Seguridad en la red
Alex Haché y Marta G. Franco

"*Paranoia es sólo tener la información correcta*." William S. Burroughs

La creación activa de espacios de seguridad no puede dejar de lado las tecnologías digitales e internet ya que estos cobran cada día mas importancia en la gestión de nuestras vidas cotidianas. Todo lo que hacemos en el ciberespacio, con un móvil o una tarjeta, cada vez con mas frecuencia, y de manera más ubicua y persuasiva, conforma nuestra identidad electrónica. Ese sinfín de datos compone un grafo social cuyo análisis lo revela casi todo acerca de nosotras y de las personas con quienes interactuamos. La seguridad en la red tiene que pensarse como un conjunto de prácticas que engloban nuestras identidades locales y electrónicas, las dos caras de la misma moneda. La seguridad se puede entender como la ausencia de riesgo o la confianza en algo o alguien. Cuando se utilizan tecnologías digitales, el desarrollo de praxis enfocadas a aumentar la seguridad de una misma, o de un conjunto de personas relacionadas entre sí, debe pensarse como un proceso multidimensional.

La percepción de seguridad varía según el tipo de tecnologías que usamos. Influyen los sistemas operativos que tenemos instalados en nuestros ordenadores[1], cómo nos conectamos, navegamos y buscamos información en internet, o incluso el tipo de contraseñas que elegimos a la hora de abrirnos una cuenta. Las finalidades con las que usamos estas tecnologías inciden en los tipos de seguridad que vamos a necesitar y cómo de importante resulta esconder o despistar acerca de los rastros[2] que generamos cuando navegamos por el ciberespacio, si entendemos la seguridad como mayor o menor grado de anonimato, privacidad, confidencialidad etc. Por ejemplo, nuestro nivel de cautela y paranoia puede depender de cómo de criminalizadas puedan resultar las acciones políticas que desarrollamos y potenciamos a través de las TIC. En circunstancias extremas, podemos enfrentarnos al ostracismo, la censura, campañas agresivas de acoso y derribo, acciones legales en nuestra contra e incluso acciones físicas violentas. En todo momento estamos, además, exponiéndonos a que nuestros datos y relaciones personales sean monitorizados por empresas que pueden utilizar esta información para realizar campañas de marketing. Cuando usamos las tecnologías para mantener nuestra redes sociales, para coordinar, documentar y comunicar acerca de qué hacemos y cuales son nuestras motivaciones, estamos exponiendo nuestras mentes y cuerpos mecanismos represores y de control social. Por ello hay que tener en cuenta e integrar la seguridad dentro de cada paso que vamos dando.

En ese sentido, otra dimensión fundamental de la seguridad en la red es la relación que tenemos con nuestro colectivo o red de afinidad. Sirve de muy poco que sólo tú o una pequeña parte de las personas con las que te comunicas a través de internet tengáis prácticas seguras, ya que si las otras compañeras difunden cualquier cosa por cualquier tipo de plataforma, o reciben tus mensajes sin preocuparse por la seguridad, seguramente acaben exponiéndote también. Por ello no debes exponer datos cuando tengas dudas respecto a su publicación y siempre debes pensar en cómo lo que publicas pueda afectar la privacidad de otras personas. La seguridad en la red requiere una responsabilidad individual y colectiva y esta empieza por un uso informado, consciente y crítico de las herramientas y plataformas que usamos.

Aumentar las prácticas seguras en la red también depende de desarrollar una visión holística de la seguridad. Hay que pensar en la seguridad como un proceso multidimensional que va desde defender tu cuerpo donde solo mandas tú, defender tu derecho a la expresión, a la cooperación, al anonimato, a la privacidad, a la autoría... hasta defender tu derecho al aprendizaje de herramientas y aplicaciones que te protejan, lo que también requiere saber que alternativas[3] existen y que implica usarlas, apoyarlas, defenderlas.

---

1 Mac y Windows son por ejemplo mucho más vulnerables a fallas de seguridad, virus y puertas traseras que los sistemas operativos libres GNU/Linux

2 Ver este interesante proyecto para entender el tipo de trazas que vamos generando: https://myshadow.org/#

3 Listado de alternativas libres y seguras: http://prism-break.org/ http://mecambio.net/category/cambiate-ya-a-que-esperas/conectividad/ https://www.riseup.net/en/radical-servers

Por ejemplo el "Kit de seguridad en una caja[4]" desarrollado por el colectivo Tactical Tech resume algunos de los diferentes pasos técnicos que hay que dar para incrementar la seguridad en la red. Su consistencia dependerá de que sepas proteger tu computadora de software malicioso, proteger tu información de amenazas físicas, crear y mantener contraseñas seguras, proteger los archivos sensibles, recuperar información perdida, destruir información sensible, mantenerte en el anonimato y evadir la censura, protegerte a ti mismo y a tus datos cuando utilizas sitios de redes sociales y utilizar los teléfonos móviles de la manera más segura posible.

Sirve de poco, por ejemplo, usar un software de anonimización de tu navegación por internet (como TOR) si no pones una contraseña de acceso a tu propio ordenador y no controlas muy bien quien puede usarlo, no sirve intentar mantener comunicaciones discretas dentro de tu colectivo de afinidad si una persona de ese colectivo va publicando y etiquetando fotos de vuestra reunión en Facebook, sirve de poco comprar espacio en un servidor para alojar y proteger tus contenidos si lo haces en algún servicio comercial que no te da garantías, etc. La seguridad en la red es como un juego de ajedrez en el cual cada movimiento puede tener distintas e insospechadas consecuencias. Por ello siempre resulta bueno intercambiar dudas con las compañeras respecto a qué herramienta usar y qué tipo de estrategia comunicacional se quiere tener, hablar y debatir acerca de lo que cada una entiende por seguridad y animarse mutuamente en tener cuidado y protegerse. Activar el chip de la búsqueda de más seguridad contribuye nuestro empoderamiento ya que se basa en una afirmación del valor de nuestras identidades electrónicas y por lo tanto de nosotras como habitantes del ciberespacio.

Pasamos ahora a introducir en más detalle las limitaciones y riesgos asociados al uso de la web 2.0. Muchos colectivos feministas usan herramientas comerciales sin darse cuenta de las desventajas que vienen asociadas a su ideología (neoliberal), diseño (cerrado y privativo) y naturaleza (comercial y antidemocrática). Muchas de esas herramientas han sido diseñadas desde valores muy conservadores. Su propio diseño promueven una concepción de las relaciones sociales en la que se hacen notar valores paternalistas, clasistas, individualistas, jerarquizantes, antidiversidad, heteronormativos, homófobos y por lo tanto opuestos a la emancipación de las mujeres y la lucha global contra el patriarcado. Recomendamos para entender mejor esos entresijos la lectura de dos libros clásicos del colectivo Ippolita[5]: *En el aquario de Facebook, el irresistible ascenso del anarco capitalismo*[6] y *El lado oscuro de Google*[7]. En esa misma línea, fomentar prácticas más seguras en internet pasa por entender de que manera nos exponemos y caemos en el fetichismo tecnológico, algo que el colectivo Wu Ming define así: "la red utilizada para explotar y pagar insuficientemente el trabajo intelectual; para vigilar y encarcelar a las personas; para imponer nuevos ídolos y fetiches alimentando nuevos conformismos; para transmitir la ideología dominante; para facilitar los intercambios del capitalismo financiero que nos está destruyendo"[8].

La cuestión de la seguridad en la red requiere también poner en entredicho la delegación de la gestión de nuestras identidades[9], así como de los datos generados por nuestros colectivos y acciones feministas, a gobiernos y empresas multinacionales. Lo que no queda tan claro es cuanto más hace falta para empezar a valorar la importancia de contar con más proveedores de tecnologías libres: ¿necesitamos de una hecatombe tecnológica como el cierre de Google y todos los servicios que provee? ¿O con saber que Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype y Apple están compinchados con el Servicio Nacional de Seguridad americano para espiarnos –el programa PRISM[10]– resultará suficiente para cambiar de hábitos? Si queremos alcanzar la soberanía tecnológica, hace falta una multitud de iniciativas, empresas, cooperativas y colectivos

4 https://securityinabox.org/es

5 http://www.ippolita.net

6 http://www.ippolita.net/es/print/68

7 http://www.ippolita.net/es/el-lado-oscuro-de-google-presentacion

8 http://www.trasversales.net/t24wm.htm

9 https://www.diagonalperiodico.net/panorama/utiles-legales-para-proteger-tus-datos.html

10 https://es.wikipedia.org/wiki/PRISM

informales que provean tecnologías cuyo diseño mismo nos dé garantías de que son libres, de que no nos espían, de que no están allí para fomentar nuestra alienación, ni para limitar nuestra libertad. Tecnologías del día a día pensadas para nuestros derechos en materia de expresión, cooperación, privacidad y anonimato.

¿Cómo hemos llegado a permitir que nuestra memoria colectiva esté en manos de estas empresas? Debemos rebobinar hacia atrás y analizar el contexto que permitió que surgiera lo que conocemos como web social o web 2.0. La web 2.0 es el resultado de una acumulación de cambios técnicos y sociales (nuevos estándares, servicios y nuevas formas de apropiarse de ellos) en las maneras de intercambiar datos y comunicarse en internet. Donde la web 1.0 habilitó las condiciones para la producción y consumo de información, la web 2.0 estableció las bases para compartir conocimiento a través de canales más interactivos, facilitando la publicación e intercambio de datos así como rebajando los niveles de accesibilidad y usabilidad de las herramientas previstas a tales efectos. El mundo de las aplicaciones 2.0 es el de los blogs y microblogs, los contenidos sindicados, las folksonomías y el etiquetado colectivo y los servicios donde se alojan, comparten y comentan fotos, vídeos, textos, bibliografías o enlaces. En él surgen las plataformas de redes sociales en internet como Facebook, Twitter, Tuenti y muchas más. Facebook, con casi 1000 millones de usuarias, es la red social en internet más transitada.

Estas plataformas son servicios basados en internet que permiten a una persona construir un perfil público o semipúblico dentro de un sistema interrelacionado, articular una lista de otras usuarias con quienes comparten una conexión, ver y revisar su lista de contactos y las realizadas por otras dentro del sistema compartido Su uso requiere generalmente proveer datos personales e involucrarse dentro de un proceso constante de gestión de identidad en línea. Hacer red social en internet se puede definir por lo tanto como la capacidad de establecer redes de contacto basadas en la curiosidad, el soporte y/o la solidaridad mutua, todo ello a través de la activación de vínculos fuertes (amistades y familia) y vínculos débiles (conocidos, relaciones profesionales, amigos de amigos u otras relaciones más superficiales basadas en interés, pasión o gusto en común). Estos vínculos pueden ser visualizados por al menos una parte de los contactos que usan el mismo servicio.

Hasta ahora la mayor parte de estas plataformas se han caracterizado por la imposibilidad de comunicarse entre ellas. Con tu cuenta de Facebook no comunicarte con gente que esté en Twitter ni viceversa. Esto es el resultado de las políticas de desarrollo aplicadas por las empresas comerciales, que en lugar de facilitar la interoperabilidad entre sus servicios prefieren encerrar a sus usuarias dentro de guetos digitales definidos como nichos. El objetivo es obligarnos a elegir un servicio u otro para aumentar su número de usuarias (estoy en Facebook no porque me guste sino porque toda la gente que conozco está allí), a la vez que reducen nuestra autonomía volviéndonos dependientes de su servicio, con el que hemos firmado un contrato en forma de fluctuantes y opacos términos de uso. Cuanto más exclusivos sean los datos que hemos ido creando y compartiendo y más difícil sea exportarlos o recuperarlos, más valor tendrá la red social. Cuando aparentemente no pagas por un servicio puedes tener la certeza de que tú eres el producto, y de que mientras lo usas estás trabajando activamente para que estas plataformas puedan enriquecerse y cotizar en bolsa gracias a como presentas quién eres, qué haces, qué piensas, qué consumes y con quién te relacionas o conspiras.

Estos guetos digitales constituyen una vulneración de uno de los principios fundamentales de la arquitectura de internet: su neutralidad. Una red neutral no puede tener restricciones sobre los dispositivos con los que se usa ni en los modos de comunicación, los contenidos ni los sitios permitidos. Este principio es lo que permite que todo el mundo pueda conectarse a internet y acceder a cualquier dato independientemente del tipo de ordenador, software, navegador o proveedor del que disponga. Con las plataformas de redes sociales comerciales este principio fundamental ha dejado de aplicarse, ya que para poder acceder a los datos producidos por esas redes normalmente es necesario darse de alta en ellas, conectarse a través de sus aplicaciones y aceptar que los datos se alojen en los servidores de estas compañías. Como nos recuerda Tim Berners-Lee, el padre de la World Wide Web, “Facebook, LinkedIn, Friendster y los demás suelen generar valor mediante la captura de información al entrar en ellas: su cumpleaños, su dirección de e-mail, sus gustos, y los enlaces que indican quién es amigo de quién. Estos sitios transforman estos datos en valiosas bases de datos y reutilizan esa información para proporcionar servicios de valor añadido pero sólo dentro de sus propios sitios. Una vez que ingrese sus datos en

uno de estos servicios, usted no puede usarlos en otro sitio".

Darse de alta en estas plataformas comerciales significa por lo tanto mermar poco a poco la neutralidad de la red, así como aceptar exponerse a la minería de datos (data mining) que practican estas empresas para extraer una plusvalía económica. Richard Stallman, creador del copyleft y la Free Software Foundation, se refiere a la web 2.0 como a "una campaña de marketing hiperbólica" y a su uso como un gesto estúpido que supone renunciar al control de nuestros datos. Obviamente, no se puede dar ningún tipo de seguridad sin un control por nuestra parte de los datos que generamos en la red. Por su parte, el colectivo Ippolita habla de "la más potente *arma de distracción masiva* jamás inventada" y describe "un impulso incontenible de publicar, etiquetar, comentar o enlazar imágenes, vídeos, tweets, SMS, suyos propios o de sus *amigxs*, en el vasto océano de las redes sociales". En la Web Social, "lxs usuarixs están contentísimxs y emocionadísimxs por tener sobre su mesa y en sus bolsillos el más moderno y caro dispositivo de autocotilleo, que está siempre conectado y tiene GPS integrado. Gracias a él pronto podrán ir de compras y dejarse la tarjeta de crédito en casa y quienes deben saberlo sabrán en efecto qué nos gusta, dónde estamos, qué compramos, qué estamos haciendo, con quién. O lo que sea". Para conseguir tales metas se viene desarrollando un minucioso trabajo previo para que nos desresponsabilicemos de nuestras identidades electrónicas, aceptemos la delegación a terceros de nuestros datos como la única opción posible y abandonemos nuestra privacidad y memoria a gestiones ajenas.

La mayoría de redes sociales comerciales estimulan un conjunto de prácticas dañinas a tal efecto. Nos referimos a niveles de seguridad bajos, nulos o irregulares, que hace posible la inquietante minería y negocio de datos llevada a cabo sistemáticamente por individuos, empresas y gobiernos. Los términos de uso y la propia configuración de estas aplicaciones suelen fomentan la paradoja de la privacidad, que consiste en que la mayoría de las personas dicen estar preocupadas por la confidencialidad de sus datos pero no toman medidas para protegerlos porque prefieren no comprometer su notoriedad pública o no saben cómo hacerlo. En la web 2.0 prevalecen las restricciones de derechos de autor, se limita la libertad de expresión por motivos aleatorios y poco honestos con sus usuarias y se practica censura moral dudosa, en muchos casos hacia mujeres, colectivos feministas y activistas en general. Además, se incurre continuamente en la privatización de la inteligencia y la memoria colectiva, no sólo por numerosos casos en los que servicios gratuitos se vuelven de pago tras años alimentándose de las contribuciones de las usuarias, sino porque el modelo de negocio se basa siempre en rentabilizarlas de alguna u otra manera. Por último, estas decisiones sobre nuestros datos se toman de manera unilateral e irrevocable, sin que existan mecanismos de participación directa de la comunidad en el desarrollo y gestión de las aplicaciones.

Cabe por lo tanto preguntarse qué soluciones y alternativas se están trabajando por parte de las personas más afectadas por estos problemas: nosotras, la sociedad civil. Definimos ésta como el conjunto de ciudadanas y colectivos cuyas acciones individuales y colectivas intentan cubrir deseos y necesidades a través del fomento de la transformación social y política. Estas acciones no están motivadas por el ánimo de lucro y tratan ceñirse a imperativos de responsabilidad social, transparencia e interactividad, por lo que se refuerzan los mecanismos de confianza que se puede depositar en ellas y crean y mueven conocimiento experto informal. De hecho la sociedad civil no se ha limitado nunca al uso pasivo de herramientas tecnológicas desarrolladas por otros (en general hombres blancos y ricos llamados Bill Gates y Steve Jobs, por ejemplo), sino que siempre ha contribuido al diseño y desarrollo de sus propias herramientas tecnopolíticas fomentando así su propia soberanía tecnológica: desde radios y televisiones comunitarias, el lanzamiento en órbita del primer satélite no militar, la invención del software libre y las licencias libres hasta el primer portal de noticias con sistema de publicación abierta y anónima, habilitado por la red Indymedia en 1999.

Estos últimos años de uso y experimentación con redes sociales en internet han permitido a sus usuarias entender mejor sus posibilidades para la acción colectiva orientada hacia la transformación social y política y tomar posturas más críticas respecto a sus limitaciones. Eso ha fomentado la emergencia de un panorama bastante efervescente y activo en cuanto al desarrollo de alternativas más o menos libres, más o menos orientadas hacia la seguridad y más o menos federadas e interoperables.

Estas circunstancias, junto con recientes cierres o retiradas de inversiones por la difusa rentabilidad económica de algunos servicios comerciales, así como escándalos a escala mundial como los asuntos filtrados por Chelsea

Manning[11] (Wikileaks) y ahora Edward Snowden, que han demostrado los niveles de corrupción, control y vigilancia y validado muchas tesis paranoicas relacionadas con la cultura hacker, nos llevan a pensar que es posible vivir una transición desde la web 2.0, de corte restrictivo y privativo, hacia la web social libre y descentralizada.

Si esta se desarrolla según los principios del movimiento del software libre, podría resultar tremendamente poderosa para devolver a las usuarias su autonomía, libertad y el control total de sus datos en internet. De esta manera se aseguraría que la neutralidad de la red no pueda ser puesta entredicha y revertida en el provecho de unos pocos. Y a través de la generalización del uso de la criptografía[12] a todos los niveles (HTTPS, navegador, servidores, cuentas de correo) se podría reconstruir un ciberespacio mucho más seguro para todas. No obstante, el desarrollo por la sociedad civil de más tecnologías libres orientadas hacia la seguridad seguirá dependiendo de que cada una se autoresponsabilize de las prácticas que le tocan.

En una web social libre descentralizada las usuarias pueden elegir dónde y cómo van a guardar sus datos y cuáles, cómo y con quién compartirlos, creando a través de mecanismos de autentificación y reputación círculos para el intercambio de información basadas en la confianza. Esta diferente perspectiva a la hora de entablar relaciones e interacciones en el ciberespacio puede resultar especialmente valiosa para los colectivos de transformación social y política. Si la difusión de sus ideas requiere pasar a través del potencial amplificador que tienen plataformas como Facebook o Twitter, y llegar adonde esta ahora mismo mucha gente, la campaña tiene que pensar previamente cuales pueden ser las consecuencias negativas o indeseables de este tipo de difusión.

Cabe subrayar que en los últimos años se ha recrudecido el numero de campañas machistas violentas en contra de colectivos y activistas feministas. Se ha utilizado la censura directa a través del cierre de perfiles justificados por una ola de denuncias y conllevando la perdida de los datos, el historial y los contactos, se han tumbado o dejado de proveer alojamiento a paginas webs atacadas por DDOS (Denials Of Services), se ha negado el permiso de subir contenidos audiovisuales considerados inadecuados a mujeres dando el pecho, a compañeras trans o a desarrolladoras de post-porno, se ha tomado el control de cuentas de correos y webcams y se ha ejercido chantaje, se ha desprotegido conscientemente los datos personales de muchas sin que ellas tuvieran conciencia de ello exponiendo direcciones y teléfonos personales. Resulta también interesante ver como esa violencia se ha orientado también hacia diversas mujeres techies que intentaban abrir un debate sobre el sexismo y el machismo en varios submundos del desarrollo de las tecnologías. Ha habido reacciones violentas que han aunado acoso, insultos, humillación y amenazas. Véanse por ejemplo los centenarios de comentarios a la carta abierta de Asher Wolf, creadora del movimiento de las cryptoparties, a la comunidad hacker[13], las reacciones a la situación vivida por Adria Richards[14] en la ultima conferencia Pycon, la descripción por la jugadora de vídeo juegos Mar-Lard[15] del sexismo dentro de las comunidades geeks, o la campaña en contra del crowdfunding de Anita Sarkeesian[16] para el desarrollo de unos episodios de Feminist Frequency[17] analizando los tropos, estereotipos y prejuicios vehiculados por los videojuegos. Todo ello muestra que la mayor parte de las tecnologías que usamos siguen siendo desarrollados por nichos de biohombres decididos a defenderse de las "feministas histéricas" que tienen la osadía de poner entredicho su estilo de vida y sus privilegios. Pero, como bien apuntaba Karen Spärck Jones, "la informática es demasiado importante para dejársela sólo a los hombres"[18] También por ello es importante que empecemos como feministas y activistas a plantearnos cual va a ser nuestro

11 http://www.npr.org/blogs/thetwo-way/2013/08/22/214440560/bradley-manning-i-am-a-female-call-me-chelsea Interesante notar que la Wikipedia no acepta el cambio de su nombre y mantiene su entrada como Bradley Manning: http://www.dailydot.com/news/wikipedia-chelsea-bradley-manning-transgender-debate/

12 https://es.wikipedia.org/wiki/Criptografia y https://en.wikipedia.org/wiki/Cypherpunks_%28book%29

13 https://n-1.cc/blog/view/1556630/dear-hacker-community-%E2%80%93-we-need-to-talk-por-asher-wolf

14 https://n-1.cc/blog/view/1640847/adria-richards-pycon-and-how-we-all-lost-by-amanda-blum

15 https://n-1.cc/blog/view/1644541/sexisme-chez-les-geeks-pourquoi-notre-communaute-est-malade-et-comment-y-remedier-parmarlard

16 http://www.feministfrequency.com/

17 http://www.feministfrequency.com/

18 https://www.diagonalperiodico.net/saberes/explorar-la-clandestinidad-clave-genero-mujeres-hacker.html

rol en el fomento de practicas mas reflexivas, tácticas y seguras con las tecnologías.

::: Documentación

> Algunos elementos de reflexión presentando la **seguridad** como algo **multidimensiona**l, por Alex Hache https://n-1.cc/file/view/1752691/seguridad-en-la-red

> **Programa "*Privacy & Expression"*** (en inglés)*:* promueve la conciencia de la seguridad digital y las competencias de las defensoras de derechos humanos, periodistas independientes, defensoras de la lucha contra la corrupción y activistas, y cualquier persona que se preocupa por los riesgos de seguridad y vulnerabilidades de las herramientas digitales. Incluye vídeos, toolkits y ejercicios. https://www.tacticaltech.org/#privacy-and-expression

> **Caja de herramientas de Seguridad**. Es un esfuerzo colaborativo entre Tactical Technology Collective y Front Line. Fue creado para satisfacer las necesidades de seguridad digital y de privacidad de activistas y defensor@s de derechos humanos. La *Caja de Herramientas de Seguridad* incluye una Guía Paso a Paso, la cual se ocupa de varios temas de seguridad digital. También proporciona una colección de Guías Prácticas, cada una de las cuales incluye una herramienta específica de software gratuito o de código abierto, así como las instrucciones necesarias sobre cómo utilizar dicha herramienta para asegurar tu computadora, proteger tu información o mantener la privacidad de tus comunicaciones por internet. Muy recomendable! https://securityinabox.org/es

> **Cuidarse**. Materiales y kits creados por take bach the tech para descubrir que pasos puedes tomar para asegurar que tu experiencia en línea sea segura. Se puede encontrar consejos e ideas acerca de como proteger tu privacidad mientras navegas y comunicas vía internet. Incluye: navegación segura por internet, caja de herramientas para trabajar de manera remota y segura, ciberacoso y cómo evitarlo, cómo gestionar las contraseñas para que sean mas seguras, buenas prácticas para protegerte cuando usas el correo electrónico y los celulares, y el uso de los móbiles para documentar y denucniar situaciones de acoso y violencia. Muy recomendable! https://www.takebackthetech.net/es/be-safe

> **Manual de seguridad en internet de Anonymous**. En: https://n-1.cc/file/view/1753124/manual-de-seguridad-en-internet-de-anonymous

> **Guía** creada por Global Voices para apoyar a los defensores y las defensoras de derechos que deseen revelar la verdad y expresarse en línea pero que podrían correr riesgos al hacerlo. (en inglés) http://advocacy.globalvoicesonline.org/projects/guide/

> **Feministing**. Red de bloggers feministas que mantienen una política de comentarios de blog para mantener la seguridad (en inglés) http://feministing.com/about/

::: Videos:

> **Ono Robot**. Serie de animación realizada por Tachtical Technology Collective con 5 episodios sobre cómo sobrevivir en la era digital. Cada episodio ofrece trucos y maneras para salvaguardar segura tu comunicación por mail, cómo mantener tu cuenta de Facebook segura y privada, cómo crear passwords mas seguras, como almacenar tus datos seguros en la nube, sobre encriptación, muestra los riesgos y vulnerabilidades de la comunicación por móvil, etc... https://onorobot.org/downloads Los subtítulos en castellano pueden descargarse aquí: https://onorobot.org/languages

::: Softwares

> **Programa Tor:** está diseñado para aumentar el grado de anonimato de sus actividades en internet y también puede utilizarse para eludir los filtros de internet. Usted puede descargar el archivo en su computadora o hacerlo funcionar mediante un dispositivo de memoria USB. https://www.torproject.org/

> **Aplicación portátil**: Es un programa de computadora capaz de archivarse y para uso desde tu USB. De esta

manera puedes abrir el programa y guardar tus datos en tu USB y no queda tu información personal y privada en la computadora que estás usando, sino en el aparato portátil que tienes. (en inglés) https://www.takebackthetech.net/es/be-safe/caja-de-herramientas-las-aplicaciones-port-tiles-de-dominemos-la-tecnolog

> **My IP**: Sitio que permite obtener información de la localización de tu IP. http://www.myip.es/

> **Listado de alternativas libres y seguras:** [http://prism-break.org/] [http://mecambio.net/category/cambiate-ya-a-que-esperas/conectividad/]

::: Artículos sobre ciberacoso, violencia en la red

> http://www.naiz.info/eu/actualidad/noticia/20130715/acoso-y-derribo-por-analizar-el-sexismo-en-los-videojuegos#.UeOehAJai8M.facebook

> http://acapulco70.com/por-que-internet-es-mas-peligroso-para-las-mujeres-que-para-los-hombres/

> https://www.takebackthetech.net/es/be-safe/ciberacoso-y-como-evitarlo