. Aquello que hoy se conoce como minería de datos puede ser formalizada de diversas formas (extracción de padrones, regularidades y cadenas causales, por ejemplo). La información cada vez más detallada de quiénes y cómo estamos conectadas/os construye perfiles minuciosos ("targets") de los usuarios/as, consumidores/as, ciudadanía (Zuazo, 2015).

Las actividades de vigilancia enfocadas en individuos o poblaciones humanas involucran, de modo general, tres elementos centrales: observación, conocimiento e intervención (Bruno, 2013). La observación puede ser efectuada de diferentes modos (visual, mecánico, electrónico, digital) e implica inspección ocular, sistemática y focalizada en individuos, poblaciones, informaciones o procesos comportamentales, corporales y físicos, sociales, entre otros.

Lúcia Santaella (2011) propone tres tipos de regímenes de vigilancia: panóptico, escópico y de rastreamento, aunque los tres operan simultáneamente. El panóptico es el que se realiza en espacios bien circunscritos y fue bien descripto por Michel Foucault en su clásico Vigilar y Castigar, de 1975. El escópico se expresa en la proliferación de cámaras de vigilancia por todos los ámbitos: calles, establecimientos comerciales, edificios y hasta en la intimidad de los domicilios. El de rastreo nace en el espacio digital. El trabajo de análisis que se precisa hacer del material captado por los sistemas panópticos y escópicos requiere procesos de observación, comparación y análisis, mientras que el tratamiento de los datos digitales por rastreo puede ser procesado prácticamente de forma instantánea. Control "ubicuo y pulverizado, de los medios móviles no hay, potencialmente, cómo esconderse. Los lugares son, más bien, puntos de un flujo continuo de vigilancia y cada uno de ellos está conectado con otro" (Santaella, 2011, p. 140, traducción nuestra).

Es preocupante, también, la manera en que la falta de transparencia que ofrecen las plataformas y dispositivos que usamos cada día, redunda en un intercambio de datos desigual que resulta en mayor control de cuerpos y

voluntades. En el medio de estos intercambios se efectúa la monetización de nuestras informaciones personales y el robustecimiento de unos algoritmos que tiempo después intentarán marcar nuestros hábitos de consumo y preferencias para vendernos productos, remedios o, directamente, un modo de vida.

Gran parte de nuestro comportamiento deja de por sí huellas digitales -inclusive de acciones tan inofensivas como viajar en taxi o andar por las calles. "Las cámaras que controlan el tránsito nos monitorean, o nuestros teléfonos celulares registran nuestros paraderos a cada momento del día y nosotros publicamos voluntariamente nuestras vidas privadas en plataformas públicas con propietarios privados" (Jansen, 2014, traducción nuestra).

Todas las comunicaciones digitales dejan rastro e involucran a terceros implicados (*third-party intermediaries*); entre ellos están los proveedores de correo, telefónicas, ISPs, empresas de tarjetas de crédito, ventas en línea, backups físicos o en la *nube* y casi todo desarrollo de apps móviles. "Las redes de los terceros implicados son capaces de rastrear la conducta de los usuarios de internet, incluso cuando los usuarios cambian de dispositivos, porque la mayoría de los sitios web y aplicaciones móviles usan uno o más de las mismas redes de publicidad y seguimiento" (Sparrow, 2014, p. 24, traducción nuestra). Hay que detenerse también, según el mismo autor, en el hecho de que aunque estas redes sean usadas con fines comerciales, las agencias gubernamentales también son capaces de rastrear esos datos y obtener una rica fuente para vigilancia enfocada en informaciones personales.

## ¿Y las leyes brasileras?

El panorama de las tecnologías digitales ha cambiado radicalmente en las últimas décadas. La vigilancia se ha vuelto una "industria comercial, que satisface el interés de los Estados por capacidades de vigilancia cada vez más expansivas. Se calcula que la industria de la vigilancia crece un 20 por ciento al año" (Privacy International, 2015, p. 7). Si bien es cierto que las tecnologías de la vigilancia en estos contextos también tienen como meta brindar protección frente a la amenaza de aumento de la criminalidad en línea, este tipo de desarrollos tecnológicos puede ser usado por los gobiernos para "hostigar a los detractores, reprimir la disidencia, intimidar a la población, disuadir de ejercer la libertad de expresión y destruir la posibilidad de tener vida privada" (Privacy International, 2015, p.7).

En junio de 2013 fue revelado un aparato de vigilancia y de espionaje en masa a partir de datos digitales a través de la filtración de copias de documentos de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos de América. La revelación realizada por el hoy perseguido político Edward Snowden (Anistia Internacional, 2015) señalaba que el programa PRISM permite a la NSA tener acceso directo a servidores de grandes empresas de internet, siendo así capaz de monitorear comportamientos de sus usuarios en escala global. Además, los documentos también detallaron el espionaje a dirigido hacia gobiernos de la diáspora estadounidense, siendo la alta cúpula del gobierno brasilero uno de sus principales focos de atención.

La ley llamada Marco Civil de Internet (Presidencia da República, 2014) fue, entonces, una reacción brasilera a la vigilancia en internet. Este documento que pasó por el Senado Federal el 22 de abril de 2014 y fue sancionado al día siguiente por la hoy depuesta presidenta Dilma Rousseff, lleva el número de ley federal 12.965/2014. "Fue el resultado de una amplia movilización de la sociedad civil buscando garantizar los derechos en y de internet – una movilización que resultó en un innovador movimiento de participación en el proceso de creación de leyes brasilero" (Alimonti, 2014, p. 83, traducción nuestra). Entre los pilares del Marco Civil, que es una ley que está a la vanguardia de los derechos digitales a nivel mundial, se encuentran respeto a la neutralidad, la libertad de expresión, la privacidad y la limitación de la responsabilidad de los intermediarios de contenidos como Google, Facebook o Microsoft para filtrar contenidos sin una intervención jurídica previa.

Así mismo, la protección de los datos personales y de la privacidad son, de manera separada, dos de los principios que la ley provee para regular el uso de internet en Brasil. Se marca un punto de inflexión acerca de la conservación de datos de usuarios/as. Vale resaltar que luego de las declaraciones de Snowden, se reforzaron las medidas relativas a la "inviolabilidad y el secreto del flujo de las comunicaciones en la internet y los datos conservados por privados, con la excepción de ser requeridos a través de una orden de la Corte" (Alimonti, 2014, p. 84, traducción nuestra). Este detalle es importante debido a las diferenciaciones que se deben hacer entre los datos como contenidos y los metadatos como huellas y rastros que deja nuestro paso por la internet. Otro de los puntos diferenciales se relaciona con informar a usuarios/as acerca de la recolección de los datos personales por parte de empresas o instituciones. La ley requiere consentimiento

expreso de parte del sujeto para la futura recolección, uso, conservación y manipulación de los datos personales, que debería ser entregada separadamente de otras cláusulas contractuales (Alimonti, 2014). En otras palabras: se trata de un acceso claro por parte de usuarios/as a la información sobre los procesos que podrían ser realizados con los datos propios, incluyendo la protección en los sistemas de acceso (*logins* y *data recording*) a aplicaciones, siendo estas últimas fundamentales pues son las de mayor uso, a partir de dispositivos móviles. Una cuestión tan sensible como la revelación de datos personales a terceros implicados solo puede ocurrir de existir consentimiento expreso, informado y libre, señala la misma autora.

Como consecuencia del artículo 7, el artículo 8 del Marco Civil declara la garantía del derecho a la privacidad y la libertad de expresión en las comunicaciones como un prerrequisito y ejercicio de acceso completo a internet. Al respecto, Veridiana Alimonti dice que

> *De manera de luchar contra la vigilancia reportada por Snowden, el Artículo 11 determina que la ley brasilera relacionada con privacidad debe ser respetada por quien brinda la conexión a internet y los proveedores de aplicaciones cuando colectan datos personales, loggeos y contenidos de las comunicaciones cuando esto ocurra o incluya una terminal localizada en Brasil (Alimonti, 2014, p. 84, traducción nuestra).*

En Brasil, proyectos de ley y agencias reguladoras de las telecomunicaciones vienen intentando instituir medidas que dañen el anonimato en internet. Estas medidas vienen siendo contestadas por sectores de la sociedad civil y de los propios gobiernos, pero aún están en disputa.

Vale destacar que en agosto de 2018 fue sancionada la Ley General de Protección de Datos Personales n.13.709/2018, que fue aprobada por unanimidad en el Congreso brasilero. La ley entrará en vigor en febrero de 2020, instituyendo un importante instrumento legal que podría ayudar a garantizar la privacidad y la protección de derechos fundamentales. Esa ley regula las posibilidades de tratamiento de los datos personales tanto por el poder público como por el sector privado. Según el texto, la ciudadanía podrá saber cómo las empresas públicas y privadas tratan los datos personales, cómo y por qué los recogen, como los guardan, por cuánto tiempo y con quiénes los comparten. Las empresas deberán explicar eso de forma clara, inteligible y simple. Sin embargo, el presidente Michel Temer vetó algunos artículos que colocan en juego la eficacia de esa norma. Los vetos se refieren a la creación de una autoridad nacional y un consejo políticamente independiente con capacidad de fiscalizar el cumplimiento de la ley y aplicar sanciones, entre otros temas. Esta ley es fruto de la larga lucha de entidades del tercer sector, organizaciones privadas y académicas que participaron activamente del proceso de negociación junto al poder legislativo y los vetos pueden significar un nuevo retroceso para los derechos digitales de los ciudadanos.

## Diagnóstico de la violencia de género en internet

Las diversas formas de vigilancia que existen en la actualidad parecen parte de un *continuum* tecno-político de vigilancias históricas sobre los cuerpos de las mujeres. Las nuevas formas de control tecnológico se verifican en la actualidad a partir de un entramado cada vez más complejo de dispositivos y plataformas digitales que atraviesan nuestras vidas.

Es cierto que el feminismo encontró en la internet una aliada para hackear el patriarcado (Boix, 2016). "El movimiento feminista tiene mucho que ver con la forma rizomática de nodos autónomos pero interconectados, con intereses específicos marcados por las diversas agendas pero compartiendo valores y principios comunes", señala Montserrat Boix (2015) acerca de la relación entre tecnopolítica y ciberfeminismo. Los nodos difuminados pero también en interconexión a través de las redes adquieren la capacidad de converger en determinados puntos para lograr "tener masa crítica para incorporar la lucha contra el patriarcado a las nuevas dinámicas de cambio que se están generando en todo el planeta. La capacidad colectiva de apropiación de herramientas digitales para la acción colectiva es imprescindible", destaca. Aunque existe una brecha digital de género (Castaño, 2008), cuyos orígenes y causas múltiples se relacionan con la posición subordinada de las mujeres en la creación de tecnología, por la educación sexista, por el techo de vidrio en las empresas *high-tech*, por la doble jornada de trabajo y por muchísimas otras causas vinculadas a la histórica subordinación de las mujeres, las cosas están cambiando aceleradamente y las reacciones misóginas no se hacen esperar.

No es por acaso que el tema emergente del activismo feminista contra la violencia de género en Brasil ha sido el fenómeno del odio misógino ejercido mediante y a través de los dispositivos electrónicos con los que interactuamos: internet y los dispositivos móviles conectados.

En internet, por ejemplo, la violencia contra las mujeres (en adelante, VCM) abarca desde el acoso, hostigamiento, extorsión y amenazas, robo de identidad, *doxing*, alteración y publicación de fotos y videos sin consentimiento y muchas de estas violencias se extienden al plano físico. Todos estos ataques afectan de manera real la vida de las mujeres porque generan daño a la reputación, aislamiento, alienación, movilidad limitada, depresión, miedo, ansiedad, trastornos de sueño y hasta suicidios. En este contexto surgen, por un lado, reclamos de mayores puniciones, más leyes y más control sobre lo que sucede en internet y por el otro, recaen sobre las mujeres la responsabilidad y a veces también la culpa de esas situaciones.

La Asociación para el Progreso de las Comunicaciones (APC, 2018) ha recolectado en los últimos seis años más de 1000 relatos de supervivencia y resistencia de mujeres. Alrededor de 2000 incidentes de VCM haciendo uso de espacios en línea y tecnologías de información y comunicación (TIC) están registrados en el mapa mundial de ¡Dominemos la tecnología! creado por APC. El propósito de dicho mapa es reunir evidencias para mostrar cómo las TIC pueden usarse para perpetrar violencias. Se buscó recolectar información para concientizar y también para que las autoridades y propietarios de las plataformas brinden respuestas y soluciones a la VCM en línea. Otro objetivo fue intentar garantizar un compromiso de los estados para facilitar el acceso de las mujeres a la justicia cada vez que enfrentan estas violencias y trabajar con sobrevivientes, activistas contra la VCM y diseñadores/as de políticas para poner fin a la VCM en línea (GenderIT, 2011).

Amenazas y acciones violentas no son cosa rara: en Brasil se han creado páginas *fake* de conocidas blogueras feministas, divulgando sus datos personales como el teléfono y la dirección del domicilio personal, como en el caso de la bloguera Lola Aronovich, que viene siendo amenazada de muerte desde hace años. A otra bloguera, Ana Freitas, periodista especializada en videojuegos, la acosaron en internet y en su casa: ella y sus vecinos recibían amenazas de muerte por correo y paquetes con todo tipo de cosas desagradables como materia fecal y animales muertos (Goldsman, 2015).

Los derechos a la privacidad, a la libertad de expresión, a decidir libremente y el derecho a la integridad personal están interrelacionados. Así mismo la VCM en ambientes digitales no justifica la vigilancia masiva ni el control extendido sobre internet de manera integral. Muchas y muchos hablan de que sería una nueva forma de violencia y que serían necesarias de nuevas leyes para punirla, cuando, en realidad, se trata de la misma violencia histórica y patriarcal traducida a nuevos formatos y espacios.

Frente a este panorama, vale reflexionar sobre las tensiones generadas por las posibilidades libertadoras de internet para el movimiento feminista y la expansión de la vigilancia a través de variados dispositivos y usos tecnológicos, que consideramos otra forma de violencia, más sutil, que es invisible en la vida cotidiana. Sostenemos que la VCM en ambientes digitales no justifica el punitivismo (inclusive, el de ciertos grupos del movimiento feminista), la vigilancia masiva ni el control extenso e indiscriminado sobre todo lo que sucede en esas plataformas. Para eso, vamos examinar las diversas nociones de privacidad (Siri, 2015; Bruno, 2013), vigilancia, y algunos ejemplos sobre cómo las tecnologías móviles y otras biotecnologías pueden ser trampas contralos derechos humanos de las mujeres en el ciberespacio.

## VCM: el Estado contra-ataca

Para los casos de VCM en entornos digitales en Brasil existen leyes nacionales y principios legales aplicables, tal como el Código Penal, que caracteriza la injuria, la difamación y calumnia, conocidos como crímenes contra la honra. Amenaza de muerte o violación también están caracterizados en la ley. No hay en el país una ley que caracterice las ofensas y discriminaciones por género como crimen, pues la ley "Maria da Penha" contra la "violencia doméstica" no caracteriza este tipo de daño. A la vez, existen en Brasil diversas iniciativas legislativas para punir los crimenes misóginos en red. Pero estos proyectos, específicos para conductas criminales, se enmarcan en una ola vigilantista y punitivista que reclama el control masivo y general de internet como la única posibilidad de prevenir y enfrentar estos hechos.

En la Argentina, por ejemplo, la Ley 26.485 de protección integral contra la violencia contra las mujeres (Consejo Nacional de la Magistratura, 2009) si bien no establece mecanismos sancionatorios de la violencia simbólica, en su artículo 5 establece que la "violencia simbólica es la que a través de patrones estereotipados, mensajes, valores, íconos o signos transmite y reproduce dominación, desigualdad y discriminación en las relaciones sociales, naturalizando la subordinación de las mujeres en la sociedad". Está en trámite un proyecto que modifica esta ley, ampliando aún más la cobertura de derechos, incorporando el concepto de "dignidad digital", entendida como cualidad de valor o estima que

le es inherente a toda mujer como persona humana en el entorno virtual". En consecuencia, define a la violencia digital como aquella que afecta la dignidad digital de las mujeres al lesionar alguno o varios de sus bienes y/o derechos digitales, tales como la reputación, la libertad, la existencia, el domicilio, la privacidad y la inclusión digitales, o afecta cualquier otro aspecto de su acceso y desenvolvimiento en el ámbito virtual, el uso de las tecnologías de la información y la comunicación, la seguridad informática de sus equipos y dispositivos y la indemnidad de su identidad digital" (Argentina, 2018).

En Guatemala, por su parte, la Ley contra la Violencia Sexual, Explotación y Trata de Personas, resulta ser un interesante y oportuno mecanismo de protección al derecho a la privacidad digital pues en su artículo 190 establece sanciones para quienes por cualquier medio, sin el consentimiento de la persona, capte mensajes, conversaciones, comunicaciones, sonidos, imágenes en general para afectar la dignidad de su persona (Fundación Acceso, 2015). En contrapartida, entre 2012 y 2014 el gobierno habría ido ampliando progresivamente sus capacidades de vigilancia, adquiriendo actualizaciones de diferentes tipos de software para esa finalidad y alquilando un edificio destinado exclusivamente al centro de espionaje. Este tipo de práctica no es nueva en la región: ya en 2016 se denunciaba la adquisición por parte de los gobiernos de México, Honduras, Panamá, Ecuador, Colombia, Brasil y Chile del software proporcionado por Hacking Team, y se sabía que al menos otros seis países de la región (incluida Guatemala) habían sostenido negociaciones para la compra de este software (Diaz, 2018).

En el Brasil, a finales de 2015 se conformó en la Cámara de Diputados una Comisión Parlamentar de Inquérito (CPI) para investigar actividades criminales online. La comisión, conocida como CPICiber, fue escenario de disputas políticas partidarias que poco favorecieron un debate racional sobre la seguridad de las comunicaciones digitales (Texeira, 2016). Las discusiones versaron sobre cómo eliminar contenidos que atentan contra la honra de las personas, los derechos autorales en internet, el acceso indebido a los datos personales de usuarias/os por parte de la policía y el poder judicial, la exigencia de identificación de todos los usuarios/as que accedan sitios web y aplicaciones, con todos los datos de filiación, el bloqueo de aplicaciones y la neutralidad de la red. Todos esos temas se organizaron alrededor de varios proyectos de ley enviados al Congreso por la relatoría de "crímenes contra la honra y otras injurias" de esa CPI, muy criticada por las entidades de la sociedad civil que defienden los derechos humanos en internet por colocar en peligro la libertad de expresión, la privacidad, el acceso. Algunas de esas propuestas constituyen verdaderas amenazas en la medida en que expresan una tendencia al aumento de la vigilancia en nombre de la seguridad de las mujeres (Intervozes, 2016). Es imprescindible el anonimato para garantizar el derecho a la libertad de expresión y al disenso político. Para poder profundizar en estos asuntos hay que entender qué es la privacidad y qué tipo de ejercicio de los derechos humanos posibilita.

En el caso de los movimientos de mujeres que luchan por los derechos sexuales y reproductivos la privacidad es una condición *sinequanon* para poder defender derechos negados. En Chile, como en otros países de la región, la internet se convirtió en una de las plataformas más importantes para que activistas de derechos sexuales y reproductivos expresen sus opiniones, proporcionen información y ejerciten su derecho al aborto. "Pero al mismo tiempo internet invita al acoso y a infringir las normas de privacidad de las comunicaciones" (Peña y Bruna, 2014, p.88).

Recordemos que en Brasil el aborto legal es permitido solo cuando el embarazo es resultado de una violación, cuando hay riesgo de muerte para la mujer y cuando el feto es anencefálico (no posee cerebro). Pero raramente el aborto legal es realizado en hospitales públicos porque médicos, iglesias y entidades antiderechos lo vienen impidiendo de formas diversas. Muchos proyectos que se tramitan en el legislativo intentan restringir todavía más el derecho al aborto. Hay un proyecto de ley que, caso sea aprobado, establece que los profesionales de salud que auxilien a mujeres en casos de aborto sin que las víctimas comprueben haber sufrido violencia sexual, podrán ser sancionados con penas de hasta tres años de prisión. El Proyecto de Ley nº 7.443/2006, cuyo autor es el ex-presidente de la Cámara de Diputados, Eduardo Cunha (PMDB-RJ), hoy preso, también propone transformar en crimen el "anuncio de medios abortivos", dificultando la difusión de informaciones sobre los derechos reproductivos y la venta o distribución de métodos contraceptivos. Más aún, el sustitutivo presentado por el relator de la materia en la Comisión de Constitución, Justicia y Ciudadanía (CCJ) de la Cámara de Diputados, diputado federal Evandro Gussi (PV-SP), también altera la reciente reglamentación de la atención de personas en situación de violencia sexual y quita la obligación a médicos y enfermeros de informar a las víctimas sus derechos legales y los servicios disponibles. Otro proyecto en trámite es la PEC nº 29/2015,

presentada por el senador Magno Malta y apoyada por 27 senadores, que está a la espera de un relator en la Comisión de Constitución y Justicia de la Cámara Alta. Esa propuesta pretende cambiar la redacción del artículo 5º de la Constitución Brasilera para "todos son iguales ante la ley **desde la concepción**" (negritas nuestras), en consonancia con otro proyecto antiderechos, el llamado "Estatuto do Nascituro", que privilegia los derechos del embrión desde el momento de la concepción y que transforma el aborto en crimen hediondo.

Otros casos que merecen destaque son los ataques a mujeres en plataformas de redes sociales. Antes de las elecciones brasileras de 2018, el grupo de Facebook creado para discutir la elección del hoy diputado federal Jair Bolsonaro a la presidencia del Brasil, llamado "Mulheres unidas contra Bolsonaro", con más de dos millones de participantes, fue hackeado, su nombre alterado y quedó un tiempo en off. Las cuentas personales de las activistas fueron invadidas por personas a favor del candidato; las activistas sufrieron amenazas físicas y sus celulares invadidos, una práctica que se encuadra en el doxing (Becker, 2018). Además, una de las creadoras del grupo sufrió una agresión directa en la puerta de su casa, en Rio de Janeiro (Martinelli, 2018). Pasadas varias semanas la investigación en nada avanzó. Facebook, con su política de nombre real, hace años facilita ese tipo de ataque al exigir múltiples credenciales a sus participantes. Gestores de la plataforma argumentan que esa medida se relaciona a la seguridad de su ambiente e identificación de agresores, pero especialistas afirman que la política del nombre real solo sirve para exponer a las personas que hacen parte de movimientos sociales y que discuten pautas sensibles. Existirían otras formas - menos riesgosas para sus usuarixs - de rastreo de criminales en la red.

Laura Siri (2015) señala que la privacidad importa por la función social que cumple para permitir la libertad y la democracia. Para ella, el libro "Privacidad Amenazada", de Helen Nissembaum (*in* Siri, 2015) sirve para entender por qué la privacidad es fundamental:

- La individualidad: porque la oportunidad de un desarrollo personal satisfactorio, creativo y saludable depende en gran parte de la posibilidad de experimentar sin el temor a la desaprobación, censura o el ridículo y sin la presión de adecuarse constantemente a las normas convencionales.
- La autonomía: la privacidad es una manera de mantener la autonomía con respecto a cierta información que una persona considera que no debe ser revelada a terceros.
- Las relaciones sociales: la autonomía de alguien para disponer de los elementos que conforman su vida privada le permite revelar voluntariamente a ciertas personas y en ciertos contextos la información personal que considera oportuna, útil y necesaria.
- La participación política: la privacidad es un valor esencial de todo sistema social y político legítimo. Es constitutiva de otros derechos, tales como la libertad de asociación y de discurso.

Por lo expuesto, la condición de privacidad y anonimato se relaciona también con las necesidades de los movimientos de mujeres y personas de las disidencias sexuales.

## Otras formas de vigilancia sobre los cuerpos de las mujeres

Podríamos afirmar que la historia del cuerpo es la historia de las panoplias correctivas (Vigarello, 1995), es decir: la trayectoria de un aparato multidisciplinario (dietas, cirugías, deportes, implantes) para modelarlo, domarlo, dominarlo. El movimiento feminista viene discutiendo las formas y definiciones e intervenciones científicas, tecnológicas y médicas del cuerpo de las mujeres que han sido usadas para (re)producir su subordinación (Natansohn, 2005). El ciclo reproductivo se destaca como uno de los principales temas de la biología femenina que parece justificar el macizo desarrollo de tecnologías para su control. La menstruación, la concepción, el parto, el puerperio, las hormonas, la menopausia, la tensión pre-menstrual, todo es objeto de intervención biopolítica. El cuerpo de las mujeres ha sido uno de los pilares sobre los cuales se sustenta la diferencia y subordinación de género y las tecnologías biomédicas han sido actoras principales en el modelaje del cuerpo femenino, sea para controlar, sea para garantizar ideológicamente la perpetuación de su dominación.

Microchips para controlar las dosis hormonales de anticonceptivos hoy sustituyen a los todavía novedosos implantes subcutáneos, utilizados también como método de prevención de los embarazos. Si los implantes ponían en cuestión a la falta de autonomía de las mujeres para controlar su funcionamiento, las versiones digitales colocan temas aún más controvertidos. Tal el caso de la empresa Microchips Biotech, Inc., analizado por Daniela Manica (2015), donde un minichip implantado debajo de la piel promete ser activado por una señal de red wi-fi que libera la dosis de droga programada. ¿De qué forma

podemos garantizar la seguridad de la administración medicamentosa a distancia? Todavía,

> *la posibilidad de que terceros accedan al dispositivo, provocando o inhibiendo la liberación de la substancia sin el control y conocimiento de la usuaria fue relatada como una de las inseguridades del método. También abordamos temas como la necesidad y los límites de una codificación de los datos de los dispositivos móviles que deben controlar los microchips, problematizando la posibilidad de que sean invadidos y controlados por terceras personas, en una especie de hackeamiento ovariano ("ovarian hacking"), inclusive, con eventuales objetivos vengativos ("revenge pregnancy"), como un desdoblamiento similar al que se conoce como pornografía de la venganza ("revenge porn") (Manica, 2015, traducción nuestra).*

En Brasil la colectiva Coding Rights se viene dedicando a estudiar el fenómeno que denominan las "Menstruapps" con el interés de indagar cómo funcionan las aplicaciones para celulares relacionadas con el seguimiento del ciclo menstrual. Estas aplicaciones son ofrecidas para controlar la ovulación, el ciclo y el período fértil, controlar el peso corporal, las medidas del cuerpo (cintura, pecho, caderas), supervisar la presión arterial y el pulso. Algunos calculan el promedio de los últimos ciclos menstruales para predecir la fecha de inicio del próximo, indicar días de fertilidad, ovulación, períodos actuales y futuros. Todos estos están disponibles en los sitios web de las tiendas oficiales de aplicaciones de los sistemas Androide (de Google) e IOS (de Apple).

> *Alimentadas con nuestros datos, estas herramientas funcionan como laboratorios para la observación de patrones fisiológicos y de comportamiento, que van desde la frecuencia de la menstruación y los síntomas asociados con ella, hasta los hábitos de compras y navegación por internet de todas sus usuarias. Con las menstruapps, monitorear tu ciclo significa informar regularmente a la aplicación si saliste; bebiste; fumaste; tomaste algún remedio; estabas muy excitada; tuviste sexo; en qué posición estabas cuando tuviste un orgasmo; cómo fue tu caca; si te sentiste triste; si dormiste bien; si tu piel está bien; cómo estás de ánimo; si tu flujo vaginal está más verdoso, tiene mal olor o un aspecto como de crema (Felizi y Varón, 2016).*

Uno de los colectores menstruales ofrecidos en el mercado de las "menstruapps" llamado Looncup promete un ciclo menstrual saludable a través de una conexión a dispositivos Android e iOS intermediado por el sistema Bluetooth. Estos sistemas permiten seguir desde el celular el color del flujo y conocer exactamente cuándo es el momento de vaciar y volver a colocar la copa en el interior del canal vaginal. Lo que significa, de alguna manera, dejar en manos del dispositivo la propia percepción del torrente de flujo sanguíneo. Otra propuesta semejante es la de los tampones My Flow, acompañados por un llavero que, combinado con el uso del celular tercerizaría esa acción de autocuidado tan simple como pasar por el baño para revisar cualquier posible filtración de sangre. Es decir, la mujer le delegaría a su dispositivo el percibir la cantidad de flujo que su cuerpo produce y la decisión de cambiarse o no. En este marco no resulta entonces tan llamativo que las empresas que llevan adelante estas apps, en este caso desde el blog la aplicación Kindara, se animen a publicar predicciones acerca de la salud de las mujeres en 2016, siendo una de esas proyecciones que "las mujeres confiarán más en sus celulares que en los doctores. En 2016, veremos a las mujeres alejándose de los consultorios hacia sus *smartphones*" (Kindara.com, 2016, online). Reafirmando la visión patriarcal vigente, una búsqueda aleatoria en internet de "aplicativos para hombres" lleva a recursos y herramientas para medir espacios físicos (reglas, metros, distancias, ángulos), para agendar eventos deportivos, ejercicios físicos para "estar en forma", kit de supervivencia y aplicativos para conocer mujeres, entre otros.

Cabe recordar que la informatización de los procedimientos clínicos (como la historia clínica de los/las pacientes, por ejemplo) ha sido puesta en debate por las entidades médicas en la medida en que la difusión, manipulación o pérdida y el acceso por personal no autorizado a los datos sanitarios puede acarrear graves consecuencias para el paciente pues vulnera gravemente el derecho a la intimidad y confidencialidad de sus datos médicos.

Los aplicativos recogen datos íntimos y los sistematizan "puertas adentro", es decir, no hacen público para qué esas informaciones pueden ser efectivamente utilizadas cuando las usuarias dan su aprobación a sus términos y condiciones. Y cuándo lo hacen no dejan del todo claro cuáles son sus posibles consecuencias sobre la salud individual y colectiva. Pero ¿cómo funcionan esas tecnologías y al servicio de cuáles intereses ellas trabajan?

> *La cantidad de datos y metadatos recopilados por estas aplicaciones ha posibilitado una cuantificación del cuerpo de las mujeres en una escala nunca antes vista… En momentos en que la privacidad de los datos se ha convertido en unos de los principales temas en debate, estas aplicaciones están recogiendo datos a ritmo veloz y los comparten con terceros que casi siempre permanecen ocultos (Rizk y Othman, 2016, p. 15).*

La condición de anonimato en internet se relaciona con la información que circula sobre las mujeres: ¿Quién la almacena, quién la ve, quién la toca, qué hacen con ella? El anonimato permite la privacidad, que es una forma autonomía y poder. La privacidad y el anonimato empoderan, y son esenciales para determinados contextos políticos, tanto para votar como para asociarse y expresarse. Aún más, el anonimato ha sido uno de los aspectos que más han contribuido para potencializar internet como el espacio cultural, artístico, político y educativo que es hoy.

Al respecto de la gestión y protección de datos personales, la autogestión de la privacidad y el consentimiento relacionado con nuestra información, Daniel Solove (2013) hace una lectura crítica acerca de lo que denomina "la autogestión de la privacidad". Para ello se basa en la noción de consentimiento y centra su análisis en si la gente autoriza determinadas prácticas respecto de su privacidad. En estos casos "el consentimiento legitima casi cualquier tipo de colección, uso o divulgación de datos personales". Y problematiza que aunque la autogestión de la privacidad sería una posible solución ante cualquier régimen regulatorio, las expectativas puestas en este régimen se encuentran fuera de sus posibilidades. "La autogestión de la privacidad no entrega a las personas un control significativo sobre sus datos. En primer lugar, investigaciones empíricas y de ciencias sociales han demostrado que existen severos problemas cognitivos que socavan la autogestión de la privacidad. Estos problemas cognitivos debilitan la capacidad de los individuos para realizar elecciones informadas y racionales respecto de los costos y beneficios de consentir en la recolección, uso y divulgación de sus datos personales" (Solove, 2013, p. 13).

Se trata, también, de detenerse a pensar sobre la digitalización masiva de los ambientes en que vivimos, en estar envueltos en conceptos como "Big Data", "Ciudades inteligentes" e "internet de las cosas", cuyos discursos traen la promesa de que a partir de la abundancia de datos, combinada con la alta capacidad de procesamiento de computadoras con algoritmos inteligentes, brindarán mayor eficiencia tanto en ventas como en la administración pública, así como sobre nuestros cuerpos y hábitos. Fenómeno ante el que debemos parar y preguntarnos ¿hasta dónde estas tecnologías permiten a las mujeres mayor capacidad de agencia y control? O por el contrario ¿aumentan la manipulación de nuestros datos (y cuerpos) sin pedir antes nuestra autorización?

## Conclusiones

Vivimos en un mundo cada vez más "datificado" y según expertas/os en el tema la vigilancia digital aún está en su "infancia" (Sparrow, 2014; Gurumurthy, 2016). En este contexto de golpes de Estado e intentos de censura a las disidencias políticas es importante contar con un análisis crítico que nos permita estar preparadas para defender derechos conquistados. "En tiempos de crisis políticas, las líneas de comunicación han sido cerradas y las formas críticas de expresión encuentran censura, acoso y arrestos" (Jansen, 2014, p. 41). Algunos proyectos de ley brasileros contra los crímenes cibernéticos van a contramano de la propia ley del Marco Civil de internet y contrarían uno de los principios más sensibles para los defensores de los derechos a una internet libre, democrática y de acceso universal: "privacidad para el débil, transparencia para el poderoso". También por eso la ley de protección de datos personales sancionada recientemente, si no sufre graves deformaciones, puede servir para garantizar derechos en la medida en da transparencia al tratamiento de estos datos.

El panorama actual es contradictorio en Brasil. Por una parte, hay una creciente consciencia y debate público sobre la VCM. Y por otro, una onda conservadora en la política amenaza los derechos humanos básicos, como el derecho a la educación sexual amplia y laica en las escuelas, los derechos reproductivos de las mujeres, y el derecho a la libertad de expresión a través de las redes.

Las alternativas tecnopolíticas que están siendo discutidas en Brasil, más allá de las características nacionales peculiares, pueden ser extrapoladas al análisis de las tendencias mundiales sobre las políticas de gobernanza para internet que inciden sobre la libertad de expresión, el derecho al disenso y a la privacidad y la situación de los derechos humanos de las mujeres. Hace falta seguir reflexionando y detallando minuciosamente cómo todos estos fenómenos inciden en el caso de la vigilancia como una forma que aumenta la intervención violenta sobre los cuerpos y las decisiones de las mujeres.

## Referencias


ALIMONTI, V. 2014. Marco Civil: A Brazilian reaction to surveillance on the internet. *Giswatch. - Communications surveillance in the digital age.*Disponibleen: https://giswatch.org/2014-communications-surveillance-digital-age.Accesoen: 08/10/2018.

ANISTIA INTERNACIONAL. 2015. 7 mudanças que ocorreram no mundo após as revelações de Snowden. *Revista F*órum. Disponible en: http://www.revistaforum.com.br/2015/06/19/7--mudancas-que-ocorreram-no-mundo-apos-as-revelacoes-de--snowden/ Acceso en: 06/10/2018.

ARGENTINA. 2018. Honorable Cámara de los Diputados. 5968-D-2018. Disponible en: https://www.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=5968-D-2018&tipo=LEY. Acceso en: 06/10/2018.

ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC). 2018. Take Back the Tech! Disponible en: https://www.takebackthetech.net/es. Acceso en: 06/10/2018.

BECKER, F. 2018. "Mulheres Contra Bolsonaro", os dilemas de ser ativista no Facebook. *El País.* Disponible en: https://brasil.elpais.com/brasil/2018/09/18/politica/1537306482_201081.html. Acceso el: 09/01/2019.

BOIX, M. 2015. Desde el ciber feminismo hacia la tecnopolítica feminista. *Pillku,* **5**(18). Disponible en: http://www.pillku.org/article/desde-el-ciberfeminismo-hacia-la-tecnopolitica-fem/ Acceso en: 05/10/2018.

BOIX, M. 2016. Hackeando el patriarcado: La lucha contra la violencia hacia las mujeres como nexo. Filosofía y práctica de Mujeres en Red desde el ciberfeminismo social. *Mujeres en Red. El periódico feminista*. Disponible en: http://www.mujeresenred.net/spip.php?article880. Acceso en: 04/10/2018.

BRUNO, F. 2013. *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade.* Porto Alegre, Sulina, 190 p.

CASTAÑO, C. 2008.*La segunda brecha digital.* Madrid, Cátedra/PUV, 368 p.

CONSEJO NACIONAL DE LA MAGISTRATURA. 2009. Ley de Protección Integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que desarrollen sus relaciones interpersonales. Argentina. Disponible en:http://www.cnm.gob.ar/legNac/Ley_26485_decreto_1011.pdf Acceso en: 17/10/2017.

DIAZ, M. 2018. Herramientas para perseguir a la oposición en Guatemala. *Derechos Digitales.* Ag. Disponible en: https://www.derechosdigitales.org/12385/herramientas-para-perseguir-a-la--oposicion-en-guatemala/. Acceso en: 06/10/2018.

FELIZI, N.; VARÓN, J. 2016. Menstruapps – ¿Cómo convertir tu menstruación en dinero (para los demás)? *Chupadados.* Disponible en: https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os--outros/ Acceso en: 07/11/2017.

FUNDACIÓN ACCESO. 2015. ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos *In:* L. PERI (coord.), *Fundación Acceso.* San José, Costa Rica. Disponible en: https://acceso.or.cr/assets/files/investigacion-resumen-ejecutivo.pdf Acceso en: 05/10/2018.

GENDERIT. 2011. El mapeo como estrategia para develar la violencia contra las mujeres en línea. *GenderIT.* Disponible en: http://www.genderit.org/es/feminist-talk/arma-el-mapa-termina--con-la-violencia-dominemos-la-tecnolog Acceso en: 04/10/2018.

GOLDSMAN, F. 2015.Una internet sin violencia hacia la mujer solo va a suceder en un mundo sin violencia hacia la mujer. *GenderIt.* Disponible en: http://www.genderit.org/es/feminist-talk/una-internet-sin-violencia-hacia-la-mujer-solo-va-suceder-en-un-mundo-sin-violencia-ha . Acceso en: 04/10/2018.

GURUMURTHY, A. 2016. Las mujeres necesitan un nuevo contrato social global, incluyendo la economía digital. *GenderIt.* Disponible en: http://www.genderit.org/es/feminist-talk/las-mujeres-necesitan-un-nuevo-contrato-social-global-incluyendo-la-econom-digital. Acceso en: 17/10/2017.

INTERVOZES. 2016. CPI de crimes cibernéticos aprova relatório que ataca liberdade na internet. *Carta Capital.* Disponible en:http://www.cartacapital.com.br/blogs/intervozes/cpi-de--crimes-ciberneticos-aprova-relatorio-que-ataca-liberdade-na--internet Acceso en: 06/10/2018.

JANSEN, F. 2014. From digital threat to digital emergency. *Giswatch. Communications surveillance in the digital age.* Disponible en: http://giswatch.org/2014-communications--surveillance-digital-age Acceso en: 01/10/2018.

KINDARA.COM. 2016. The Kindara App. Disponible en: https://www.kindara.com/. Acceso en: 04/10/2018.

MANICA, D. 2015. Sob a pele: de implantes a chips contraceptivos. *Anais do III Simpósio Internacional Lavits.* Disponible en: http://lavitsrio2015.medialabufrj.net/anais/ Acceso en: 01/10/2018.

MARTINELLI, A. 2018. Administradora do grupo 'Mulheres Contra Bolsonaro' é agredida no Rio de Janeiro. *HuffPopst Brasil.* Disponible en: https://www.huffpostbrasil.com/2018/09/25/administradora-do-grupo-mulheres-contra-bolsonaro-e-agredida-no-rio-de-janeiro_a_23541746/ Acceso el: 09/01/2019.

NATANSOHN, G. 2005. O corpo feminino como objeto médico e mediático. *Estudos Feministas,* **13**(2):256. Disponible en: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104--026X2005000200004 Acceso en: 07/10/2018.

PEÑA, P.; BRUNA, F.2014. Fighting the criminalisation of

abortion with online information: The case of Aborto Libre. *Giswatch, Communications surveillance in the digital age.* Disponible en: https://www.giswatch.org/ar/node/5707. Acceso en: 02/10/2018.

PRESIDENCIA DA REPÚBLICA. 2014. Lei n. 12.965 de 23 de abril. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acceso en: 17/10/2017.

PRIVACY INTERNATIONAL. 2015. Demanda y oferta: la industria de la vigilancia al descubierto. Disponible en: https://privacyinternational.org/sites/default/files/2017-12/DemandSupply_Espanol.pdf Acceso en: 05/10/2018.

RIZK, V.; OTHMAN, D. 2016. Quantifying Fertility and Reproduction through Mobile Apps: A Critical Overview. *Arrow para el cambio,* **22**(1):13-21. Disponible en: http://arrow.org.my/wp-content/uploads/2016/08/AFC22.1-2016.pdf Acceso en: 02/10/2018.

SAKAMOTO, L. 2015. Meu nome é Lola e estou ameaçada de morte por ser feminista. *Blog do Sakamoto.* Disponible en: http://blogdosakamoto.blogosfera.uol.com.br/2015/11/08/meu-nome-e-lola-e-estou-ameacada-de-morte-por-ser-feminista/ Acceso en: 01/10/2018.

SANTAELLA, L. 2011.As ambivalências das mídias móveis e locativas. *In:*G. BEIGUELMAN; J. LA FERLA (org.), *Nomadismos Tecnológicos.* São Paulo, Ed. Senac, p. 133-149.

SIRI, L. 2015. ¿Qué es la privacidad? Privacidad y vigilancia en entornos digitales. Curso online de Fundación Vía Libre y Artica. Disponible en: https://canvas.instructure.com/courses/981219/pages/1-dot-1-que-es-la-privacidad?module_item_id=8288975 Acceso en: 17/10/2017.

SOLOVE, D. 2013. Autogestión de la privacidad y el dilema del consentimiento, *Revista Chilena de Derecho y Tecnología,* **2**(2). Disponible en http://comunicacionymedios.uchile.cl/index.php/RCHDT/article/view/30308. Acceso en: 03/10/2018.

SPARROW, E. 2014. Digital surveillance. *Giswatch. Communications surveillance in the digital age.* Disponible en: http://giswatch.org/2014-communications-surveillance-digital-age. Acceso en: 30/09/2018.

TERRA. 2007. EUA: Suicídio inspira lei que pune assédio na web. Disponible en: http://tecnologia.terra.com.br/noticias/0,,OI2108890-EI12884,00-EUA+Suicidio+inspira+lei+que+pune+assedio+na+web.html. Acceso el: 09/01/2019.

TEXEIRA, L. 2016. O caso da CPICiber no Brasil: discurso de ódio e outros crimes cibernéticos como porta de entrada para censura e vigilância. *Oficina Antiviligancia.* Disponible en: https://antivigilancia.org/pt/2016/09/cpiciber-discurso-de-odio/ Acceso en: 06/10/2018.

VIGARELLO, G. 1995. Panóplias Corretoras: Balizas para uma história. *In:* D. SANT'ANNA (org.), *Políticas do corpo.* São Paulo, Estação Liberdade, p. 21-38.

ZUAZO, N. 2015. *Guerras de Internet.*Buenos Aires, Editorial Debate, 320 p.

*Submetido: 27/10/2017*
*Aceito: 22/10/2018*