REDES SOCIALES EN PERSPECTIVA DE GÉNERO: GUÍA PARA CONOCER Y CONTRARRESTAR LAS VIOLENCIAS DE GÉNERO ON-LINE

JUNTA DE ANDALUCIA
Instituto Andaluz de Administración Pública
CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

REDES SOCIALES EN PERSPECTIVA DE GÉNERO: guía para conocer y contrarrestar las violencias de género on-line

JUNTA DE ANDALUCIA
Instituto Andaluz de Administración Pública
CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Sevilla-2017

ecoedicion ecoedicion.eu

Este libro se ha impreso utilizando papel procedente de una gestión forestal sostenible y fuentes controladas, todo ello aplicando buenas prácticas para la sostenibilidad editorial, dentro del Proyecto Life+ Ecoedición de la Consejería de Medio Ambiente y Ordenación del Territorio de la Junta de Andalucía.

JUNTA DE ANDALUCIA
CONSEJERÍA DE MEDIO AMBIENTE Y ORDENACIÓN DEL TERRITORIO

LIFE08 ENV/E/000124

RESERVADOS TODOS LOS DERECHOS. NO ESTÁ PERMITIDA LA REPRODUCCIÓN TOTAL O PARCIAL EN NINGÚN TIPO DE SOPORTE SIN PERMISO PREVIO Y POR ESCRITO DEL TITULAR DEL COPYRIGHT

TÍTULO: REDES SOCIALES EN PERSPECTIVA DE GÉNERO: GUÍA PARA CONOCER Y CONTRARRESTAR LAS VIOLENCIAS DE GÉNERO ON-LINE

Coordinación:

Núria Vergés Bosch

Autorías:

Alex Hache
Núria Vergés Bosch
Gema Manzanares Reyes, EnRedadas
María Martha Escobar, EnRedadas
Haydeé Quijano Rosado
Indira Cornelio
Anamhoo

© INSTITUTO ANDALUZ DE ADMINISTRACIÓN PÚBLICA

AENOR ER Empresa Registrada ER-1420/2002

IQNet

Gestión de publicaciones en materias de Administraciones Públicas

Edita: Instituto Andaluz de Administración Pública

Diseño: 4tintas

ISBN 978-84-8333-683-0 (Ed. electrónica)

AGRADECIMIENTOS:

Esta publicación no hubiera sido posible sin la ayuda y colaboración de otras personas y colectividades. Queremos agradecer especialmente a Eva Cruells y Lucía Egaña su colaboración en la fase de diseño de esta publicación y sus ideas aportadas en cuanto a contenidos. Así como las autoras en cuyo maravilloso activismo se basan los contenidos sobre violencias de género on-line y autodefensa, Gema Manzanares Reyes y María Martha Escobar de EnRedadas, Haydeé Quijano Rosado, Indira Cornelio y Anamhoo. También a Dolça Moreno Grabulós le damos las gracias por su labor en la revisión de contenidos en la jornada de puesta en común de contenidos junto con Alex Hache y Núria Vergés. En un plano más colectivo, agradecemos al colectivo de mujeres y nuevas tecnologías Donestech y a la asociación de mujeres para la investigación y acción Alia su apoyo incondicional y en todos los sentidos. También queremos dar las gracias a las feministas y ciberfeministas que trabajan y actúan en relación a las TIC y que han compartido sus conocimientos y nos han generado tantos aprendizajes que empapan esta publicación. También gracias a las personas activistas del software libre y la cultura libre que nos han proporcionado tantas herramientas y conocimientos para trabajar sobre ello, además de espacios de socialización y práctica tecnopolítica. Finalmente, queremos agradecer y anotar que algunos contenidos directamente parten e incluyen el trabajo previo realizado para la guía sobre género y seguridad “Zen y el arte de que la tecnología trabaje para ti” coordinado por Alex Hache, así como el trabajo realizado por Tactical tech en Myshadow.org, gendersec.tacticaltech.org y securityinabox.org. Para acabar queremos dar las gracias a la Junta de Andalucía, especialmente a las personas de publicaciones que han trabajado directamente con nosotras, su apoyo y esta posibilidad de publicación que nos han brindado.

Índice de contenidos

PRESENTACIÓN

Las redes sociales somos tú, yo, ellas, nosotros y todas. Son un espacio relacionado con la familia, las amigas, las conocidas, la calle, la plaza pública y la sociedad en general. Las redes sociales permiten encontrar oportunidades, intercambiar recursos, cubrir necesidades y poner en común nuestro ser social, nuestras sociabilidades, nuestras formas de ser, pensar, hacer y vivir mundos. Los espacios conectados también representan un campo de acción para escenificar demandas y reclamos por parte de los movimientos sociales y los colectivos pro-derechos así como para todas las personas que defienden la igualdad y justicia social de género. El uso de las redes sociales en internet permite dar a ver, conectar, amplificar, crear sinergias, grupos y otras redes de transformación social y política.

No obstante, en la sociedad actual, tampoco internet, nuestros móviles y las redes sociales on-line están libres de violencias de género. La inercia heteropatriarcal y machista sigue afincada en nuestras estructuras. Aunque con algunas diferencias, las violencias y discriminaciones contra las mujeres, personas trans y disidentes sexuales pueden ser tan intensas en Internet como en el espacio público y privado off-line. Los machismos persisten, a la vez que nuevos neo-machismos aparecen y se actualizan utilizando las nuevas tecnologías y las redes sociales como plataformas de actuación violenta privilegiadas y en auge. El uso de las TIC puede facilitar y multiplicar exponencialmente los efectos de las violencias machistas. Además de facilitar el anonimato y la suma de agresores, las redes sociales permiten la repetición, viralidad, difusión e, incluso, la normalización de estas violencias.

Dentro de ese entramado de redes sociales que se despliegan en nuestras vidas conectadas y fuera de Internet operan una multitud de posibilidades que se entrelazan fuertemente. Por todo ello, es cada vez más importante entender dónde y cómo nos movemos por los espacios conectados, para poder saber cómo operar e influenciar cambios positivos, así como para poder cuidar y cuidarnos entre nosotras para contrarrestar y sobrepasar estas violen-

cias, agresiones y vulnerabilidades que pueden amplificar, complementar o, incluso, cambiar las que ya se experimentan en la vida física.

Pese a la gravedad de las violencias on-line, el interés de nuestras administraciones para producir datos e información pública es gravemente ausente, así como políticas específicas al respecto. Además, entradas en la era del Big Data que analiza y comercializa gran parte de la información que compartimos en las redes, sorprende la inexistencia de datos públicos sobre ataques y violencias de género on-line. Si queremos acercarnos a estas violencias de género sólo podemos acudir a estudios puntuales de la academia, de instituciones internacionales, de algún departamento o institución pública, de alguna periodista comprometida y/o, como pioneras en esta y otras luchas de género, remitirnos a las entidades y colectivos feministas que se esfuerzan para visibilizarlas y hacerles frente.

Por todo ello esta publicación incluye, en una primera parte, la presentación de algunas de las características de las redes sociales en general y de las plataformas de redes sociales on-line. Lo abordamos de forma crítica y con perspectiva de género, así como relacionamos internet, las identidades, la privacidad y la seguridad con el género. Seguidamente nos adentramos en las violencias de género y, específicamente, las violencias de género on-line. Partimos de un análisis del panorama de datos cuantitativos y cualitativos existentes para, en la medida de lo posible, visibilizar qué está pasando si nos preguntamos sobre este tipo de violencias. Después, en una segunda parte, exponemos en detalle las violencias de género on-line, así como las posibilidades de hacerles frente. En este sentido, identificamos y definimos un conjunto de violencias de género que están ocurriendo en las redes sociales on-line y presentamos, a la vez, pistas, recomendaciones e iniciativas para profundizar en ellas y lograr autodefendernos, así como contrarrestarlas.

Esta publicación pues, está pensada para que pueda utilizarse también como guía y manual para entender mejor cuales son los componentes de género que atraviesan las redes sociales on-line. Sin embargo, y sobre todo, buscamos contribuir a que desde una posición más informada, crítica y feminista se puedan detectar y conocer las violencias de género on-line y,en la medida de lo posible y en un futuro próximo, se puedan sobrepasar. Por ello, esta publicación puede resultar muy útil a las mujeres, especialmente a las mujeres vocales, feministas y disidentes sexuales y de género, que de forma creciente se ven afectadas por las violencias de género on-line. Además, por el idioma utilizado, las autorías, voces y miradas, así como la mayoría de datos y referencias utilizadas, esta guía resulta especialmente interesante para las mujeres latinas e iberoamericanas.

Desde el colectivo Donestech, junto con tantas otras ciberfeministas, hace años detectamos la necesidad de trabajar para que internet y las redes sociales on-line se convirtieran en espacios seguros y libres, especialmente para las mujeres y las personas disidentes de género. A lo largo de los últimos años las ciberfeministas hemos ido generando informaciones, manuales, kit encuentros, eventos, talleres y acciones en pro de unas redes sociales seguras y libres de violencias de género. Una muestra de ello lo constituyen nuestras contribuciones en trabajos anteriores como el manual Zen y el arte de que la tecnología trabaje para ti que, de alguna forma, se han reincorporado en esta publicación y fusionado con otras y nuevas informaciones generadas por otras investigadoras, activistas y ciberfeministas en la materia.

Aunque llevamos un tiempo dedicadas a estas tareas resultaba imprescindible poder contar con una publicación que recogiera los conocimientos generados y sirviera de guía para muchas más. Además, era necesario poderlo realizar en condiciones y desde las miradas y experiencias del sur, pues las especificidades iberoamericanas y latinas resultaban aún minorizadas en el contexto internacional. En este sentido, la propuesta de publicación por parte de la Junta de Andalucía de esta guía se ha convertido en una oportunidad magnífica para que esto fuera posible.

Las autoras

PARTE 1. REDES SOCIALES, GÉNERO Y VIOLENCIAS DE GÉNERO

1. INTRODUCCIÓN

En esta parte, por un lado, presentamos las redes sociales on-line con una mirada crítica. Sobre todo, buscamos la reflexión en torno a las desigualdades, así como las identidades, la privacidad y la seguridad on-line. Todo ello lo relacionamos con el género y una de las principales problemáticas que emergen, las violencias de género, también on-line. Iniciamos pues esta parte con una introducción a las redes sociales para, prontamente, introducirnos en las redes sociales on-line y darnos cuenta que quizás no sean tan abiertas y libres como creíamos. Detrás de las redes sociales hay modelos de negocio que esconden desigualdades y diversas problemáticas que nos deben llevar a cuidar y atender nuestra privacidad y seguridad digital. Más aún si lo relacionamos con el género. Las primeras ciberfeministas celebraron con gran optimismo las posibilidades que se abrían para las mujeres en el ciberespacio. Sin embargo, pronto, el trabajo en pro de la erradicación de las violencias de género empezó a conectar y concentrar sus acciones on-line. Actualmente, también las violencias de género mediadas por las TIC, con sus propias especificidades, centran parte del trabajo de las ciberfeministas.

Por otro lado, y ya habiendo introducido las violencias de género y sus rasgos fundamentales cuando se ven mediadas por las TIC, introducimos algunas luces sobre las violencias de género on-line. Con ello buscamos responder a la pregunta de qué está pasando. Lo que está ocurriendo apunta, en primer lugar, a la persistencia de las viejas estructuras patriarcales, la actuación de los agresores machistas y su actualización en las nuevas redes sociales apoyadas por la emergencia de los neomachismos. Ello hace que reivindiquemos la generación de datos públicos y sistemáticos sobre las violencias de género on-line, pero también, que debamos ser conscientes de los riesgos existentes en las redes sociales y cuidarnos. Sin embargo, apuntamos que esto no puede limitar la libertad de movimiento, actuación y presencia de las mujeres en los espacios on-line. Finalmente, A través de los pocos datos existentes y de algunos ejemplos clarificadores, del contexto iberoamericano sobre todo, intentamos mostrar el alcance, intensidad y gravedad de las violencias de género on-line. De forma específica también tratamos la pornografía no consensuada, así como los ataques on-line a mujeres vocales, feministas y personas disidentes sexuales y de género.

2. REDES SOCIALES Y GÉNERO

2.1 Las redes sociales on-line: una aproximación crítica

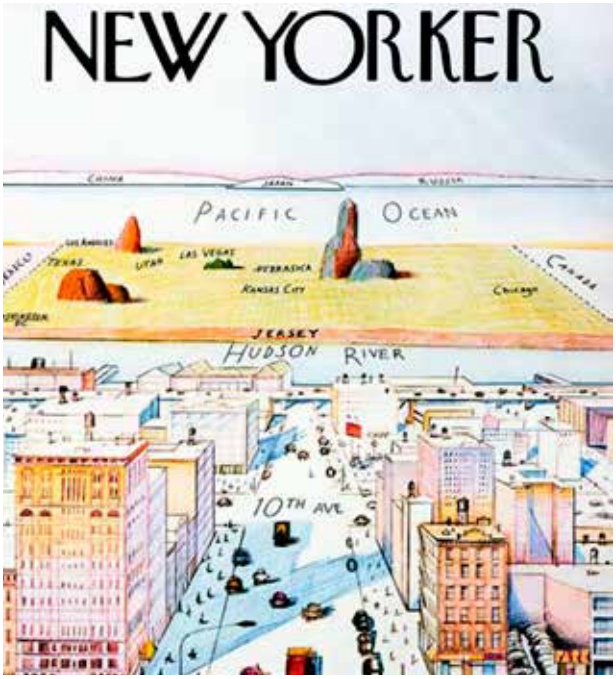
Las redes sociales son estructuras sociales compuestas por personas y grupos de personas, conectadas entre ellas a través de uno o varios tipos de relaciones (familiares, amistades, profesionales, ocio, soporte, conocidas, etc). Estas redes operan en varios niveles de interacción y complejidad. Se pueden hacer mapas de los vínculos entre los nodos y también mapas de una red completa. También se puede visualizar la red que envuelve a una persona, su red personal, o visualizar el gráfico social que la rodea (amigas de amigas).

Los estudios sobre las redes sociales se remontan a la primera mitad del siglo XIX con investigadores sociales como Auguste Comte y Émile Durkheim. Estos investigadores buscaban explicar los sistemas sociales a partir de analogías con los sistemas biológicos y epidemiológicos, pero también con las infraestructuras eléctricas, financieras o de información y comunicación.

En la década de 1950, Simon Kochen y Sola Pool, escribieron un artículo conocido hoy como el problema del mundo pequeño: Si dos personas fueran seleccionadas aleatoriamente en una población, ¿cuáles serían las posibilidades de que ellas se conocieran y, más genéricamente, cuántas posibilidades para una cadena de convivencia que las conectara entre sí? Dos décadas después, Stanley Milgram experimentó empíricamente sus proposiciones llegando a la noción conocida popularmente hoy como “seis grados de separación”. Esta teoría supone que entre una persona y otra desconocida en otra parte del mundo, existen seis personas que podrían establecer el vínculo entre ambas. Dicho de otro modo, estamos todas potencialmente conectadas con un máximo de seis grados de separación de cualquier persona que admiremos o que no conozcamos de nada.

Pero en realidad, por mucho que consideremos que el mundo es una pequeña “aldea global”, es más grande de lo que podemos imaginar. Nuestro mundo está dividido y fracturado por vectores culturales, sociales, raciales, étnicos y de género. Si bien Internet parece haber hecho el mundo más pequeño, quizás sólo ha reducido algunas de sus partes, haciendo invisibles ciertas realidades aunque éstas se encuentran bastante cerca.

Al final dentro de las redes sociales se dan muy pocas estructuras de redes sociales aleatorias. Saul Steinberg dibujó en 1976 como los Neoyorkinos veían el mundo desde la 9a. avenida. No obstante su realidad podría aplicarse a la mayor parte de personas, para quienes la mitad de sus conocidos se encuentran en su propio barrio y/o ciudad, un cuarto de sus conocidos se encuentran en el resto del país y otro cuarto en el resto del mundo. Si nuestras redes sociales fuesen más aleatorias entonces contaríamos con muchos más contactos y amistades distribuidas por todo el mundo.



Saul Steinberg, The New Yorker

2.2 Del capital social y el efecto mateo a los filtros burbujas

Algunos conceptos importantes para entender por qué no se arman más conexiones aleatorias dentro de nuestras redes sociales tienen que ver con el capital social, el efecto mateo y los filtros burbujas.

El sociólogo francés Pierre Bourdieu distinguió tres principales formas de capital en Poder, Derecho y Clases Sociales (1983). El capital económico que se base en el concepto marxista de control sobre los recursos económicos. El Capital cultural como las formas de conocimiento, educación, habilidades, y ventajas que tiene una persona. Y el capital social como recursos generalmente intangibles basados en la pertenencia de una persona a grupos, relaciones, redes de influencia y colaboración. Bourdieu describe el capital social como "un capital de obligaciones y relaciones sociales".

Por ello, el capital social es considerado la variable que mide la colaboración social entre los diferentes grupos de un colectivo humano, y el uso individual de las oportunidades surgidas a partir de ello. El capital social mide, por tanto, la sociabilidad de un conjunto humano y aquellos aspectos que permiten que prospere la colaboración y el uso, por parte de los actores individuales, de las oportunidades que surgen en estas relaciones sociales. Una sociabilidad entendida como la capacidad para realizar trabajo conjunto, la de colaborar y llevar a cabo la acción colectiva (Tacticaltech, 2017).

En cuanto al efecto Mateo es la denominación sociológica de un fenómeno de acumulación de bienes, riqueza o fama, simplificado por la frase «el rico se hace más rico y el pobre se hace más pobre». Aunque se atribuye el uso de este término por primera vez al sociólogo Robert K. Merton su uso se ha extendido a la comprensión de los efectos de capitalización de recursos o prestigio social que se dan en las redes

sociales. Cuantos más contactos tienes, más fácil te es establecer nuevos contactos y poder disfrutar de tus privilegios y las oportunidades que te otorgan tus redes sociales.

Desde una perspectiva de género, el efecto Mateo puede ser extendido al análisis de los sistemas de privilegios y relaciones de poder de las cuales disfruta cada persona. Generalmente privilegian los hombres sobre las mujeres en el contexto de nuestras sociedades patriarcales, pero también tienen que ser analizados desde la interseccionalidad, un término acuñado por la activista y académica Kimberlé Williams Crenshaw (1989).

"Esta trata del estudio de las identidades sociales solapadas o intersectadas y sus respectivos sistemas de opresión, dominación o discriminación. La teoría sugiere y examina cómo varias categorías biológicas, sociales y culturales como el género, la etnia, la raza, la clase, la discapacidad, la orientación sexual, la religión, la casta, la edad, la nacionalidad y otros ejes de identidad interaccionan en múltiples y a menudo simultáneos niveles. La teoría propone pensar en cada

Take Back The Tech! APC - https://www.takebackthetech.net/-

elemento o rasgo de una persona como unido de manera inextricable con todos los demás elementos, para poder comprender de forma completa la propia identidad. Este marco puede usarse para comprender cómo ocurre la injusticia sistemática y la desigualdad social desde una base multidimensional"

Muchas de estas características propias a las redes sociales también se han visto replicadas y copiadas en las plataformas de redes sociales que replican en el mundo on-line los sistemas de privilegios y las relaciones de poder que se dan entre personas y entre grupos sociales privilegiados y discriminados off-line. Además, el uso intensivo de las redes sociales en internet no significa forzosamente crear red y ser capaz de llegar a una diversidad de públicos y/o mas perfiles o grupos sociales hacia los cuales se quiere comunicar o con los cuales se quiere intercambiar. Las características relacionadas con el capital social, así como el efecto mateo influencian para cada una de nosotras y nuestras oportunidades.

Todas vivimos en co-dependencia con nuestros privilegios, o su ausencia, y las relaciones de poder que derivan de estas estructuras. Estas marcan y delimitan nuestras opciones y libertades. Por ello, el reverso del efecto mateo, el efecto Matilda, justamente consiste en que cuando ya se parte de una situación de discriminación se tiende incluso a menos. Ni siquiera los méritos, bienes y contactos conseguidos sirven para ir a más.

Añadido a estas estructuras sociales y económicas, encontramos los desarrollos tecnológicos que refuerzan estas tendencias. Las plataformas de redes sociales han establecido una lógica y una narrativa construida alrededor del mito de que el protagonista del mundo eres tú facilitando que se obvien las relaciones de poder descritas anteriormente. Así es como aparecen conceptos como el "prosumidor", quien produce y consume a la vez contenidos. Muchas redes sociales son "gratis", aunque esta gratuidad se base en realidad en convertirnos a nosotras mismas en productos. En el fondo no se nos están brindando servicios gratuitos, sino que los estamos pagando con nuestra propia exposición y generación de contenidos.

La evolución en los últimos años de muchas plataformas de redes sociales ha sido marcada por el diseño de algoritmos e interfaces que estimulan de manera creciente los llamados filtros burbujas. Estos personalizan el resultado de tus búsquedas y navegación gracias a algoritmos de predicciones. Dan a ver la información que a la persona usuaria le gustaría ver basándose en información acerca de una misma (como localización, historial de búsquedas, y elementos a los que les dio clic en el pasado). Un ejemplo son los resultados de la búsqueda personalizada de Google y el hilo de noticias personalizadas de Facebook. Como resultado, nos encontramos alejados de la información que no coincide con nuestros puntos de vista, aislándonos efectivamente en burbujas ideológicas y culturales propias.

Muchas de las plataformas de redes sociales tienen una arquitectura que se enfoca en una dimensión individualista de las redes y vuelve difícil encajar dinámicas de trabajo colaborativas y de creación colectiva. Sus interfaces no son empáticas, sus términos de uso, políticas de privacidad y prácticas de seguridad dan mucho que desear.

Así, como ya apuntamos en otros trabajos (Cabello, Hache, Franco, 2012) "Si celebramos la posibilidad de intercambiar correos electrónicos independientemente del proveedor (gmail, yahoo, hotmail, tutanota..) o gestor de correo (thunderbird, outlook, webmail) que escojamos y de publicar y enlazar páginas web sabiendo que serán accesibles independientemente del navegador que empleemos, ¿por qué deberíamos aceptar que los perfiles y vínculos sociales que construimos a través de la web queden zonificados en función de la red social que escojamos, renunciando así a relacionarnos con quienes no pertenezcan a ella y debiendo además dejarlos atrás si decidimos mudarnos a otra distinta? En definitiva, ¿por qué la web de las redes sociales debería ser distinta de la web a secas?"

Es decir, si no participas de una red social determinada te quedas fuera de todo lo que circula allí. Aunque parezca que en las redes sociales está el mundo

Pillku - https://pillku.org/

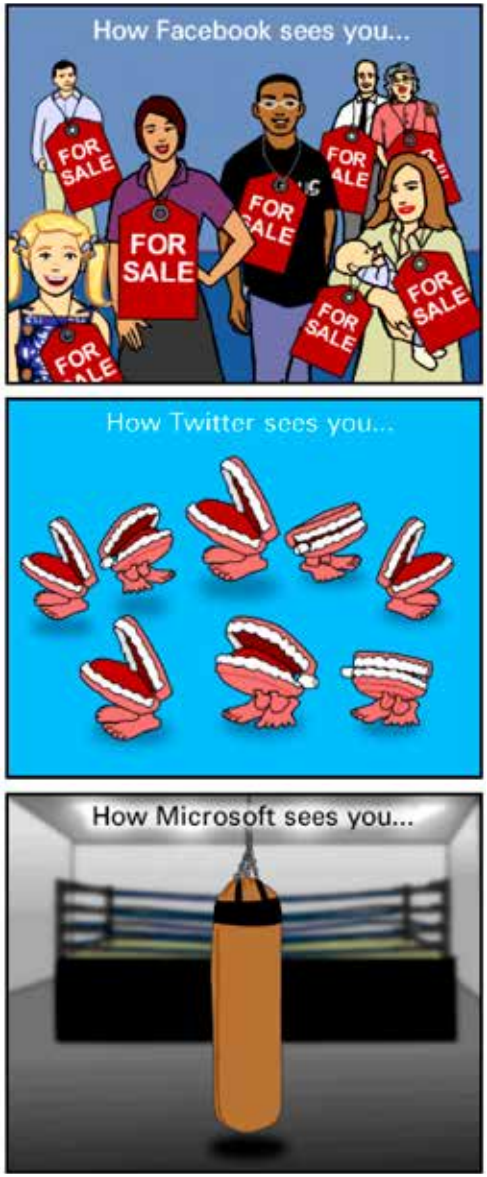
entero, la mayoría de las veces, debido a los algoritmos y formatos propios de estas herramientas, nos quedamos en contacto con personas bastante parecidas a nosotras mismas. Es lo que hemos definido anteriormente como el fenómeno de los filtros burbujas. Además, hay burbujas que incluyen redes más privilegiadas y con posibilidades de influencia que otras. Entonces se produce un efecto inercia muy potente que nos puede ir aislando, a la par que excluyendo, manteniendo con ello, un estatus quo muy resistente al cambio y a la transformación social y de género.

2.3 Nuevos modelos de negocio: privacidad y libertad de movimiento ¿Para quién?

Desde finales del siglo XX, una vorágine de inversiones y starts ups intentaban ver como generar dinero con internet. Aunque muchas no sobrevivieron al crash de las puntodot en la década 2000, algunas sí entendieron que el modelo de negocio radicaba en la colecta de nuestros datos (y el rastreo de nuestras sombras digitales) y pensaron que la mejor manera de engancharnos era "regalándonos" servicios útiles, accesibles e innovadores. Con la difusión de esa falsa idea de gratuidad, canjeamos nuestra privacidad, así como el derecho a re-inventarnos y ser múltiples. Guardamos en el armario el pasamontañas zapatista y la máscara de gorila de las guerilla girls para poder hacernos selfies en los centros comerciales panópticos creados por google, facebook, amazon, twitter y etc.

Ese cambio de rumbo quedó patente en 2010 cuando Mark Zuckerberg (Fundador y CEO de la empresa Facebook) declaró que la era de la privacidad se había acabado. Esta perspectiva señalaba una nueva orientación de la agenda mundial neocon (buscando "transparencia radical" para todos menos para los gobiernos y las empresas) así como también resaltaba que las nuevas reglas del juego iban a ser guiadas por el uso de nuestro nombre real y por la multiplicación de información personal identificable. Anoten que el mismo Zuckerberg compro en 2013 las 4 casas vecinas a la suya para mantener su privacidad.

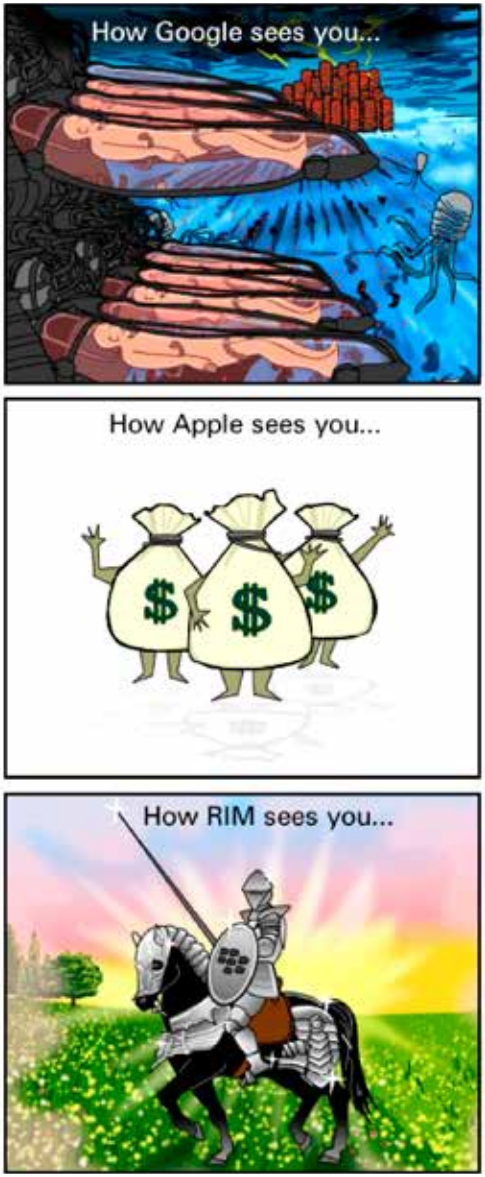
Las redes sociales comerciales y masivas como Facebook y Twitter definen sus relación con las usuarias según sus modelos de negocios. Por ejemplo, en el caso de Twitter Inc. el modelo de negocio es conocido como mercado de datos (data market), para el cual se puede almacenar y vender de vuelta a las usuarias los datos que en principio ellas mismos colocaron allí. En ese mismo sentido, estas plataformas y sus interfaces suelen habilitar la interacción y la recolección de datos de usuarios, orientados hacia la colocación publicitaria más eficiente posible, antes que hacia el desarrollo de comunidades en línea que buscan cubrir y mover sus necesidades de transformación social y política.



Joy of Tech - http://www.geekculture.com/joyoftech/

La recopilación y análisis de datos es cada vez más sofisticada y podemos ver los resultados de esta agregación y su análisis en la forma en que se comercializan y se nos proporcionan servicios cada vez más convenientes. Frente a este contexto en el cual la privacidad es un valor en vía de desaparición, cabe preguntarnos cuales son actualmente las estrategias y tácticas de mitigación y resistencia. Si no podemos sencillamente apagar la computadora y el celular, deberíamos pensar en re-aprender a jugar con nuestras identidades conectadas y ver cómo podemos alterar y modificar nuestras sombras digitales para nuestro gozo, así como para hacerle la vida más difícil a todos los adversarios que hemos listado anteriormente. Las identidades conectadas más apropiadas son las que tienen en cuenta el contexto, los riesgos y deseos específicos de las personas y colectivos que las desarrollan.

Resulta útil pensar en todos los datos digitales que existen acerca de ti como tus rastros digitales. Estos componen una especia de “sombra digital” a la cual vamos agregando más datos cuando usamos herramientas y servicios digitales. Sabemos que las empresas los colectan con la finalidad de analizar nuestro comportamiento y hábitos para vendernos productos y servicios. También sabemos que los gobiernos quieren tener acceso a la mayor cantidad de información posible para controlar, vigilar y/o castigar. Finalmente, personas malintencionadas pueden desear esa información para acosar, chantajear o espiar a miembros de su familia, a sus parejas o simplemente a personas cuyo estilo de vida, ideología o opiniones no son de su agrado.



Joy of Tech - http://www.geekculture.com/joyoftech/

2.4 Incluyendo el género en la privacidad y seguridad digital

Nicole Shepard (2016), en su artículo sobre Big Data y la vigilancia sexual, nos recuerda que "cuando el control de la información de una persona está fuera de las manos de esa persona, también lo es la naturaleza de la transformación potencial". Cita a Manovich, quien identifica tres clases emergentes en nuestras sociedades: "Las que crean datos (conscientemente y generan huellas digitales), aquellos que tienen los medios y poder para recopilarlos y los que tienen experiencia y poder para analizarla. El primer grupo incluye prácticamente todo el mundo que está usando la web o teléfonos móviles; El segundo grupo es más pequeño; Y el tercer grupo es mucho más pequeño todavía".

En este sentido, cabe recalcar que la brecha de género en cuanto al acceso a las TIC sigue siendo fuerte a nivel mundial ya que la comisión broadband del International Telecommunications Union estima que unas 200 millones menos mujeres que hombres con acceso a internet. Además, y sobre todo, si nos fijamos en quién tiene la capacidad de creación, diseño, análisis y beneficio de las TIC y las redes sociales la desigualdad de género resulta abrumadora. Para el estado español, los datos de la Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares del Instituto nacional de estadística español (2016) nos indica que las mujeres en España ya usan mas las redes sociales que los hombres (70.3% de mujeres contra 60.4% de hombres). Sin embar-

go, aunque crezca el número de mujeres que acceden y usan las TIC y redes sociales esto ni significa que ellas se beneficien socialmente o económicamente de este acceso. Aún las mujeres representan una minoría de estudiantes y trabajadoras qualificadas en el sector TIC. Además, hemos podido ver anteriormente como las plataformas comerciales replican las estructuras de poder y discriminación que existen en nuestras sociedades patriarcales. Y, finalmente, otro claro indicio de desigualdad de género consiste en ver que las personas que deciden acerca de la gobernanza de estas plataformas y sacan los mayores beneficios de las redes sociales son hombres blancos y occidentales como Zuckerberg (Facebook), Dorsey (Twitter), Brin y Page (Google), Gates (Microsoft), entre otros.

Incluir el género en la privacidad y la seguridad nos obliga a adoptar un enfoque interseccional - uno que se relaciona con la diversidad de culturas, condiciones sociales, identificaciones de género, orientaciones sexuales, razas, etnias, creencias y otras estructuras de poder que pueden crear desigualdades para los individuos y las comunidades en cuanto a su acceso a las herramientas y prácticas de privacidad y seguridad digital. También nos obliga a mirar a la privacidad y la seguridad desde una perspectiva de género, a través de la cual se tenga una visión amplia de la tecnología, que incluye tener en cuenta las condiciones de producción y las leyes relacionadas con la gobernanza de internet. Todo ello abarca:

1. Reconocer que las brechas de género, la discriminación y la violencia de género son a la vez estructurales y discursivas ya que están profundamente arraigadas en el lenguaje, las narrativas, las definiciones, las estructuras sociales y las leyes. Todas ellas influyen profundamente en las condiciones en las cuales las mujeres acceden y experimentan la tecnología e internet.

2. Entender cómo las mujeres en diferentes condiciones encuentran formas de acceder a las tecnologías, y una consideración hacia cómo pueden protegerse a sí mismas y a otros en ese proceso.

3. Compartir habilidades y conocimientos desde la base para que las mujeres puedan fortalecer su libertad de opinión y de expresión.

4. Recordar que es importante hacer visible las experiencias de las mujeres en la gestión y desarrollo de las tecnologías (no sólo las digitales, sino también las tecnologías de la salud, por ejemplo).

5. Trabajar para permitir una mayor participación de las mujeres en las instituciones que contribuyen a la gobernanza de internet, así como dentro de las empresas y organizaciones que proveen servicios que apoyan nuestro trabajo en red e identidades en línea.

6. Imaginar tecnologías liberadoras que permitan la plena realización y el ejercicio de los derechos humanos, y que se muestren inclusivas de la diversidad, es la responsabilidad de cualquier persona involucrada en la creación de un Internet inclusivo, accesible, descentralizado y neutral, no sólo de las mujeres y las organizaciones que defienden la igualdad y justicia social de género.

Artista Frustrado - http://artista.frustrado.com.br/desenhos/

2.5 Información digital, identidades y género

¿Cuánta información digital (o «datos») existen sobre ti? ¿Qué tipo de datos se han creado sobre tu identidad, relaciones sociales y hábitos cuando utilizas plataformas comerciales - como Facebook o Google - y dispositivos digitales, como un celular o una computadora? ¿Cómo se relacionan y reflejan lo que eres y lo que haces cuando estas conectada o fuera de línea?.

Todas estas preguntas implican que a día de hoy el uso de las tecnologías de información y comunicación (TIC) genera huellas y señas personales que te pueden identificar en la vida material y física. Nos referimos a Información Personal Identificable (IPI) que puede incluir desde tu nombre y apellido, tu dirección, fotografía, numero de seguridad social, número de teléfono, numero de identidad, matriculas, currículum, biométricas varias, etc. Así como a Información Personal Sensible (IPS) como pueden ser tus datos médicos, psicológicos, preferencias sexuales, creencias religiosas. Tu sombra digital está compuesta por tu IPI e IPS y de tus contactos.

No obstante en los inicios de internet las perspectivas que se tenían en cuanto a privacidad y modos de presentarse y construir un conjunto de identidades conectadas eran muy diferentes. Por ejemplo, un dibujo publicado en 1993 en el New Yorker mostraba dos perros conversando sobre el hecho de que en internet nadie sabia que eran perros. Internet era percibido como un nuevo territorio en el cual las personas podían expresarse, comunicarse y relacionarse liberadas del peso de los prejuicios y estereotipos asociados al género, edad, etnicidad, orientación sexual, etc. Se consideraba lógico usar avatares o pseudónimos y navegar combinando identidades variadas. Por todo ello, algunas ciberfeministas vislumbraron en internet nuevas formas de empoderamiento para las mujeres, las disidentes del género y en general para las comunidades marginales o marginalizadas.

Inspiradas por la criatura Cyborg, las primeras en definirse expresamente como ciberfeministas fueron el grupo de artistas australianas VNS Matrix que declararon su existencia en 1991 con el «Manifiesto de la Zorra

Mutante»: "Succionado, absorbido por un vórtice de banalidad... acabas de perderte el siglo XX […] Lo cautivador es la mezcla de fundidos. El contagio ardoroso de la fiebre del milenio funde lo retro con lo posmo, catapultando cuerpos con órganos hacia la tecnotopía… donde el código dicta el placer y satisface el deseo». Les siguieron la red Old Boys Network fundada en 1997 en Berlin compuesto por varias artistas y tecnólogas, quienes organizaron dos congresos ciberfeministas y publicaron las 100 anti-tesis de lo que no es el ciberfeminismo. Ambos colectivos fueron pioneros en generar imaginarios radicales alrededor del ciberfeminismo.

Además, ciberfeministas como Plant (1997) plantearon que el ciberespacio se relacionaba estrechamente con los quehaceres desarrollados y tradicionalmente adjudicados a las mujeres. Las tareas de comunicación y compartir información entre los miembros de las comunidades y familias, así como tejer redes tenía mucho que ver con el género y las mujeres. Otras ciberfeministas como Padilla y Mezquita (2006) o Zafra (2015), además, destacan que no sólo se va habitando, haciendo y tejiendo, sino y sobretodo, cabe la posibilidad de ir deshaciendo y destejiendo género y la red, también desde afuera de las mismas redes. Deconstrucción, ironía, juego, placer, parodia, performatividad, exageración y sobreidentificación son algunas de las actitudes y estrategias usados por estas ciberfeministas para cuestionar las identidades de género y la cultura tecnológica establecida (Salas, 2008).

Wu Ming Foundation - https://www.wumingfoundation.com/

Mary Allen Wikes - https://es.wikipedia.org/wiki/Mary_Allen_Wilkes

El ciberfeminismo social arranca también con fuerza en 1993, desde la Asociación internacional para el progreso de las Comunicaciones que crea el grupo APC-Mujeres. Sus primeros pasos se sitúan en los debates que se celebran a través de listas de correo electrónico acerca de las posiciones que se quieren trasladar a la IV Conferencia Mundial de Mujeres. El proceso culmina en 1995 en Pekín donde un equipo de 40 mujeres de 24 países asegura la formación y apoyo a 1.700 usuarias creando además un espacio electrónico con información de las ONGs presentes disponibles en 18 idiomas y que contabilizó más de 100.000 visitas en su página web (Núñez Puente, 2008). Por primera vez y sin estar físicamente presentes mujeres de varios países pudieron hacer un seguimiento on-line de los trabajos de la Conferencia y expresar sus opiniones en tiempo real.

En esa misma conferencia se reivindica también por primera vez el derecho a la comunicación como uno de los Derechos Humanos básicos y como elemento estratégico para el cambio social que las mujeres exigen en la lucha por la igualdad de derechos: "Podemos invertir la relación de fuerzas porque tenemos los contenidos y las prácticas. La clave es valorarlas. Es imperativamente necesario tener una estrategia ofensiva, incluso agresiva. No tenemos nada que perder y todo a ganar. Es así como podremos cambiar la imagen en los media: en tanto que actrices (autoras, conceptoras, artistas, realizadoras...), en tanto que sujetos (vida cotidiana, política, trabajo, violencias....), en tanto que público" relata Joelle Palmieri, mediactivista y creadora en 1996 de la red "Penelopes" en Francia. Otra iniciativa pionera en la experimentación audiovisual con contenidos feministas emitidos a través de programas de televisión vía Internet, así como del uso del software libre para la publicación abierta de contenidos on-line.

De 1995 a 2005 proliferan la creación de redes y espacios ciberfeministas en ese nuevo territorio llamado ciberespacio. Entre muchos proyectos encontramos en Italia porticodonne.org, en Canadá cybersolidaires.org,

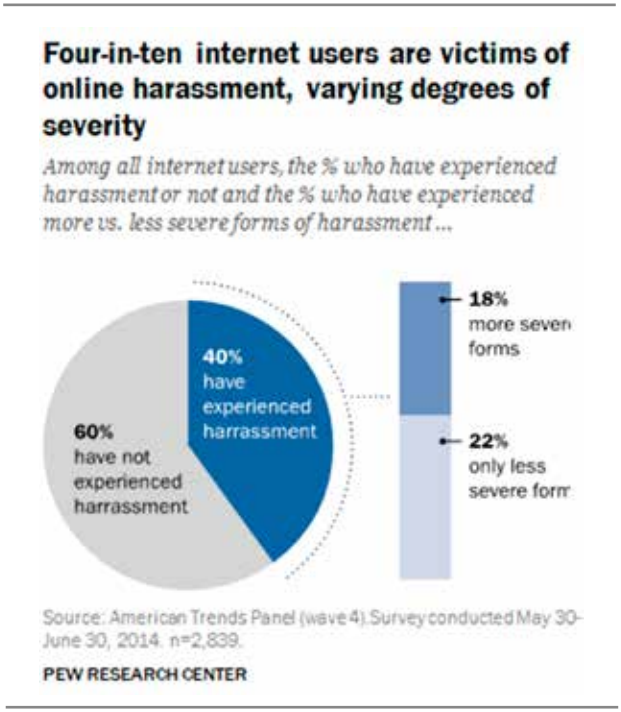
en España mujeresenred.net, espacio de mujeres de Pangea, Ciberdona, en Francia penelopes.org, en Europa del Este Witt project, en África Famafrique.org y en América Latina Rima.org. Muchas de estas iniciativas no se limitan tampoco a un uso pasivo de herramientas tecnológicas desarrolladas por otros (hombres blancos, ricos y a menudo misóginos llamados Steve Jobs o Marc Zuckerberg), sino que contribuyen al diseño y desarrollo de sus propias herramientas tecnopolíticas fomentando su autonomía y soberanía tecnológica (Hache. 2014). Es así que encontramos desde medios comunitarios y radios y televisiones on-line, desarrollos varios de software libre, contenidos compartidos con licencias libres, servidores autónomos hasta portales de noticias con sistemas de publicación abierta.

La posibilidad de modificación del código, del contenido y de los formatos es una de las bases para la apropiación de las herramientas libres, dotando a las mujeres de libertad para la participación y la transformación social (Vergés et al., 2014). Tal y como dice Laurence Rassel en una entrevista con Donestech (2008) sobre la relación entre feminismo y software libre: "En francés, un sistema operativo se llama "système d'exploitation", así qué lo mínimo de lo mínimo es ser dueñas de nuestro propio sistema de explotación y poder modificarlo!".

Por todo ello, como ya apuntó Boix (2006), los ciberfeminismos se proponen hackear al patriarcado y plantean la lucha contra las violencias de género como nexo. Trabajan como nodos interconectados entre distintos ámbitos, lugares y espacios, así como entre la diversidad de feminismos. En este sentido, los esfuerzos iniciales de las ciberfeministas se concentraron en visibilizar las violencias contra las mujeres en sus múltiples formas y lugares. Como fenómeno universal y, a su vez, con particularidades específicas como las de ciudad Juárez. También se dedicaron a denunciar y dar altavoz a casos que iban ocurriendo, así como alertar de la impunidad que generaba la inacción de los gobiernos y comunidades al respecto. Además, a través de las redes, ayudaron a coordinar las distintas luchas contra estas violencias. Actualmente, además de seguir luchando y trabajando para visibilizar y comunicar información sobre éstas violencias, a raíz de las desigualdades y violencias que operan en el propio ciberespacio, las ciberfeministas estamos enfrascadas en visibilizar y luchar, también, contra las violencias de género que operan on-line.

2.6 Violencias de género

La declaración de las Naciones Unidas (1993) sobre la Eliminación de la Violencia contra las Mujeres la define como "cualquier acto de violencia basada en el género que resulta en, o puede resultar en daño o sufrimiento físico, sexual o psicológico en la mujer, incluyendo la amenaza de tales actos, la coerción o la privación arbitraria de la libertad, ya sea que ocurra en la vida pública o privada".



Pew Research Center - http://www.pewinternet.org/2014/10/22/on-line-harassment/

Respecto a la legislación española esta indica que "la violencia de género no es un problema que afecte al ámbito privado. Al contrario, se manifiesta como el símbolo más brutal de la desigualdad existente en nuestra sociedad. Se trata de una violencia que se dirige sobre las mujeres por el hecho mismo de serlo, por ser consideradas, por sus agresores, carentes de los derechos mínimos de libertad, respeto y capacidad de decisión. Por ello, la Constitución Española incorpora en su artículo 15 el derecho de todos a la vida y a la integridad física y moral, sin que en ningún caso puedan ser sometidos a torturas ni a penas o tratos inhumanos o degradantes. Además, continúa que estos derechos vinculan a todos los poderes públicos y que sólo por ley puede regularse su ejercicio.

La campaña Dominemos las tecnologías que se celebra desde hace 12 años a nivel global define la violencia en contra de las mujeres como "cualquier hecho que resulta en daño y afecta de manera desproporcionada a las mujeres. La causa principal de violencia en contra de las mujeres son las relaciones de poder desiguales entre los hombres y las mujeres en casi todo los aspectos de la vida. Algunos ejemplos de violencia en contra de las mujeres incluyen la violencia doméstica, violación y hostigamiento sexual". Esta campaña es coordinada desde el programa mujer de la Association for Progressive Communications (APC) y nos recuerda que la violencia de género on-line atenta contra el Artículo 19 que estipula que toda persona tiene derecho a la libertad de opinión y de expresión. Este derecho incluye el de no ser molestado/a a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

A nivel autonómico, la junta de Andalucía cuenta desde 2015 con el primer protocolo de detección e intervención a víctimas de ciberdelicuencias de género que define esta como "la violencia de género que

se lleva a cabo aprovechando las TIC. Normalmente coexiste la violencia usando las TIC con la violencia por vías "tradicionales" o "analógicas", pero la intensidad, la repercusión a nivel relacional y psicológico, las diferencias a nivel de protección y judicial, y las peculiaridades de la prueba electrónica, hacen que siempre sea necesario en la actualidad tener presente el enfoque específico de la Ciberdelincuencia de Género" (Instituto Andaluz de la Mujer, 2015). Este protocolo busca facilitar la detección y registro de este tipo de violencias así como incorporar en las actuaciones de los y las profesionales vinculadas al Instituto Andaluz de la Mujer que realizan atención directa, pautas específicas de actuación ante la Ciberdelincuencia de Género.

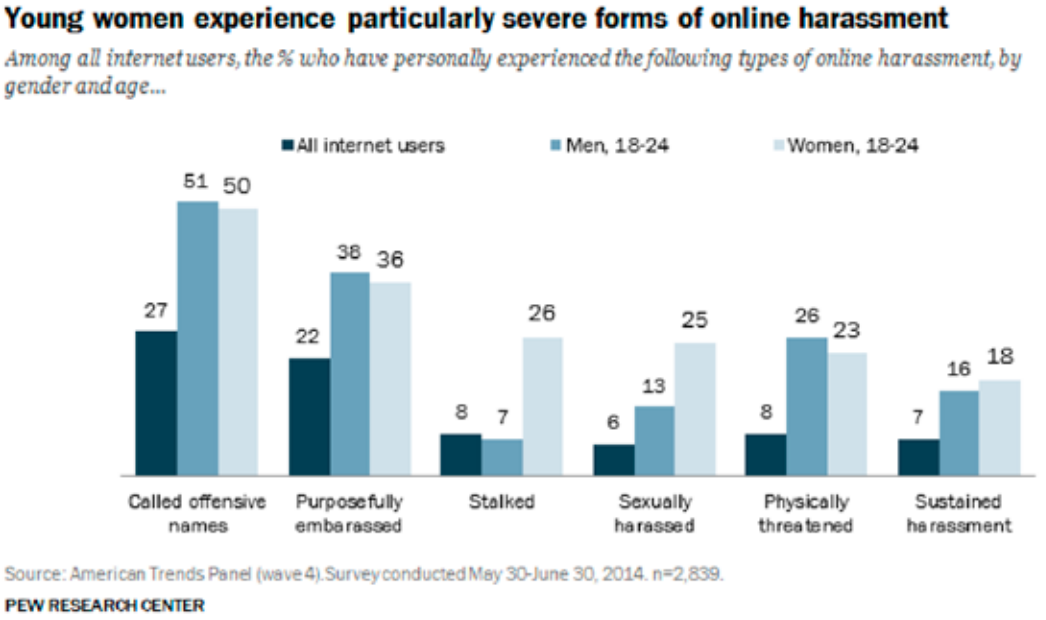
Como hemos podido ver, se cuentan con varias definiciones y marcos legales que definen la violencia contra las mujeres. Pero contrariamente a la Junta de Andalucia, muchos marcos legales aun no han querido o sabido abarcar las nuevas formas de violencia de género ocurriendo en el marco del uso de TIC y las redes sociales. Los cambios legislativos son lentos y a menudo faltan recursos para poder formar las personas trabajando en instituciones públicas acerca de como detectar estas violencias, como entender su impacto en las vidas de las personas que las sufren y/o como hacer que se aplique la ley cuando esta existe.

Esto significa que a veces los representantes de la ley no saben cómo operar porque las plataformas donde operan estas violencias dependen de la legislación de otro país. Otras veces invisibilizan o minimizan estas violencias instando las mujeres a sencillamente desconectarse de Twitter o apagar el móvil para dejar de recibir amenazas por esos canales. También se dan demasiado a menudo campañas públicas que revictimizan las personas sujetas a estas violencias haciendo recaer en ellas la responsabilidad de lo ocurrido. Un caso paradigmático es el tratamiento que se hace del envío de imágenes íntimas instando las mujeres en no hacerlo cuando no se pone de la misma manera el foco en los agresores que comparten esas imágenes sin el consentimiento de las personas.

Antes de profundizar en algunas de las características de las violencias de género on-line queremos destacar que estas operan dentro de una brecha digital respecto al acceso, uso, desarrollo de tecnológicas que sigue impactando de manera mucho más fuerte las mujeres, así como las minorías culturales y las comunidades marginalizadas.

2.7 Violencias de género on-line

Las TIC permiten acceder y producir información, crear canales de comunicación multi-direccionales (uno hacia varias y varias hacia varias) y también permiten producir narrativas y representaciones del mundo. Las TIC suman por lo tanto una dimensión informativa, comunicativa y representativa al mismo tiempo.



Pew Research Center - http://www.pewinternet.org/2014/10/22/online-harassment/

Danielle Citron indica que aunque las definiciones del acoso cibernético varían, a menudo concuerdan en la intención sustancial de infligir sufrimiento emocional de manera lo bastante persistente como para ser entendido como un curso de conducta mas que un incidente aislado. Las intenciones son las de crear en los sujetos blanco de estos ataques vergüenza, represión, depresión, auto censura, soledad y/o miedo usando el discurso y su expresión en espacios conectados (Chemaly, 2014).

Esta definición subraya el componente escrito o hablado del discurso como vehículo por donde se transmite las violencias de género on-line. Esta visión tiene como problema relacionado el de tener que decidir cuál es discurso legítimo y cual no es, a la hora de emprender una visibilizacion de las violencias de género y saber cómo abordarlas.

Sarah Jeong (2015) nos habla de “El Internet de la Basura”. Ella sugiere otra perspectiva para analizar el

acoso cibernético. Para ella, "el acoso existe en dos espectros a la vez - uno que se define por el comportamiento y uno que se define por el contenido. Si miramos el acoso solo como contenido, nos fijamos en las "amenazas de muerte" a un extremo del espectro, y "mensajes molestos" en el otro extremo. De esta manera, el debate termina girando en torno a los derechos civiles frente a la libertad de expresión, ¿dónde está la línea entre los comentarios molestos y el peligro inminente? ¿Entre los chistes y las amenazas?. El comportamiento es una lente mejor y más útil para mirar el acoso. Vemos la fuga de números de Seguridad Social, la publicación de fotografías privadas, el envío de equipos SWAT a direcciones físicas, y el asalto físico a personas".

Esta reflexión nos lleva a pensar el acoso cibernético y las violencias de género dentro de un marco analítico que valora los comportamientos y los impactos y consecuencias diferenciadas que pueden tener según quien las perpetra, quien las sufre y en qué contexto social, cultural, económico, político están teniendo lugar. Analizar el discurso es importante pero tiene que tenerse en cuenta también los efectos que se dan entre el o los emisores y las personas que reciben esos ataques.

Un marco analítico para entender de qué maneras las violencias de género on-line impactan consiste en tener en cuenta cómo la experiencia del acoso es vivida a nivel:

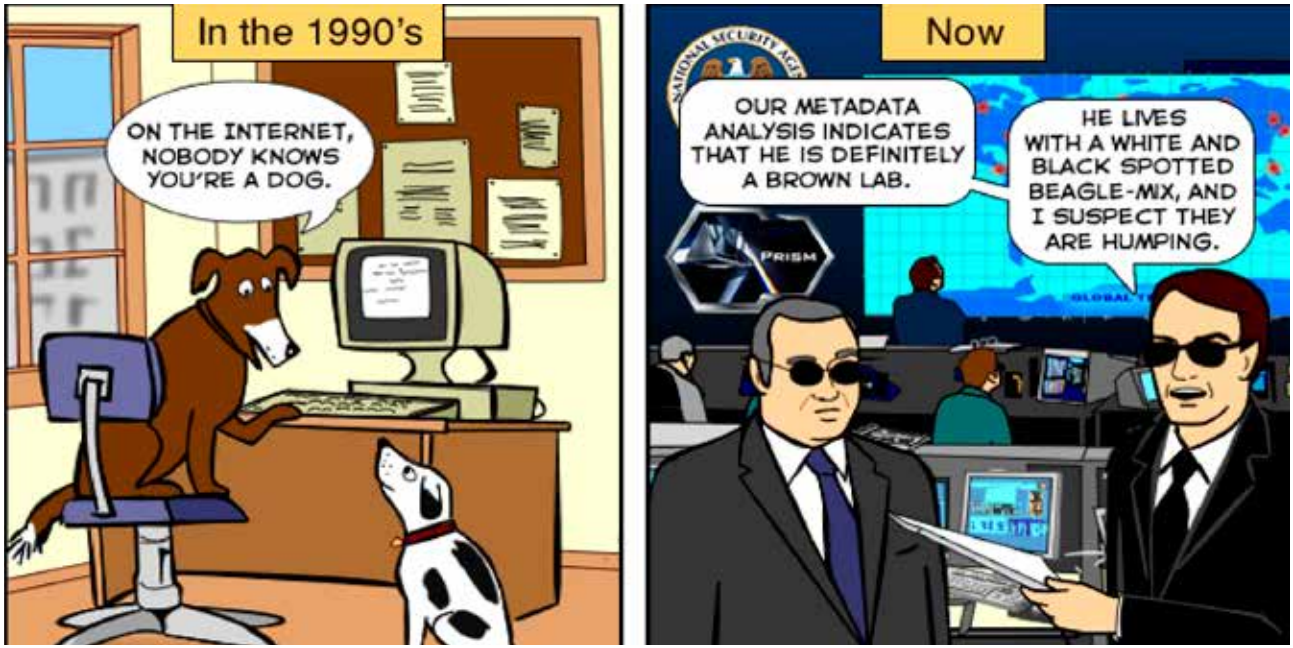
- **Subjetivo** ya que cada persona interpreta y entiende de manera diferenciadas los mensajes, discursos y violencias implicadas.

- **Corporal** porque el miedo, la depresión, la frustración o la rabia tienen consecuencias a nivel físico y generan secuelas psicológicas. Así como porque los ataques en linea pueden fomentar ataques físicos y psicológicos en la vida física subrayando la interacción existente entre lo on-line y lo off-line.

- **Social y cultural** porque vivimos en sociedades patriarcales regidas por normas y valores que influencian como las personas entienden o interpretan las violencias de género.
- **Político y legal** porque la gobernanza, transparencia y modificación del código detrás de las plataformas de redes sociales está en manos de las empresas que lo desarrollan. Y también porque muchas de las instancias legales encargadas de aplicar las legislaciones vigentes y las medidas de protección son violentas y patriarcales.
- **Poder y privilegios** ya que las personas tiene grados de autonomía y opciones diferenciadas frente a situaciones de acoso o violencia.
- **Mediático y narrativo** porque los imaginarios detrás de las violencias de género están presentes en todas las capas de nuestras sociedades. Los tropos culturales se vuelven estereotipos y prejuicios que alimentan más discriminaciones y situaciones de injusticia social.

Todo ello determina los impactos de las violencias de género en nuestras subjetividades, autoestima, salud física y emocional, oportunidades educacionales, laborales, estatus social, libertad de expresión, cooperación y movimiento de las personas que sufren una violencia de género o acoso cibernético.

Pasamos a detallar otros rasgos fundamentales que diferencian las violencias de género mediadas por las TIC de las violencias de género en general. Por un lado, lo referente a la temporalidad y extensión de las violencias de género. Por el otro, una reflexión en torno al anonimato y la libertad de expresión en relación a éstas violencias. Finalmente, un apunte sobre los tropos y el sexismo.



Joy of Tech - http://www.geekculture.com/joyoftech/

2.8 Temporalidad y extensión de lo que se comparte

Un fenómeno asociado a las violencias y acoso usando las redes sociales on-line tiene que ver con su temporalidad. Pueden darse situaciones en las cuales el acoso se de manera casi permanente, 24 horas 7 días a las semana. Esto profundiza y agrava las consecuencias de la violencia, haciendo casi imposible para las personas agredidas poder desconectarse y reconstruirse.

A esta situación se suma el hecho de que internet no olvida. Esto significa que cuenta con una arquitectura que hace fácil replicar contenidos y alojarlos en lugares varios. Se conoce el efecto Streisand como un fenómeno de Internet en el que un intento de ocultar o acallar cierta información fracasa o inclu-

so acaba resultando contraproducente y, así, provocando una mayor difusión de lo que se pretendía silenciar. En la Unión Europea exista una ley desde 2014 que regula el "derecho al olvido" en internet. Este implica que los buscadores como Google tienen la obligación de eliminar de sus listas de resultados aquellos enlaces que violen ciertos derechos de una persona ciudadana, a petición de esta. No obstante sigue siendo un proceso difícil de llevar a cabo y muchos contenidos de violencia de género aun no se contemplan oficialmente dentro de este marco legislativo.

Además, el internet y más concretamente la world wide web, donde se referencian y sindican los contenidos para que estos puedan ser encontrados por los motores de búsqueda, ha completamente cambiado la escala de lo que compartimos. Cualquier contenido subido a la red puede ser potencialmente encontrado y visto por cualquier otra persona que se conecte. Esto hace que las audiencias puedan ser locales, regionales, nacionales o internacionales. En general los contenidos que subes serán visto por tus contactos si es que prestan atención a tus publicaciones. De la misma manera existen estrategias y tácticas varias para mejorar el impacto de lo que se publica en internet y conseguir volverlo viral. Eso también se aplica a redes y foros especializados en los cuales las personas usuarias comparten y difunden contenidos que fomentan o documentan violencias de género. Una agresión filmada y subida a internet, al poder ser vista por otras personas, perpetua el ciclo de violencia revictimizando la persona sujeto del ataque y exponiéndola a nuevas formas de violencias. De la misma manera esta extensión global permite a los agresores juntarse en redes coordinadas, o no, sumando sus acciones violentas y amplificando sus consecuencias negativas.

2.9 Anonimato y derecho a la libertad de expresión

El derecho a la privacidad y el anonimato son fundamentales para todas las personas que usamos internet. Sin el derecho al anonimato se pone el peligro el derecho y la libertad de expresión. Todas necesitamos el derecho a expresarnos libremente y para muchas personas ese derecho requiere de ciertos niveles de privacidad o anonimato, sea por encontrarse en regímenes autoritarios, sea por la necesidad de protegerse, sea por experimentar con su subjetividad, sea por poder expresar puntos de vista impopulares. Cuando hablamos de libertad de expresión no incluimos en este el discurso de odio y el discurso peligroso que apelan a la violencia contra otras personas sea por su género, raza, opción sexual, diversidad funcional o su condición social. Las legislaciones internacionales y nacionales varían muchísimo en cuanto a lo que puede quedar tipificado como delito respecto a la libertad de expresión, y queda fuera de este manual poder profundizar en estos matices.

VNS Matrix - https://vnsmatrix.net/

No obstante, queremos apuntar que no creemos que la vía para solucionar las violencias de género on-line pase esencialmente por prohibir el anonimato en internet o recurrir a mas censure y ataques a la libertad de expresión. Entendemos que la privacidad y el anonimato son necesidades vitales para todas pero que estas son sujetas a relaciones asimétricas de poder. No contamos todas con los mismos privilegios y opciones y no estamos en un pie de igualdad a la hora de poder expresarnos libremente y de forma anónima en el internet. La cara oscura radica en el hecho de que muchos maltratadores se esconden y se aprovechan del relativo anonimato que pueden brindar las redes sociales. Eso hace que sean a menudo muy difíciles de identificar o que su identificación dependa de la voluntad de las plataformas comerciales que gobiernan esas redes.

2.10 De los tropos al sexismo y machismo normalizado en las redes sociales

Las TIC y las redes sociales contienen narrativas y representaciones del mundo que se basan en la producción y circulación de tropos. Los tropos son unidades culturales que funcionan como analogías, por ejemplo, la idea de que existen princesas y que viven

en castillos es un tropo recurrente a través de la historia y este se repite en multitud de cuentos y historias varias. Pero los tropos pueden volverse estereotipos. Por ejemplo si hay princesas y viven en castillos se dice a menudo que estas necesitan ser salvadas de algo o alguien y estos estereotipos pueden volverse prejuicios ya que las personas pueden creer que las mujeres son débiles y frágiles y necesitan de un hombre que las rescate. De los prejuicios podemos expandirnos rápidamente hacia la discriminación y el sexismo y machismo normalizado.

Hoy en día existen varios proyectos que se dedican a estudiar como la producción de narrativas en internet sigue produciendo tropos y estereotipos que sientan y reproducen el machismo y el patriarcado. Un ejemplo es el programa en internet de Anita Sarkasian llamado Feminist Frequency y que se dedica a analizar estos tropos en el cine, las series y los vídeojuegos. Otro ejemplo es el programa (e)stereotipas, conducido por Catalina Ruiz-Navarro y Estefanía Vela que también se dedica a desmontar tropos y estereotipos.

Hasta aquí, y a grandes rasgos, hemos introducido las redes sociales en relación al género. En las siguientes secciones nos adentraremos aún más en las violencias de género on-line, es decir las violencias mediadas, facilitadas y/o amplificadas por las redes sociales. Con ello buscamos mostrar qué está pasando para después, en una segunda parte, poder identificarlo y conocerlo en más detalle y vislumbrar algunas tácticas y estrategias para contrarestarlo.

Cosmopolitan Magazine 1967.

3. SOBRE LAS VIOLENCIAS DE GÉNERO ON-LINE: ¿QUÉ ESTÁ PASANDO?

3.1 Heteropatriarcado y machismos: de las viejas estructuras a las nuevas redes sociales

Desde los feminismos se han realizado grandes esfuerzos para visibilizar la relación entre el patriarcado y las violencias machistas. Además ya se han conseguido grandes logros y generar acciones para ir erosionando el heteropatriarcado y hacer frente a las violencias de género. También, desde entrado el siglo XXI, gobiernos y administraciones públicas han empezado a atender al problema de las violencias de género y han elaborado leyes y actuaciones contra la violencia de género, en Andalucía también e incluso más que en otras comunidades autónomas. Sin embargo, de momento, resultan claramente insuficientes pues el patriarcado sigue fuertemente anclado en nuestras estructuras y, con ello, la violencia de género no disminuye (Vergés, 2012; FRA, 2014). Incluso peor, siguen reproduciéndose y adaptándose a nuevos ámbitos y nuevas formas de relacionarse afectivamente, tal y como la violencia de género en las redes sociales que, aunque a priori pueda parecer más inocua para las mujeres por ser menos física, puede resultar de mucho más alcance y mucho más dañina a largo plazo.

¡Dominemos la tecnología! APC - https://www.apc.org/es/project/%C2%A1dominemos-la-tecnolog%C3%ADa

En este sentido, la inercia heteropatriarcal y machista tan poderosa de antaño, sigue anclada en nuestras estructuras, ejerce violencia contra las mujeres y personas LGTBIQ y dificulta la transformación de género de nuestra sociedad en su conjunto. Además, los machismos también se han actualizado, incluso más rápidamente a las nuevas tecnologías y redes sociales. Allí, reaccionan ejerciendo más y nuevas violencias también contra las mujeres empoderadas y las feministas que los cuestionan. Por ello sigue siendo crucial el fortalecimiento del feminismo en nuestra sociedad en su conjunto y, específicamente, de los ciberfeminismos que actúan en red y en las redes.

EnRedadas, por el arte y la tecnología - https://enredadasnicaragua.blogspot.com.es/

Aunque hace más de una década que las redes sociales se implantaron en España, con un uso que va in crescendo, y en plena era del big data, resulta sorprendente los pocos datos que tenemos para analizar y diagnosticar con exactitud la prevalencia de las violencias de género en España y Andalucía en la actualidad, aunque también a nivel internacional. Ello es tremendamente grave, e incluso podría incurrir en violencia institucional por omisión en la prevención e investigación de las violencias de género (Bodelón, 2015), porque facilita la impunidad ante las agresiones, así como su justificación y reiteración. Por falta de datos públicos, oficiales y disponibles las violencias de género ejercidas on-line se pueden ver como puntuales, accidentales, casos aislados de depravados o, incluso, fácilmente negables. Esto dificulta visibilizarlas y diagnosticarlas con exactitud, así como darnos cuenta de que se trata de violencias sistémicas, persistentes y profundamente arraigadas en nuestra cultura y estructuras, como las violencias de género en el mundo físico. Además, resulta especialmente grave ante el auge de los neomachismos que están cuestionando con fuerza los últimos avances políticos en materia de género, así como a las mujeres y feministas que trabajan para ello.

Así, ninguna administración pública en España ha generado datos oficiales, públicos, sistemáticos y a lo largo del tiempo para permitir un análisis adecuado de las violencias de género on-line o internet en general. Tampoco las principales redes sociales comerciales implantadas a nivel global han generado informaciones sobre ello, a pesar de, como se ha visto, comercializan con nuestros datos y lo que compartimos libremente por internet como personas usuarias. Por todo ello, sólo nos cabe acudir a investigaciones parciales, limitadas pero tan necesarias, por parte de la academia, instituciones públicas españolas e internacionales, periodistas y, sobretodo, colectivos y organizaciones feministas. En este apartado pues, intentaremos arrojar algunas luces sobre qué está pasando sobre este fenómeno creciente de las violencias de género on-line, especialmente para el caso español y andaluz, pero con apuntes internacionales. Sin, embargo, previamente, plantearemos una breve reflexión con algunos datos, en torno a la seguridad, el género y los riesgos cuando hablamos de redes sociales.

3.2 Poder tener relaciones digitales libres y seguras

Si atendemos al género y la seguridad, y aprovechando que nos situamos en el traspaso de lo antiguo a lo nuevo, se da una paradoja a sobre la percepción de inseguridad y uso de espacio público que podría aplicarse también al ciberespacio. El miedo a la agresión no siempre se corresponde con lo que ocurre en la realidad y esto aparece de forma clara si tenemos en cuenta el género (Pérez Tejera, 2012). Las mujeres seguimos teniendo más miedo a ser agredidas que los hombres, también on-line (Henson et al., 2013, Pereira y Matos, 2016). Además tenemos más miedo a los desconocidos cuando son los conocidos y los más cercanos quienes más nos agreden. De hecho seguimos renunciando a ciertos espacios públicos cuando la mayoría de violencias contra nosotras se ejercen en los espacios privados. Ello puede ser debido a que la seguridad percibida, también para quién utiliza las redes sociales y tecnologías, se apoya más bien en procesos de socialización fuertemente sesgados y estereotipados de género. Así, lo privado resulta para ellas y lo público para ellos, la familia y las tareas reproductivas para ella, mientras que las tecnologías y las tareas productivas para ellos, la dependencia y el control para ellas y, en cambio, la independencia y el descontrol para ellos, y así sucesivamente en formato binario.

Esto se constituye como un elemento más de las estructuras patriarcales de nuestras sociedades y tiene importantes consecuencias para la sociedad y para las mujeres. Así, las mujeres, no sólo reportamos mayores niveles de inseguridad, vulnerabilidad y miedo al crimen, sino que somos víctimas de restricciones sociales y espaciales debido a ello, a su vez, reflejo y reproducción de la opresión social y roles de género. Esto limita nuestra libertad de acceso y de movimiento en el espacio público on-line y el mundo de las tecnologías. Constantemente recibimos mensajes alarmantes de que las redes sociales y las tecnologías son peligrosas para nosotras, esencialmente masculinizadas y potencialmente violentas, de manera que, incluso se nos culpabiliza de estar ahí y de esa manera cuando somos agredidas, en vez de dedicar recursos a erradicar la cultura de la violación y la violencia y perseguir a los verdaderos culpables de limitar nuestros movimientos, también on-line.

Take Back The Tech! APC - https://www.takebackthetech.net/

No se trata de dejar de tener relaciones digitales, sino de poder tener relaciones digitales libres y seguras. Sigue siendo cierto e importante que minimicemos riesgos en el mundo virtual siendo conscientes que, como se ha visto, la sociedad sigue siendo patriarcal y necesitamos poner atención y herramientas para garantizar el derecho a la privacidad, valorando que compartimos on-line y como mejorar la seguridad de nuestras acciones. Sin embargo, deberíamos erradicar las violencias de género atacando y cambiando los comportamientos de quienes las ejercen, no de quienes las sufren ni limitando la libertad de expresión y exposición de las personas, especialmente de las mujeres y otras personas LGTBIQ.

3.3 Acerca de los riesgos en las redes sociales on-line

El tiempo que dedicamos, especialmente las y los adolescentes, a internet y las redes sociales cada vez es mayor. En España, según los últimos datos del INE (2017), incluso es mayor el uso de redes sociales por parte de las mujeres que de los hombres. Un 70.3% de mujeres utilizan las redes sociales, como facebook, twitter, tuenti o similares, frente a un 60.4 de hombres. La brecha digital de género entre niños y adolescentes es prácticamente inexistente y su uso de internet es prácticamente universal, aproximadamente un 95% de menores utiliza internet. Sin embargo, pese a su creciente importancia tenemos aún pocos datos públicos sobre el uso de redes sociales y, sobre todo, respecto a lo que ocurre en relación al género.

Entonces, con el incremento de uso de internet y de las redes sociales, las relaciones sociales se ven mediadas en aumento por las nuevas tecnologías, así como las relaciones afectivas. Una vez más, no existen datos públicos y sistematizados al respecto. El negocio de las webs de citas on-line va en auge y es una muestra de la creciente intervención de las redes sociales en las relaciones sexo-afectivas (Constantini, 2016). Sin embargo, compartir nuestra información sexo-afectiva en este tipo de plataformas también tiene sus riesgos, no sólo por la posibilidad de que las webs sean crackeadas, sino también porque dejamos nuestras vidas afectivas en manos de plataformas comerciales, así como nuestra defensa en caso de violencias de género. Por ello es crucial, sobre todo para las mujeres, ser conscientes de la importancia de cuidar nuestra privacidad.

Este incremento de exposición y relación a través de las redes sociales y, en menor medida, del contacto físico, también puede comportar mayores posibilidades de sufrir agresiones y violencia on-line. El estudio de Donoso-Vázquez y Rubio (2014) expone que los y las adolescentes consideran que los espacios virtuales se prestan más a la violencia que el cara a cara (84%). Los adolescentes son moderadamente conscientes de que ciertas acciones conllevan un riesgo asociado de padecer violencia,

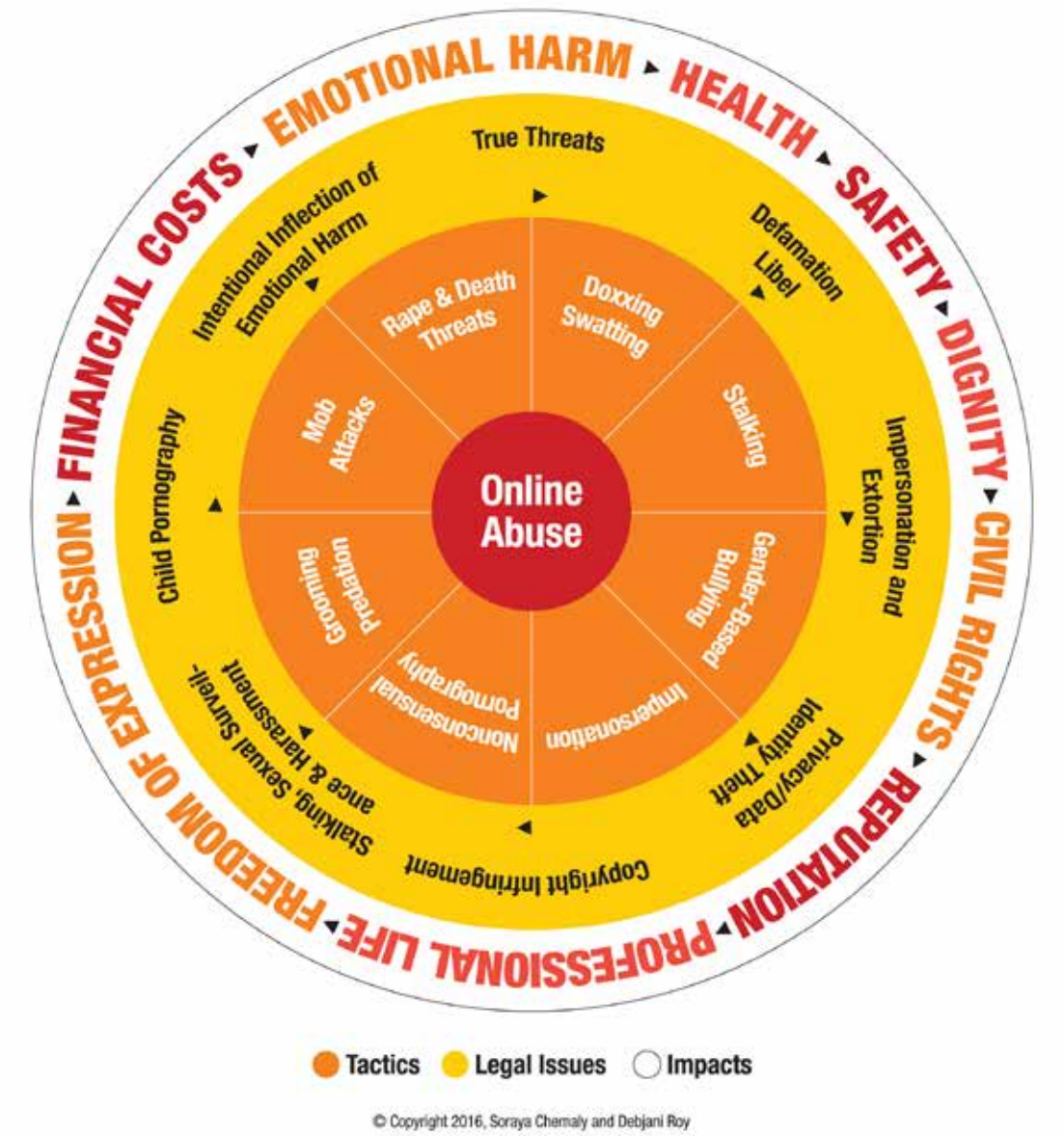
Ayuntamiento de Sevilla.

pero son más conscientes de ello las chicas que los chicos. Las acciones consideradas de más riesgo según Donoso-Vázquez y Rubio (2014) serían: poner información personal en las redes sociales y chatear con personas desconocidas, seguido de tener un perfil abierto en las redes y publicar vídeos personales y, en menor medida mostrar fotos. De todas formas, cabe recordar, si no hubiera agresores dispuestos a utilizar indebidamente estas fotografías y contenidos en la red no existirían personas agredidas. Es decir, acceder a ciertos espacios virtuales y compartir ciertas informaciones nunca debería ser utilizado para culpabilizar a las personas agredidas ni negarles su agencia. De hecho, algunas campañas alarmistas también pueden generar efectos de género contraproducentes que apartan a las mujeres de algunos espacios virtuales. Las mujeres y personas de colectivos LGTBIQ también deberían poder habitar libremente los espacios públicos on-line.

3.4 Algunas luces sobre la incidencia de las violencias de género on-line

Las pocas investigaciones internacionales sobre violencias on-line recogidas por el Women's Media Center en las estadísticas del Speech project (s.f), aunque mayormente provienen de estudios más amplios sobre cyberbullying en general, contienen informaciones relacionadas con las violencias de género. Además los diversos estudios difieren en porcentajes por países, año de publicación e, incluso, definiciones, pero coinciden en algunos aspectos y tendencias respecto a las violencias de género on-line relevantes para esta publicación. La mayoría de violencias on-line las sufren las mujeres y buena parte de ellas son violencias de género. Los participantes en chats y juegos con nicks en femenino reciben más mensajes amenazadores y con contenido sexual. La mayoría de agresores son hombres y gran parte de éstos son conocidos por estas mujeres, mayormente se trata de sus parejas o exparejas. Finalmente, anotar que las personas del colectivo LGTBIQ también resultan fuertemente agredidas por las violencias on-line basadas en género, tres veces más que las personas heterosexuales.

En Europa, según una investigación europea que analizaba la violencia de género para todos los países EU-28 (FRA, 2014), el 11% de las mujeres europeas había sido víctima de violencias en internet (por web, correo electrónico o móvil). Este estudio señala, además, que un 21% de las mujeres que habían experimentado este tipo de violencia, lo sufrió más de dos años e, incluso, un 23% tuvieron que cambiar de correo electrónico y/o número de teléfono. Es necesario señalar que más del 70% de las mujeres que habían experimentado violencias on-line también habían sufrido al menos una forma de violencia física o sexual por parte de su pareja. Además, el mismo estudio señala que este tipo de violencia afecta a las mujeres jóvenes en particular.



Women's Media Center Speech Project - http://www.womensmediacenter.com/speech-project/

Ciberseguras - http://ciberseguras.org/

Si no hacemos urgentemente nada al respecto estas inercias patriarcales no van a desaparecer y van a incrementar pues los datos alertan que el fenómeno es grave entre adolescentes. Según una investigación de la delegación del gobierno para la Violencia de género (Díaz-Aguado et al. 2014) a un 32.5% de las adolescentes y jóvenes españolas entre 12 y 24 años les habían tratado de controlar a través del teléfono móvil y el 20% había comprobado cómo utilizaban sus contraseñas dadas con confianza a sus parejas, para supervisar sus actividades on-line. A un 6% les habían suplantado la identidad utilizando esas contraseñas dadas. A un 4,3% le habían difundido mensajes y fotos sin su consentimiento por internet o a través del móvil. Casi un 12% había sido intimidada por mensajería móvil y hasta un 10% había sido acusada de provocar la violencia sufrida. También, el estudio de Donoso-Vázquez y Rubio (2014), que aplicó el cuestionario de violencias de género 2.0, alerta que un 40% de adolescentes han observado alguna o varias veces estas violencias, aunque sólo vivido en un 10%. Cuando han sido víctimas, sobre todo, han recibido insultos, se han sentido controladas en las redes sociales y les han revisado las llamadas de móvil. Datos más avanzados relacionados con este último estudio con adolescentes, también destacan que las violencias on-line también se ejercen para imponer relaciones basadas en el amor romántico y la heteronormatividad, que incluye la presión hacia un canon de belleza heteronormativo y la heterosexualidad obligatoria (Vilà, 2016)

3.5 Agresiones sexuales y pornografía no consensuada

Aunque hay muy pocos datos al respecto, el último informe Europeo del Instituto europeo para la igualdad de género (EIGE, 2017) alerta de la incidencia de la pornografía no consensuada. Por un lado, encontramos el porno de venganza, donde el agresor a menudo es la expareja que obtuvo las imágenes y vídeos durante la relación o, incluso, crackeando su ordenador y busca hacer daño a la mujer a través de la humillación y vergüenza pública , incluso en el mundo real. La investigación al respecto estima que el 90% de las víctimas de porno de venganza son mujeres y que el número de casos crece, así como crecen el número de webs dedicadas al intercambio de porno de venganza.

Coding Rights - Tactical tech - https://www.codingrights.org/webinar-derechos-sexuales-y-la-violencia-en-linea/

El mismo informe también señala otra práctica aún más perversa y creciente de pornografía no consensuada que consiste en el registro y difusión (incluso en directo) de agresiones sexuales a mujeres (EIGE, 2017). Otros informes internacionales recogidos en la compilación de investigaciones y estadísticas del Speech project (Women's media center, s.f) señalan que, además, la mayoría de amenazas de compartir pornografía no consensuada on-line se materializan y que un 48% de las víctimas son molestadas después de que alguien vea esa pornografía no consensuada. Cabe añadir, como apuntan Henry and Powel (2015), que aunque los vídeos y fotografías tomadas durante agresiones sexuales no sean finalmente difundidas por internet parece que crece también el fenómeno de su uso para el continuo acoso y agresión de las mujeres, como la extorsión sexual, donde la amenaza de compartir imágenes previas el abuso sexual se convierte en recurrente en el tiempo. Las víctimas son muy conscientes que una vez la imagen se vuelve viral es muy difícil garantizar que sea borrada.

El reciente caso de los San Fermines Pamplona en el 2016, muy a nuestro pesar, es una muestra de agresión sexual a la vez que de pornografía no consensuada. 5 sevillanos fueron acusados de violar a una joven de 18 años en grupo, lo grabaron en vídeo y lo compartieron por whats app en los grupos llamados Manada y Peligro. Además, al investigar el caso se les atribuye otra agresión sexual en grupo en Pozoblanco (Andalucía). A nivel internacional tenemos noticia

Hamara Internet - Digital Rights Foundation - https://digitalrightsfoundation.pk/work/hamara-internet/

de casos penosos donde se han compartido agresiones a través de servicios de difusión en redes sociales, como una violación a través de facebook live sin que hubiera denúncia de ninguna de las 40 personas que lo vieron (La Vanguardia, 2017). Otras notícias internacionales muestran como las agresiones compartidas en las redes se apremiaban con cientos de favoritos y apoyo de otros hombres como ocurrió en Brasil (Barrena, 2016) , Perú (Periodista digital, 2017) o en Suecia (BBC, 2017). Más aún, la viralidad con la que se ha propagado un contenido, la difusión en diferentes canales y redes sociales compartida por muchas personas, aunque pueda responder a una acción para reclamar justicia, acaba aumentando la victimización de la persona agredida, cuando en realidad compartir este tipo de vídeos puede y debe ser penado.

La pornografía no consensuada, y más cuando implica este elevado grado de agresión, es un reflejo de la cultura de la violación que aún persiste en nuestras sociedades patriarcales. Las mujeres se convierten en objetos, se las agrede y encima se las culpabiliza de la agresión por simplemente estar ahí o estar de esa manera, por ser mujeres. Los agresores, a menudo impunemente por las autoridades y el resto de la sociedad, libremente cometen los hechos y los reproducen y retransmiten en red. Y lo más grave de ello es que lo hacen con el orgullo de saberse actuar de acuerdo con la cultura dominante que sigue siendo machista y patriarcal. Por eso muestran sus trofeos a su manada de hombres, conocidos o desconocidos, en forma de mujeres ensangrentadas, humilladas, insultadas, agredidas, violadas. Y esos y otros hombres lo apoyan, animan, comparten y viralizan de modo que las víctimas siguen sufriendo casi eternamente debido al mayor alcance geográfico y temporal cuando se comparte on-line.

3.6 Control y agresión on-line a mujeres vocales y a feministas

Otra de las grandes expresiones del patriarcado y del control machista sobre las mujeres que merece atención específica lo constituye el ataque directo a las mujeres empoderadas y a las feministas, a los feminismos y a sus logros. Nuevamente, los pocos datos e investigaciones que existen nos alertan de la gravedad de esta cuestión. Según la recopilación de datos del proyecto Speech watch (Women's media center, s.f.), , 2/3 partes de las mujeres periodistas reportan experimentar amenazas, abuso sexista, intimidación y acoso al realizar su trabajo. Un 21% reportan que sus cuentas son vigiladas y un 20.3% que han sido crackeadas. Además, un 25% de las amenazas que reciben estas mujeres periodistas e, incluso, sus familiares, se realizan on-line. Un reciente estudio de Gardiner et al. (2016) en The Guardian que buscaba responder a la pregunta de si las mujeres eran más atacadas en los comentarios que los hombres lo confirma. De las 10 personas más

atacadas e insultadas de su periódico 8 eran mujeres. También destaca que las personas LGTBI y no blancas tienden a recibir ataques. Además, es también más elevado el número de mensajes abusivos cuando las noticias tratan de violaciones y feminismos, así como en secciones muy masculinizadas como los deportes o la tecnología). Algo parecido le ocurre a las mujeres que despuntan en el deporte, las artes o las que están alcanzando elevadas cotas de poder como, por ejemplo, las mujeres que se dedican a la política. Recientemente las mujeres políticas del Estado Español, desde Ada Colau, hasta Anna Gabriel, Cristina Cifuentes o incluso Susana Díaz han sufrido graves insultos sexistas como "puta", "golfa", "fea", "zorra", "guarra" etc… por las redes sociales on-line que solo se explican por el hecho de ser mujeres, pues ni siquiera comparten partido ni ideología.

Digital Rights Foundation - https://digitalrightsfoundation.pk

Al igual que antaño, además, una de las estrategias machistas, fundamentadas en el heteropatriarcado, ha sido desprestigiar y atacar los feminismos y a las feministas y disidentes de género y sexuales. Como apunta Momoitio (2014) este ataque organizado en las redes, aunque aparente que no, se realiza para evitar que nos reconozcamos sujetos oprimidos y para que no actuemos conjuntamente tampoco ahora. Como ejemplo de ello, Momoitio (2014) nos recuerda los casos vividos en Pikara Magazine, como el de Alicia Murillo con el proyecto del cazador cazado o de Emi Arias con las tetas y los toros. Por ejemplo, el cazador cazado de la sevillana Alicia Murillo buscaba mostrar, denunciar y combatir el acoso callejero sexista hacia las mujeres. Sin embargo, paradójicamente, youtube la acusó de intimidar, acosar y amenazar después de la solicitud de un grupo de cibermachistas organizados y retiró todos sus vídeos. Aún hoy Alicia Murillo sigue recibiendo cientos de mensajes insultándola. Algo parecido con insultos de todo tipo como "zorra", "puta", "feminazi", "gorda", "amargada", "ojalá os violen", etc, así como incluso amenazas de muerte tipo "feminazi muerta, abono para mi huerta", "algo malo pasa en este país si Barbijaputa no ha sido asesinada aún", las reciben periodistas y tuiteras feministas como la conocidísima @barbijaputa, June Fernández de Pikara Magazine, Jessica Fillol de Locas del coño o Anita saarkesian de Feminist Frequency, que denunció el sexismo en los videojuegos y sus acosadores, incluso, crearon un videojuego que consistía en dar golpes en su rostro hasta que sangrara.

Las plataformas mediáticas y las redes sociales no siempre reaccionan prontamente y adecuadamente ante los ataques machistas a mujeres y feministas. Incluso, en demasiadas ocasiones, los acaban protegiendo. Como apunta Momoitio (2014) este fue claramente el caso de la página de facebook "Pues te violo", que no fue retirada en su momento a pesar de numerosas denuncias feministas. Algo parecido ocurre con tantos comentarios de noticias, páginas de facebook, cuentas de tuitter, etc., que no son retiradas o, si lo son, solo después de grandes esfuerzos por parte de las feministas.

En cambio, las políticas de publicación de diversas plataformas acaban actuando como censuradoras de las mujeres, las personas LGTBIQ, las feministas y sus reivindicaciones, así como les limitan su agencia. Recientemente, en el 2017, Facebook censuraba el monólogo feminista "No solo duelen los golpes" de la jienense Pamela Palenciano y penalizaba la página spanish revolution. Ya en el 2013 había censurado páginas feministas españolas tan relevantes como memes feministas o feministas ácidas. También la página mejicana "no quiero tu piropo, quiero tu respeto". Páginas como facebook, aunque tienen la última palabra al respecto, responden así a las denuncias en masa de neomachistas, de manera que, en realidad, los acaban protegiendo e, incluso, alentando.

Además, plataformas como Facebook limitan la agencia de las mujeres y el derecho sobre su propio cuerpo. Las imágenes de mujeres desnudas o en topless en actos reivindicativos sí son censuradas como en el caso de Mariana Pizarro. En el 2014 el beso de amor entre dos mujeres lesbianas también fue censurado en Facebook. Incluso, algunas plataformas caen en el absurdo de censurar a madres amamantando a sus bebés, por considerarlo contenido obsceno. El primer caso de censura en facebook que salió a la luz fue en Chile en el 2011 y desde entonces se habían denunciado más de 400 casos. Una muestra más del control sobre el cuerpo de las mujeres que parece que, al menos para el caso de Facebook y gracias a las campañas de mujeres parece que podrá revetirse prontamente.

3.7 Los agresores apoyados on-line por los neomachistas

Los machistas también son muy activos en las redes sociales. Aunque no siempre sus actuaciones son tan extremas, sus comentarios y argumentos sirven de base, justifican e, incluso, animan demasiadas agresiones a mujeres y, también hacia personas del colectivo LGTBIQ y otros colectivos minorizados. No hay más que ver algunos de los comentarios que aparecen ante noticias sobre mujeres asesinadas por sus parejas o ex parejas que defienden el agresor y culpabilizan a la víctima. Un claro ejemplo de ello seria el reciente caso del tuit de Jose Alberto ante el tuit del ayuntamiento de Málaga respecto al feminicidio en Mora. El agresor apuntaba “algo haría la puta de ella para acabar así” (Periodicoclm, 2017). Los machistas, además, no sólo agreden a las mujeres sino a cualquier persona que salga de sus cánones de género y orientación sexual. Por ello también son comunes las agresiones a personas de colectivos LGTBIQ. Un ejemplo, en forma de juego on-line,sería el “ass hunter” que, después de la denuncia del observatorio contra la homofóbia, fue retirado de la tienda google en 2015 (Vargas, 2015)

En relación a ello y en general ante las violencias de género, los neomachistas, sobre todo, actúan en lo políticamente correcto (Donoso-Vázquez y Prado, 2014). Afirman que la mayoría de denuncias de las mujeres son falsas, que la igualdad ya se ha alcanzado, defienden el derecho a la vida para cuestionar el aborto, afirman que la violencia no tiene género, se muestran en contra del matrimonio homosexual y de las leyes de igualdad y contra la homofóbia, etc, de hecho, se presentan como víctimas de las nuevas legislaciones de género, así como de las que llaman feminazis. Sin embargo, generar este tipo de discursos es extremadamente grave y contribuye a justificar las violencias, y más cuando se es diputado del congreso español. Toni Cantó en el 2013 envió diversos tuits poniendo en duda la violencia de género e, incluso, afirmando que la mayoría de denuncias de las mujeres eran falsas. Por suerte, ante la evidencia de los datos públicos al respecto y de haberse equivocado tuvo que disculparse (Requena, 2013).

Power & Control

1 Doxxing
2 Harmful Language
3 Surveillance
4 Kyriarchy
5 Isolation
6 Using Intimidation
7 Sexual Coercion & Harassment
8 Gaslighting

Modeled from the popular Power & Control Wheels that have been created for discussing domestic and intimate partner violence, we extend those conversations to the violence we have experienced and survived online. We have described the violence we have experienced and seen online.

The Digital Alchemist - http://femtechnet.org/wp-content/uploads/2016/06/Nov10_Control-and-Respect-Wheels-Document.pdf

Los neomachismos son un fenómeno reaccionario. En este sentido, aparecen como reacción a los logros feministas de las últimas décadas, sobre todo, ante la posibilidad de perder los privilegios que antaño el machismo les había otorgado por el simple hecho de haber nacido hombres cis y comportarse de acuerdo a la masculinidad hegemónica y heteronormativa. Por ello, se caracterizan por cuestionar los recientes avances en materia de género y las legislaciones que se han conseguido, pero también por atacar ferozmente, a menudo en forma de machitrols, a las mujeres empoderadas y feministas, incluso creando un nuevo concepto para llamarlas feminazis.

La distribución viral de imágenes como los memes pueden servir a la causa neomachista y las consiguientes violencias de género (Burgos et al, 2014). Existen célebres memes con frases tremendamente machistas como “mujer déjame que te diga lo que tienes que hacer”; “Machista dios que las hizo inferiores”, “stop feminazis”, “cuidado! La violencia no tiene género, la mujer también mata”, y tantos más que pueden consultarse libremente en machirulos. com.

Sin embargo, y finalmente, los pocos datos disponibles que tenemos al respecto confirman las dificultades, pasividad o incluso violencias institucionales al respecto. Según un estudio de ACP (2015) publicado en GenderIT , un 60% de las agresiones on-line que se reportan no son investigadas y solo en 1 de cada 3 agresiones reportadas generan alguna acción al respecto por parte de los proveedores de internet o plataformas donde ocurre la agresión. Además de la omisión en generar datos para poder estudiar y diagnosticar con precisión el fenómeno de las violencias de género on-line, la falta de acciones por parte de los responsables públicos y privados de la comunicación on-line para perseguir y castigar estas violencias genera impunidad para los agresores y sus grupos de apoyo, haciendo que el problema persista, se agrande y se agrave.

Por todo lo expuesto pues, es preciso hacer frente a todo tipo de agresores y ejecutores de violencias de género off y on-line, impliquen violencia física o no, extrema o no. Las consecuencias no solo son graves para las mujeres y las personas LGTBIQ, sino para el conjunto de la sociedad que no consigue erradicar la lacra machista y patriarcal de sus estructuras básicas y, por tanto, acabar con tantas violencias. Por ello es imprescindible el compromiso de las autoridades en aras de generar datos y políticas que permitan hacer frente a las violencias de género, también on-line. Además, es necesario el compromiso de las plataformas on-line, así como de la sociedad en su conjunto para avanzar hacia unas prácticas on-line libres de violencias . Solo así internet y las redes sociales on-line resultaran realmente accesibles y permitirán su uso y disfrute por parte de todos, también de las

mujeres y feministas que, como se ha visto, resultan aún fuertemente perjudicadas.

Hasta aquí, además de presentar las redes sociales en relación al género, hemos arrojado algunas luces, en forma de datos y ejemplos, sobre lo que está ocurriendo on-line cuando atendemos a las violencias de género. En la siguiente parte entraremos en la identificación y detalle de las diversas violencias de género on-line, así como apuntaremos algunas acciones a tomar y recomendaciones para cuidarnos y hacerles frente.

PARTE 2. DESGRANANDO LAS VIOLENCIAS DE GÉNERO ON-LINE Y APUNTANDO A ACCIONES, INICIATIVAS Y RECOMENDACIONES PARA LA AUTODEFENSA

1. INTRODUCCIÓN

En esta parte pretendemos mostrar el panorama de violencias de género on-line que se están dando actualmente en internet. Presentamos éstas violencias con cierto detalle para facilitar su reconocimiento y alertar del impacto que pueden tener para las personas, especialmente las mujeres. Analizamos sus especificidades, así como de qué maneras se pueden solapar y complementar. Los ataques pueden enfocarse a insultar/avergonzar, calumniar/desprestigiar, silenciar/censurar y chantajear/extorsionar, así como basarse en procesos sociales y herramientas tecnológicas más o menos sofisticados. A su vez, presentamos ejemplos de acciones e iniciativas que responden o contrarrestan estas violencias, así como recomendaciones que incluyen prácticas de privacidad, seguridad digital y autocuidados on-line.

Empezamos introduciendo, a grandes rasgos, a los principales protagonistas de las violencias de género on-line. Seguidamente nos adentramos en los distintos tipos violencias de género on-line. En primer lugar, un conjunto de violencias más generalistas como el acoso de género on-line, el discurso del odio de género o el discurso peligroso de género. Seguidamente, las estrategias más comunes empleadas por los agresores como el mansplaining, flamear, doxing, robo de identidad, acusaciones falsas, gaslighting y swating. Después detallamos los que se basan en insultar, avergonzar y minar la autoestima como slut shaming, fat shaming o inducir a prácticas dañinas, así como nos adentramos en las violencias de género que se basan en el chantaje y la extorsión como la sextorsion, pornografía no consentida, los packs, el grooming y el reclutamiento para fines sexuales. Finalmente, entramos específicamente en los ataques que conllevan un fuerte componente tecnológico como los programas espías, crackeo de cuentas, ataque a servidores, ataques a sitios webs y perfiles feministas o bombeo en google. Para acabar, incluimos unas recomendaciones generales y transversales de autocuidado y autodefensa, así como algunas otras para distintos ámbitos y para hacer frente a las violencias de género on-line.

Anotamos que esta parte no pretende generar miedo, parálisis o rechazo al uso de las tecnologías sino más bien permitir entender las especificidades de las violencias de género on-line, cómo detectarlas y conocerlas y, sobre todo, como implementar prácticas tecnológicas y sociales que contrarresten estas violencias y creen una internet más segura, libre y amigable para todas las personas.

Finalmente, apuntar que, en cualquier caso, debes informarte sobre las leyes y políticas de tu comunidad y país en relación a internet, la libertad de expresión, el derecho a la privacidad y contra el acoso en línea y fuera de línea,a sí como las normativas de igualdad y de género existentes. Estas leyes no existen en todos los países, y cuando existen no se enmarcan o no se aplican del mismo modo.

Lelacoders Donestech - https://donestech.net/lelacoders

2. VIOLENCIAS DE GÉNERO ON-LINE Y AUTODEFENSA AL DETALLE

2.1 En torno a los agresores y perpetradores de violencias de género on-line

Como hemos apuntado anteriormente, las violencias de género, también on-line, se caracterizan por ser ejercidas mayormente por los hombres. Además, gran parte de los agresores resultan ser conocidos de las víctimas, a menudo sus parejas o exparejas. Ello dota a este tipo de violencias de una enorme perversidad, pues quién debería quererte o haberte querido acaba atacándote y agrediéndote.

Más allá de ello, su carácter estructural y sistémico, implica que las violencias de género se asientan en las bases de nuestra cultura y sociedad. Con ello los agresores se justifican y encuentran demasiados aliados entre otros miembros de su ideología machista que ejercen este tipo de violencias con demasiada impunidad, especialmente on-line. Éstos serían comúnmente conocidos como trols machistas o machitroles.

Los trols machistas o machitroles son usuarios con pensamientos y actitudes machistas que habitan la red y que de forma intencional se presentan para acosar a otras personas, principalmente a mujeres o feministas. Son usuarios que hacen uso de la tecnología y las redes sociales para continuamente contactar, fastidiar, amenazar, y/o asustar y su comportamiento no es un incidente aislado si no que es recurrente.

El Machitrol es una especie de cibernauta que se caracteriza por el impulso feroz de atacar a otras personas usando comentarios, gifs e imágenes violentas en la web cada vez que encuentra contenidos feministas en internet. Además de opinar sobre lo que dicen o hacen las mujeres en la red, también inunda el ciberespacio con comentarios machistas, sexistas y misóginos.

Ante esta expresión de violencia digital puedes ignorar o lidiar con los provocadores. Existen dos maneras para lidiar con ellos, una es bloquearlos y luego reportarlos a la plataforma que estás usando. La otra opción es involucrarte. La decisión de qué camino tomar depende de lo que quieras conseguir.

Bloquear trols puede ser efectivo algunas veces y puede permitirte continuar con tu trabajo sin obstáculos, pero si los trols están ensañados con atacarte bloquear no siempre ayuda ya que existen opciones para seguir con la táctica, como crear nuevas cuentas e identidades en línea para acosarte, así como organizar un acoso grupal, como se verá más adelante.

La otra opción es involucrarte con ellos, puedes intentar entrar al plano de una argumentación racional con ellos, intentar avergonzarlos o usar el humor para desinflar sus egos. Por último, puedes crear un enjambre para ahogar su voz, creando una comunidad

de apoyo con aliadas que puedan bombardear con contramensajes al atacante. La eficacia de tu estrategia también dependerá del tipo de perfil de machitrol que esté acosándote. Seguidamente te mostramos algunos de ellos para ayudar a su identificación:

El preocupado: Se trata de un troll que dice estar "a favor de la igualdad" e intenta hacerse pasar por feminista, pero hace comentarios en las publicaciones de mujeres y feministas con la intención de desacreditar y denigrar su presencia on y off line.

El policía bueno: La hipocresía es la especialidad de este troll quien se presenta como seguidor, fan o simpatizante de tu tema o causa, con la intención de enmascarar su hostilidad a través de una "crítica constructiva". Se acerca dando pie a un interrogatorio por un crimen que la víctima nunca cometió y a menudo se dirige a través de sugerencias "útiles" sobre cómo mejorar la apariencia o adoptar un tono más amigable. Un buen ejemplo es cuando una feminista a través de su cuenta de Twitter denuncia la violencia contra las mujeres, entonces aparece el "policía bueno" y empieza una conversación para sugerirle que sea más amigable y menos "violenta", puesto que ella está hablando de violencia, todo ello con la intención de desacreditar su publicación y hacerla quedar mal.

El León marino: Es cuando un extraño no invitado aparece en tu conversación y agrega comentarios o preguntas no solicitadas de forma deshonesta. El León marino siente que tiene la moral política para exigir evidencias y argumentos de peso, cuando él mismo incluye declaraciones mundanas o auto-evidentes, e insiste para que la víctima de su troleo justifique sus opiniones hasta que él esté satisfecho, cosa que nunca va a suceder, puesto que él te está haciendo preguntas desde la mala fe.

Un ejemplo sería cuando haces una publicación sobre cualquier tema que te interesa, por ejemplo comida saludable o consumo responsable, y de la nada aparece este personaje, pidiéndote explicaciones y argumentos sobre tu publicación. Para lidiar con estos trolls, puedes dedicar tiempo a demostrar su falsedad, error y mala intención o evitar dar pie a su acoso, ignorándolos.

2.2 Ciberviolencia de género grupal

Este ataque consiste en muchas personas sincronizadas y coordinadas que emprenden acciones en contra de una mujer o un colectivo feminista. Pueden llevar a cabo una denuncia en masa de su página, perfil o contenidos en las redes sociales para que estas sean cerradas y censuradas. También se pueden coordinar para un ataque distribuido de denegación de servicios (DdoS), causando que una página web no esté disponible para su consulta, o desarrollar conjuntamente otras acciones que veremos más adelante al detalle, como el doxing, el robo de identidad, falsas acusaciones y campañas de desprestigio, discurso de odio y amenazas de muerte.

El Churo y La Libre - https://elchuro.org/nuestro-trabajo/encuentro-internacional-de-ciberfeminismo/

A menudo, el acoso grupal se orienta hacia la mujer que tiene una participación y exposición más pública, ya sea en espacios físicos o en internet, y puede darse en respuesta a nuevos roles, carreras o trabajos que se feminizan o hacia campañas e iniciativas centradas en la igualdad, los derechos sexuales y reproductivos o la justicia social de género. También se han registrado varios casos con mujeres que denuncian situaciones de violencia o agresiones que recibieron dentro o fuera de internet y por ello comienzan a recibir acoso grupal en las redes sociales.

Este tipo de acoso puede silenciar a las mujeres, llevándolas a que se auto-censuren cuando se expresen o directamente cierren sus cuentas en las plataformas donde están recibiendo un acoso grupal. Salir de las redes también puede ser en su momento una adecuada práctica de autocuidado.

Existen grupos identificables en cada país que cuentan con espacios de coordinación variados, más o menos horizontales e informales. Por ejemplo se sabe del uso de forocoches para coordinar campanas misóginas por parte de machitrolls en España, o de los foros “4chan/8chan” y el portal “Reddit” para intercambiar entre las personas que se reivindican como parte de los movimientos “gamergate” y “alt +right” en Estados Unidos. Sus miembros pueden identificarse mutuamente haciendo uso de palabras clave en sus biografías o en los nombres que usan en sus cuentas de redes sociales. También hay que apuntar que las cuentas que se utilizan en estos ataques pueden ser bots (una aplicación de software que ejecuta tareas automatizadas a través de Internet), así como cuentas conocidas como “sock puppet” que son cuentas falsas controladas y compinchadas con intereses manipulativos y de tergiversación.

Durante este tipo de ataques es común que la comunidad alrededor de la persona que está siendo agredida se sume o haga publicaciones en su apoyo o condenando los ataques. Esto a su vez puede llegar a generar que quienes se suman puedan recibir a modo de “rebote” mensajes o ataques por los mismos medios. También puede darse que las personas que quieren ayudar acaben por empeorar la situación al no tener en cuenta el contexto y necesidades particulares de la persona bajo ataque.

Algunas estrategias para contrarrestar estas agresiones consiste en documentarse acerca de buenas prácticas a la hora de prestar apoyo, hablar sobre el acoso grupal que se está viviendo en espacios seguros, producir narrativas y respuestas en las cuales se ponen en evidencian los abusadores o se burlan de los mensajes recibidos, denunciar los perfiles a las plataformas de redes sociales, así como crear mecanismos de bloqueo masivo compartiendo listas de cuentas bloqueadas.

Otra medida útil consiste en conocer tus configuraciones de seguridad y privacidad así como de bloqueo y reporte de contenidos y usuarios en las plataformas

que usamos para expresarnos. A veces también es preferible no bloquear si se da un componente ilegal o de difamación para poder documentar y reportar los ataques.

2.3 Acciones e iniciativas de autodefensa:

- Alerta Machitrol. De Fundación Karisma en Colombia, que consiste en identificar al machitroll y detectar si es rescatable o incurable. A través de esta campaña se está alertando y evidenciando el auge de acosadores en internet. Ver en: https://actua.karisma.org.co/alertamachitroll/

- Zero Tollerance. El colectivo alemán Peng! diseñada como un programa de auto-ayuda de seis pasos para reformar a los trolls ya que estos "necesitan ayuda seria y práctica para superar su sexismo, lidiar con sus problemas de ira y cambiar su comportamiento." Ver en: https://zerotrollerance.guru/

- Block Bot. Aplicación de twitter que bloquea acosadores conocidos y trolls en Twitter para tí. Ver en: http://www.theblockbot.com/sign_up

- Block Together y Sharing block lists. Sirve para compartir tus listas de bloqueo en Twitter. Ver en: https://blocktogether.org/ y https://blog.twitter.com/2015/sharing-block-lists-to-help-make-twitter-safer

Alerta Machitroll Fundacion Karisma - https://actua.karisma.org.co/alertamachitroll/

- Trolldor. Trabaja como una lista de Trolls y está abierta a cualquier usuaria de Twitter. Ver en: https://www.trolldor.com/faq

- HeartMob. Una plataforma para documentar y dar apoyo en tiempo real a personas viviendo acoso en línea. Ver en: https://iheartmob.org/

- Manual Zen. También puedes encontrar en esta sección del manual zen unas recomendaciones para saber como apoyar una persona bajo acoso grupal. Ver en: https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Apoyando_a_otras

2.4 Tipos de violencias de género on-line y autodefensa

2.4.1 Acoso de género on-line

Es un tipo de hostigamiento en línea que se basa en el uso de adjetivos ofensivos asociados a la condición de género o a lo femenino. Este tipo de violencia fomenta la producción de insultos, estereotipos, prejuicios y, a menudo, contenidos gráficos y audiovisuales para comunicar hostilidad hacia las niñas y las mujeres, por el hecho de ser mujeres.

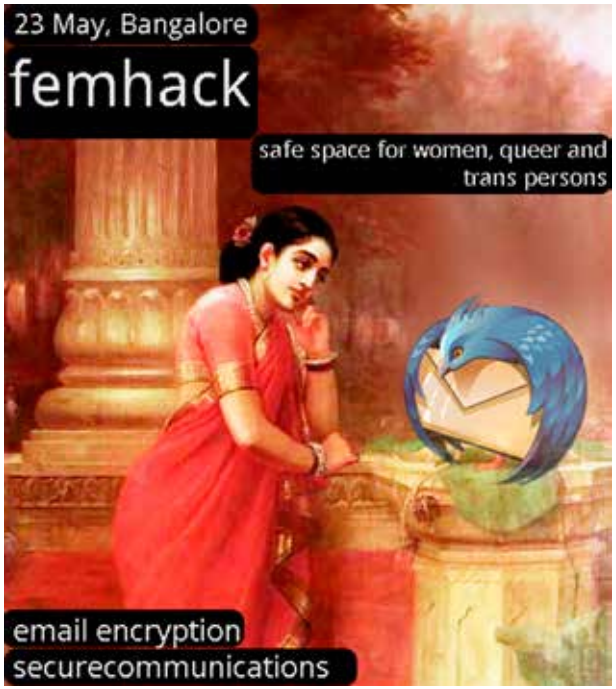
Usualmente los acosadores recurren a frases ofensivas como: “puta”, “zorra”, “feminazi”, “coño”, “gorda”, “histérica”, “seguro anda con la regla”, “mal follada”, “perra”, además de incluir comentarios sobre la apariencia física de mujeres y activistas con el objetivo de cosificarlas y denigrarlas. Este tipo de comentarios y publicaciones a veces sobrepasan los insultos y se tornan en amenazas de violación o feminicidios. Se producen con el fin de intimidar, silenciar y paralizar generando el miedo a expresarse libremente en línea, así como el miedo a estar sola en su casa o a salir a la calle.

Muchas mujeres, activistas y feministas activas en internet, tienen que lidiar con este tipo de violencia, que no es ni nueva ni exclusiva del entorno conectado, pero que en internet y las redes sociales ha cobrado auge. Sin embargo, desde el feminismo y haciendo uso de estas mismas plataformas digitales, se producen datos y documentación de estos ataques, redes de apoyo y solidaridad con las personas bajo ataque así como contenidos. Se realiza a manera de respuesta, incluso utilizando la ironía y la comedia como recurso para ridiculizar a los que nos violentan.

2.4.2 Acciones e iniciativas de autodefensa:

2.4.2.1 Documentar violencias

- Dominemos la tecnología: Una campaña internacional de APC que ha recopilado más de 500 relatos de mujeres y su experiencia de violencia en línea. Ver en: https://www.takebackthetech.net/mapit/main?l=es_AR.
- La wiki de feminismo geek: Una proyecto colaborativo donde se han estado documentado incidentes sexistas, en línea y fuera de línea, en comunidades aficionadas a la tecnología. Puedes ver la línea del tiempo de tales incidentes, además de sus páginas de recursos para aliados de mujeres. Ver en: http://geekfeminism.wikia.com/index.phptitle=Timeline_of_incidents y en http://geekfeminism.wikia.com/wiki/Resources_for_men
- Mujeres, Acción y los Medios (WAM!) analizan las diferentes formas de violencia en línea y han desarrollado un trabajo profundizado acerca de la plataforma Twitter. Ver en: https://women-actionmedia.org/cms/assets/uploads/2015/05/wam-twitter-abuse-report.pdf



Femhack Bangalore.

2.4.2.2 Redes de apoyo y solidaridad

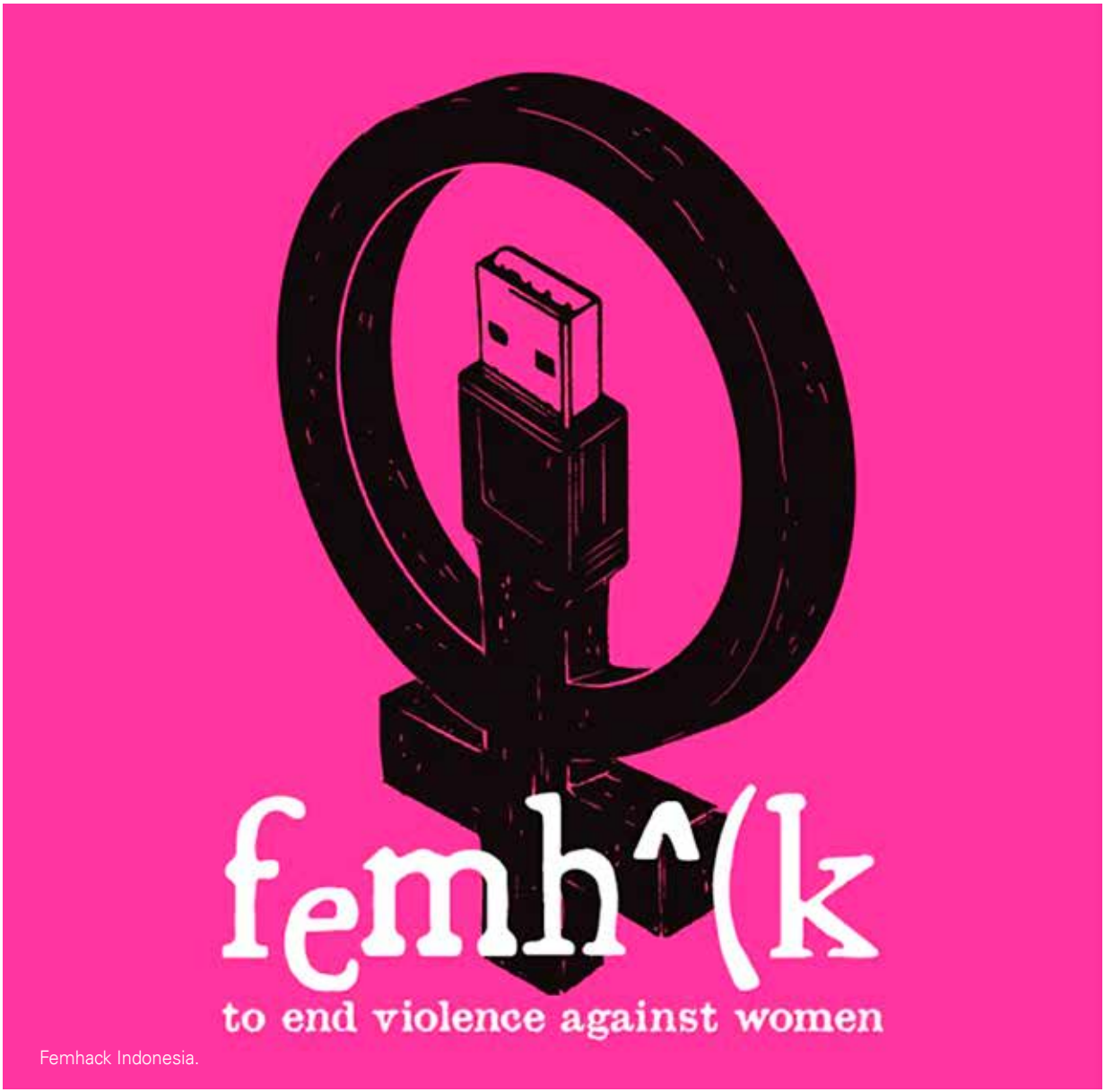
- Digital Rights Foundation Cyberharassment helpline: es un numero de teléfono gratuito mantenido por un equipo de personas que atienden víctimas bajo ataque y les provee con información y recursos para poder mitigar o contrarrestarlos. Se trata del primer servicio de este tipo en Pakistán. Ver en: https://digitalrightsfoundation.pk/cyber-harassment-helpline/
- Crash Override Network: es una red de contención y asistencia para grupos de personas que han estado bajo ataques en línea, y está conformada por personas sobrevivientes de ataques. Estas personas trabajan preventivamente y de forma reactiva con personas bajo ataque para que puedan permanecer a salvo. También les proveen con estrategias para desapoderar acosadores, reducir los daños, y reconstruirse. Ver en: http://www.crashoverridenetwork.com/
- La Iniciativa de Prevención de Abuso en Línea (OAPI): es una organización sin fines de lucro que se dedica a reducir y mitigar el abuso en línea a través del estudio y el análisis de patrones de abuso, la creación de herramientas y recursos antiacoso, y la colaboración con empresas que están haciendo esfuerzos para mejorar el apoyo a sus comunidades. Trabaja en colaboración con Crash Override Network. Ver en: http://onlineabuseprevention.org/
- HeartMob: es una plataforma para documentar y dar apoyo en tiempo real a personas viviendo acoso en línea. Ver en: https://iheartmob.org/

2.4.3 Discurso de odio

Cualquier discurso que trivializa, glorifica o incita a la violencia contra las mujeres es discurso de odio. El discurso de odio incluye expresiones escritas, verbales o visuales de discriminación, acoso, amenazas o violencia contra una persona o grupo por motivo de su género, discapacidad, orientación sexual, etnia o creencia religiosa.

En línea, como en todas partes, tenemos derecho a la libertad de expresión, pero algunas personas usan este derecho para expresar puntos de vista bastante ofensivos sobre las mujeres. Si la expresión es particularmente agresiva, difamatoria o insistente, puede entonces considerarse discurso de odio (Take back the tech, s.f).

El discurso de odio no es libertad de expresión. En la mayoría de los países, el discurso de odio está prohibido cuando incita a la violencia o a acciones perjudiciales contra otras personas, mientras que sólo en algunos también abarca la denigración o intimidación. Teniento en cuenta el artículo 19 del Pacto internacional de derechos civiles y políticos, es posible buscar protección y reparación bajo la ley civil, la ley penal o ambas.



Femhack Indonesia.

Las mujeres que escriben sobre género, entre ellas periodistas, blogueras feministas, o las mujeres que abordan temas en apariencia dominados por hombres, como los vídeo juegos o la política, reciben una cantidad desproporcionada de comentarios inflamatorios y amenazas. Por otra parte, se les ataca no por sus ideas sino por su género, sexualidad y apariencia física, o simplemente porque son mujeres vocales que utilizan sus voces para expresarse y dar a conocer sus opiniones. En estas situaciones, la meta de los abusadores es intimidar y, en última instancia, silenciarlas a través de la censura directa o la autocensura.

2.4.4 Discurso peligroso

Se trata de una expresión particular del discurso de odio que, según lo investigado por la profesora Susan Benesch (2013), tiene una probabilidad razonable de catalizar o amplificar la violencia de un grupo hacia otro. El marco que identifica el discurso peligroso establece cinco variables:

- Cuando el agresor es una figura pública con un alto grado de influencia sobre la audiencia, podría ser un líder religioso, un periodista famoso, un youtuber popular o un profesor de prestigio, etc.
- La audiencia tiene prejuicios que pueden ser fácilmente manipulados y cultivados por el agresor.
- El discurso se entiende claramente como un llamado a la violencia.
- Un contexto social o histórico propicio para la violencia, por una variedad de razones, incluyendo la competencia entre grupos por recursos y/o la falta de voluntad para resolver quejas o episodios previos de violencia.
- Se distribuye por un medio de comunicación muy popular o influyente, por ejemplo porque es una fuente única o primaria de noticias relevantes para el público.

Alguna de las estrategias para contrarrestar el discurso de odio consisten en usar y promover la comunicación activa y no violenta, así como producir activamente contra-narrativas. Crear contranarrativas en línea, o “contestar a conciencia”, busca hacer visibles el sexismo y la violencia de género en respuesta a los ataques y persecuciones en línea. Puede ser una táctica efectiva, creando una sensación de pertenencia y haciendo visible la efectividad de las acciones feministas en línea.

Cuando planeamos un contradiscurso es importante preguntarse a quién va dirigido, cuáles serán los principales objetivos que perseguirá dicho discurso (llamar la atención, cambiar las normas, apoyar a otras, compartir experiencias) y de que maneras se alcanzaran ese objetivo (usando la parodia, el humor, el chequeo fáctico, la llamada a acciones, etc.).

Memes Feministas - https://memesfeministas.wordpress.com/

2.4.4.1 Acciones e iniciativas de autodefensa:

- Sexismocotidiano. Proyecto global para exponer y catalogar episodios de #sexismocotidiano. Ver en: https://twitter.com/SexismoES.

- Byefelipe. Es una cuenta de Instagram que repostea comentarios abusivos de hombres que se vuelven hostiles al ser rechazados. Ver en: https://instagram.com/byefelipe/.

- DistractinglySexy. Una campaña de mujeres científicas después de las declaraciones sexistas del premio nobel Tim Hunt para mostrar cómo se ven ellas #DistractinglySexy. Ver en: https://twitter.com/search?q=%23DistractinglySexy&src=typd.

- La campaña ONU Mujeres en contra de las sugerencias sexistas de las búsquedas de Google. Ver en: http://www.unwomen.org/en/news/stories/2013/10/women-should-ads.

Luchadoras - http://luchadoras.mx/

- GenderIT.org: Un portal que surge del trabajo de incidencia política en tecnologías de la información y la comunicación del Programa de Derechos de las Mujeres de la Association for Progressive Communications (APC). Se desarrolló como respuesta a la necesidad expresada por responsables políticos y defensoras de las TIC de contar con ejemplos de políticas nacionales, de uso de lenguaje no sexista, de recursos de incidencia y de lograr comprender el impacto que pueden tener tanto las buenas políticas públicas como las deficientes. Ver en: http://www.genderit.org/

- El tornillo. El programa El tornillo, un espacio en Youtube3 dirigido por la periodista española Irantzu Varela. Ver en: http://www.publico.es/publico-tv/la-tuerka/el-tornillo

- Feminist Frequency: Este proyecto incluye la serie de video "Tropos vs. mujeres", creado por Anita Sarkeesian y que, junto con Bitch Magazine, examina tropos y estereotipos comunes en el cine, televisión y videojuegos. Algunos vídeos producidos en esta serie incluyen "Mujeres en refrigeradoras", "El principio de Pitufina" y "Personajes femeninos positivos en los videojuegos". Ver en: http://feministfrequency.com/

2.5 Estrategias comunes de los machitrols y algunas respuestas

2.5.1 Mansplaining

Como concepto amplio el mansplaining se da en el contexto de relaciones de poder en el cual una persona privilegiada explica a una persona de un grupo discriminado sus propias condiciones de opresión. Por ejemplo un hombre blanco explicando lo que es el racismo a una persona negra o un hombre cis lo que es discriminación de género a una mujer etc. Una aceptación más restringida se refiere a un hombre que explica a una mujer, de una manera considerada condescendiente y paternalista algo que ella conoce mejor o acerca de lo cual tiene más experiencia.

Esta expresión machista que se da tanto fuera como dentro de internet, comprende una mezcla heterogénea de comportamientos, donde se expresa el menosprecio del hablante por la mujer a la que le supone una capacidad menor de comprensión. También incluye situaciones en las que un hombre monopoliza la conversación con la única intención de jactarse o dejar claro que es más culto que la mujer que lo escucha. Algunos ejemplos es cuando un hombre en el aula de clase o en una conversación en las redes sociales te corta la palabra, se pone a hablar más fuerte que tu o te dice: "Lo que tu quieres decir es…", "Las feministas deberían…", "Eso que cuentas es tu experiencia, pero según", "Me ha gustado mucho lo que dices, pero". Estos comentarios se presentan como consejos, sugerencias sutiles o recomendaciones pero la motivación real no es de mejorar tu comprensión del tema sino de cohibir y corregir las mujeres que se atreven a opinar y compartir sus conocimientos.

2.5.1.1. Acciones e iniciativas de autodefensa:

- (e)stereotipas: Es un proyecto multiplataforma interactivo y feminista, conducido por Catalina Ruiz-Navarro y Estefanía Vela, y producido por Marcela Zendejas, cuyo principal objetivo es comunicar ideas feministas usando la estética del pop y el humor, a través de los espacios que abren las tecnologías digitales. Ver en: https://estereotipas.com/ y https://www.youtube.com/watch?v=02auOuRcvBk
- Persona: Este colectivo feminista utiliza el stand up como plataforma de comunicación para abordar desde el humor y la parodia la cultura machista contemporánea. Puedes ver por ejemplo el trabajo de la la comunicadora argentina Malena Pichot. Ver en: https://www.facebook.com/malenapichot/ y en https://www.youtube.com/watch?v=lz4mLjxXA9I

Ekka hacklab Feminista -https://eskalerakarakola.org/2017/10/18/hacklab-feminista/

2.5.2 Flamear (Flaming)

Como ataque consiste en lanzar mensajes hostiles o insultantes que no tienen la intención de ser constructivos, sino que buscan establecer una posición de autoridad y/o superioridad. Los flames buscan crear disrupción y enzarzar las personas en una telaraña de acusaciones, mensajes enfadados o insultantes. Suelen ser enviados por personas con sentimientos muy fuertes respecto a un tema o por machitrolls centrados en crear disensión, mal rollo o miedo.

Este tipo de comportamiento verbal agresivo es común en muchas comunidades en línea, redes sociales así como plataformas de videojuegos. En muchos espacios conectados los flames sirven para generar un ambiente hostil para las mujeres, personas LGTBIQ y las minorías culturales para que estas abandonen esos espacios (O'Toole, L. L., & Schiffman, 1997). En su aceptación amplia el flame puede referirse a discusiones largas, intensas y acaloradas, sin que necesariamente se intercambien insultos ni discurso de odio. En cualquier caso resulta muy poco amigable para las mujeres y otras colectividades minorizadas y tiene un impacto excluyente sobre éstas. Este tipo de agresión se ha documentado ampliamente en las comunidades tecnológicas, científicas, de software libre pero también en las empresas y entornos de desarrollo tech.

Internet Es Nuestra MX - http://internetesnuestra.mx/quienes-somos

Al ser una estrategia que busca excluir a las mujeres de los espacios públicos en línea, una posible solución sería crear espacios seguros on-line, mixtos o no mixtos, según las necesidades de las personas. Los espacios seguros se basan en acordar medidas básicas que permitan tener un control sobre quienes tienen acceso a los grupos y quién puede ver o comentar qué y cómo. También contemplan el tipo de herramientas y plataformas usadas para informar y comunicar dentro del grupo y se orientan hacia alternativas más seguras y respetuosas con la privacidad de sus usuarias.

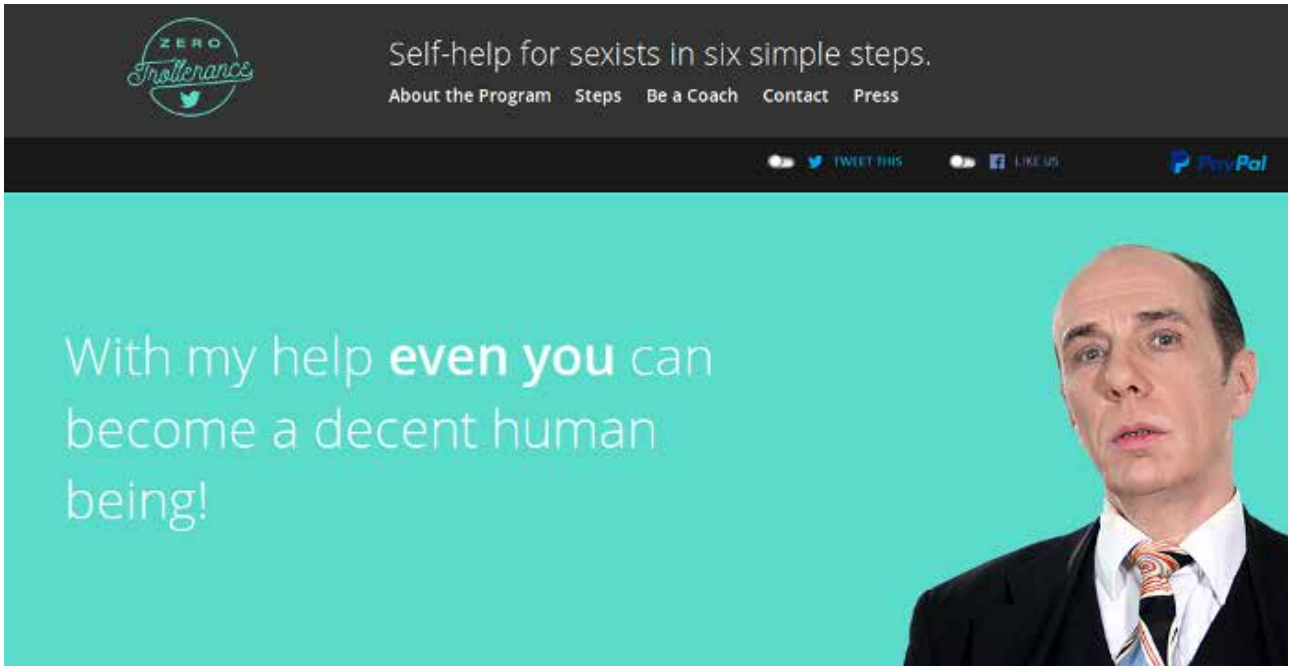
Finalmente, tener una política visible y explícita muestra que se da valor a mantener el espacio compartido como un espacio seguro para sus miembros. También puede ayudar decidir qué nuevas personas deberían poder unirse al espacio seguro y quiénes no. Para asegurarse de que las normas de uso no caen en el olvido o se convierten en un documento que nadie lee, podéis recordar su existencia regularmente y decidir de qué maneras puede cambiar y evolucionar estas reglas y valores compartidos.

2.5.2.1 Acciones e iniciativas de autodefensa:

- Feminismo Geek. Ejemplos de normas de uso por Feminismo Geek, que pueden ser adaptadas a vuestras propias necesidades. Existen para comunidades sólo de mujeres y para comunidades mixtas que incluyen a hombres. Ver en: http://geekfeminism.wikia.com/wiki/Statement_of_purpose/Women-only_communities y en: http://geekfeminism.wikia.com/wiki/Statement_of_purpose/Communities_including_men
- Ada Iniative. Incluye ejmplos de políticas anti acoso para encuentros presenciales. Ver en: http://geekfeminism.wikia.com/wiki/Conference_anti-harassment/Policy
- Wikipedia. Ver sus lecciones sobre la brecha de género y cómo superarla: Ver en: https://meta.wikimedia.org/wiki/Gender_gap
- Advocates for youth. Consejos y estrategias para la creación de un espacio seguro para la juventud LGBTQ: Ver en: http://www.advocatesforyouth.org/publications/publications-a-z/496-tips-and-strategies-for-creating-a-safe-space-for-glbtq-youth
- Women friendly events. Consejos sobre cómo crear y llevar a cabo eventos amigables para las mujeres. Ver en: http://geekfeminism.wikia.com/wiki/Women-friendly_events

2.5.3 Doxear (Doxing)

Doxear es “compilar información detallada acerca de alguien usando fuentes libremente disponibles, aunque también puede implicar usar métodos ilegales para tener acceso a ellas, especialmente cuando se practica para atacar a otras personas” (Hache, 2016).



Zero Trollerance Peng! - https://pen.gg/campaign/zerotrollerance/

La información que es obtenida es de carácter personal y privado y parte del ataque consiste en hacer pública dicha información. El doxeo constituye una violación de tu derecho a la privacidad. La iniciativa Crash Override Network (s.f) menciona que se trata de "los ataques que más predominan, debido a la facilidad con la que puede realizarse y el gran impacto emocional que generan".

Doxear genera un ambiente de intimidación y amenaza ya que no se sabe cuando alguien podría usar estos datos para dañar. Cuando se hace pública la información, en ocasiones la persona comienza a recibir una gran cantidad de mensajes a su número telefónico o perfiles en redes sociales, otras veces se incluyen amenazas donde se incita a ir a la dirección del domicilio o lugar de trabajo de las personas para llevar a cabo escraches o agresiones sexuales.

Los métodos utilizados para doxear incluyen la exploración de archivos, imágenes, bases de datos gubernamentales, directorios de teléfono, motores de búsque-

da y otros recursos de información pública; investigar los perfiles en plataformas de redes sociales, foros y listas de correo. Doxear también incluye buscar información de la persona propietaria de una página web a través del sencillo "who is" (en páginas webs como http://www.whois-search.com/ o similares).

En muchas ocasiones el agresor busca comprobar que la información que hizo pública es verídica, haciendo llamadas o enviando correos. Para valorar el tipo de información que fue expuesta y para qué podría ser utilizada, Crash Override (s.f.) destaca como datos más sensibles el domicilio de una persona, ya que puede llevar a ataques físicos o información adicional relacionada con el trabajo, la escuela o los espacios de ocio. Otros datos especialmente sensibles puede ser el número de seguridad social, el documento nacional de identificación, el número de tarjeta de crédito pero también tu historial médico, tu orientación sexual o tus creencias religiosas o espirituales.

Por todo ello se recomienda antes de decidir cuál es la adecuada respuesta para mitigar los posibles daños hacer una evaluación sobre el nivel de sensibilidad y riesgo que implica el tipo de información que se hizo pública (teniendo en cuenta el momento y contexto así como quien podría aventajarse de ello y de que maneras). El "auto-doxeo" es otra recomendación para prevenir este tipo de ataque ya que nos permite investigar qué tipo de información existe en internet sobre nosotras. Conformemente eso nos ayuda en hacer una revisión general de las configuraciones de seguridad y privacidad de nuestras cuentas así como evaluar si otros datos y contenidos podrían ser dados de baja. Creemos que el auto-doxeo puede tener resultados inesperados, por ello se recomienda practicarlo contando con amigas que podrían ayudarnos en caso de encontrar contenidos inquietantes o dolorosos. También podemos crear alertas asociadas a palabras clave acerca de nosotras para hacer un seguimiento de nuevos contenidos creados relacionados (google ofrece este servicio por ejemplo). Finalmente, podemos hacer una revisión de los "amigos" y "contactos" que tenemos en nuestras cuentas ya que a menudo son a través de ellos que se filtra nuestra información personal.

2.5.4 Robo de identidad

Esta práctica deriva de que alguien consiga de manera maliciosa el acceso a tus datos personales para hacerte pasar por ti. Puedes no darte cuenta de ello porque se accede a tus perfiles de manera sigilosa. Pero también se pueden llegar a crear perfiles falsos o contenidos en las redes sociales en tu nombre sin necesidad de acceder a tus cuentas personales. El robo de identidad suele incluir:

- El acceso a tu información personal: nombre y apellidos, numero de seguridad social, DNI, tarjeta de crédito, dirección física, correo electrónicos, teléfono, fotos, vídeos, contactos.

South Park - https://en.wikipedia.org/wiki/South_Park_(season_20)

- La creación de cuentas, perfiles o contenidos falsos en redes sociales usando datos reales o falsos.
- La utilización para finalidades maliciosas de información personal identificable y/o sensible tuya.

Si notas una actividad extraña en alguna de tus cuentas revisa tus carpetas de correo enviado, basura y spam. Si te avisan de que han intentando acceder a tu cuenta desde otra ubicación, cambia tu contraseña lo antes posible. Pon atención también en los papeles que contienen información personal, manteniéndolos en lugares seguros y privados. Ten en cuenta lo que tiras en tu basura. Puedes también crear perfiles en todas las plataformas conocidas que piden el uso de un nombre real o legal (por ejemplo facebook o linkedin) para impedir que terceros abran perfiles usando tu nombre y apellido.

2.5.5 Acusaciones falsas

Se basan en la creación de ficciones sobre las acciones o la vida de las mujeres, y se dan especialmente en contra de las defensoras de derechos humanos, teniendo consecuencias negativas en sus cotidianidades.

Para ello se crean perfiles falsos y páginas en redes sociales dedicadas a publicar rumores, calumnias o mentiras. Pueden aprovechar el formato de memes para facilitar su viralidad, manipular imágenes y vídeos o publicar datos falsos para la desacreditación social. Generalmente se acusa las defensoras de ser corruptas, estar involucradas con actividades ilegales, mostrarse violentas en sus propias organizaciones, “odiar a los hombres”, entre otras.

La publicación de estas acusaciones falsas puede tener consecuencias de desprestigio social así como también legales. La publicación de contenidos acusatorios puede atraer la atención de la policía e incluso servir como justificación para dar inicio a procesos judiciales en contra de los movimientos sociales. Y en países en los que existen leyes contra la blasfemia, acusar a una mujer de haber cuestionado una institución religiosa puede llevarla a la cárcel y, en casos extremos, significar su asesinato.

Una iniciativa que hace un seguimiento extenso de esta problemática es la Digital Rights Foundation en Pakistan quien estudia el impacto que estas acusaciones tienen en la vida y seguridad de las mujeres y trabaja para proponer nuevos marcos legales y de actuación pública. Ver en: https://digitalrightsfoundation.pk/

2.5.6 Lámpara de gas (Gaslighting)

Este ataque conocido en español como “hacer luz de gas”, consiste en manipular la autopercepción de la otra persona, para hacerla dudar de su propia realidad, su memoria, su percepción y/o su cordura. Puede incluso consistir en la escenificación de situaciones extrañas con el fin de desorientar a la víctima.

Otros ejemplos consisten en mensajes que reciben las víctimas donde se les "informa" de que su pareja les está engañando, o que familiares o compañeras suyas actúan o filtran información a sus adversarios.

Este ataque es una manipulación usada contra las mujeres y defensoras de derechos humanos para hacerlas dudar de su propia red de apoyo, generando en ellas una sensación de aislamiento. Esto también comporta el efecto de extraerlas de sus actividades para que enfoquen sus esfuerzos en atender la situación que se les ha planteado hasta resolver el trasfondo o descubrir la "verdad". Todo ello las imposibilita en continuar con su trabajo o labor activista.

Asaf Hanuka - Mother jones - http://www.motherjones.com/politics/2016/09/katherine-clark-fight-against-internet-trolls-gamergate/

Este tipo de ataque puede ser usado por personas cercanas a la víctima o por personas que no tienen contacto con ella pero que han compilado bastantes datos acerca suyo para planear una manipulación. Por ello la práctica del gas lighting se asocia fuertemente a prácticas de monitoreo, vigilancia e intervención de las comunicaciones.

Si te encuentras bajo un ataque de estas características practica en la medida de lo posible el auto-cuidado. Ten en cuenta los aspectos físicos, psico-sociales y digitales de tu seguridad. Revisa los niveles de confianza que depositas en las personas que te rodean y busca aliadas que puedan darte apoyo a la hora de evaluar si las informaciones recibidas son reales.

2.5.7. Falsa alerta (Swatting)

Se trata de una palabra derivada de las siglas SWAT asociadas al Equipo Especial de Tácticas y Armas de los Estados Unidos de Norteamérica. En Estados Unidos el SWAT es el despliegue de fuerzas armadas que responde a denuncias para la desactivación de bombas y otras amenazas a la seguridad pública. El swatting implica la creación de una situación de violencia en la cual un equipo de personas armadas irrumpen en tu casa pensando que eres una persona potencialmente peligrosa o implicada en actividades ilegales o terroristas.

En su vertiente más soft, también se manifiesta en acciones que grupos misóginos y anti-derechos ejecutan para distorsionar, mortificar o problematizar la vida de las mujeres objeto del acoso. Pueden, por ejemplo, ordenar enormes cantidades de pizza a los domicilios particulares y cancelarlas al momento de su entrega. Ambos ataques buscan causar una interferencia violenta con la vida cotidiana y los espacios íntimos de las personas atacadas.

2.6 Ataques basados en insultar, avergonzar y minar la auto-estima

2.6.1 Slut-shaming

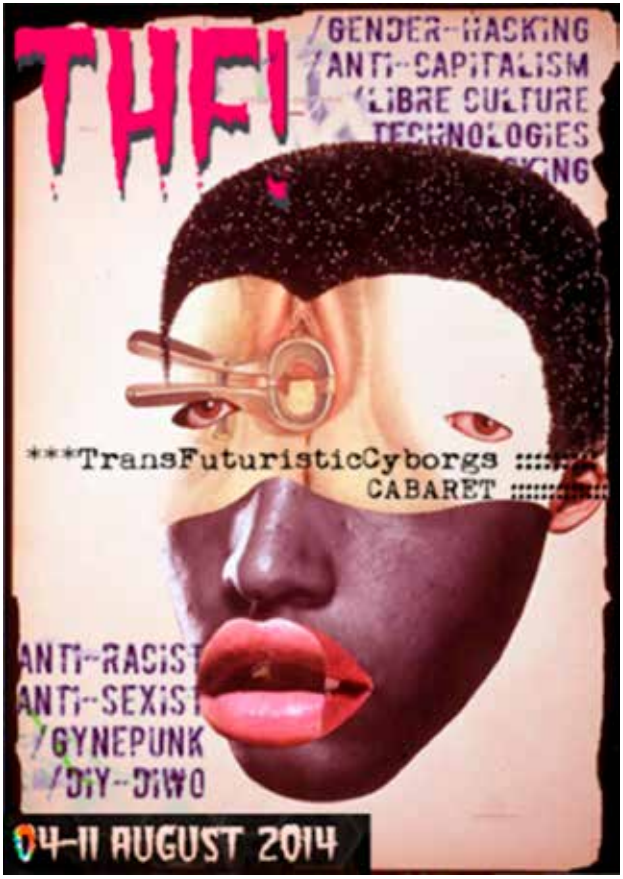
Palabra compuesta, del inglés: Slut - Puta y Shaming – Vergüenza. Se trata de la práctica de avergonzar o hacer sentir culpable a una mujer o adolescente por vivir su sexualidad. Se describe como una forma social para ejercer presión y control de la sexualidad femenina (Crothers, 2016), perpetuando una caracterización negativa de las mujeres que son percibidas como "promiscuas" o fuera de la norma social aceptada. En sociedades en las que la reputación de las mujeres es considerada "lo más importante" la acusación o sospecha de promiscuidad tiene un efecto negativo que trastoca completamente su entorno social y autopercepción. Se utiliza para justificar la violencia sexual y otras expresiones de violencia.

Tactical Tech - FRIDA - https://vrr.im/2cd1

En entornos digitales, el slut-shaming se presenta como una práctica común. Una mujer que denuncia violencia a través de sus redes sociales, será sometida al escrutinio público de sus propias redes de "amistades". Una foto con ropa considerada "inapropiada" será blanco de comentarios ofensivos y humillantes, que en ocasiones pueden hacer sentir a las mujeres que realmente tuvieron la culpa de haber sido violentadas.

Las estrategias para lidiar con este tipo de ataque son diversas y dependen de las características de cada situación. Se puede optar por eliminar y reportar a la

persona que está queriendo avergonzarnos, se puede dar respuesta a los comentarios y desmantelar los argumentos patriarcales bajo los cuales se nos juzga o se puede buscar redes de apoyo feministas, para dar respuestas colectivas a estos ataques.



TransHackFeminist convergence - http://anarchaserver.org/

2.6.1.1 Acciones e iniciativas de autodefensa:

- Clementine Canibal. Ella es una escritora, artista y bruja canadiense, editora del zine "Lamiendo las estrellas del techo"; reconocida por la viralidad del vídeo en el que lee el poema en primera persona "Sí, soy una puta" en el que se denuncia la perversidad del slut-shaming como expresión de la cultura patriarcal. Ver en: https://www.youtube.com/watch?v=9bdqUu35prU
- A nivel internacional, la respuesta más organizada sobre la problemática del Slut-Shaming es la deconstrucción de la negatividad del término Slut o Puta a través de las llamadas SlutWalks (Stampler, 2011) o Marcha de las Putas (Lancheros, 2014). Al reapropiarse del término se busca desligar la carga simbólica y empoderar las mujeres que han vivido este tipo de agresión.

2.6.2 Fat-Shaming

Palabra compuesta, del inglés: Fat - Gordura y Shaming – Vergüenza. En esta práctica lo que se pretende es avergonzar o humillar a una persona, en la mayoría de los casos a mujeres, en base a su peso. Esta tiene que ver con la percepción social negativa sobre las mujeres que no cumplen con estándares físicos de "belleza y salud". En las redes sociales, cuando una mujer gorda publica una foto con ropa considerada "no apropiada" recibe comentarios negativos porque

se asume que su gordura la asexualiza y que debe mantener dicha gordura oculta o disimular y utilizar ropa “apropiada”.

2.6.2.1 Acciones e iniciativas de autodefensa:

- Stop Gordofobia. La iniciativa StopGordofobia es un sitio web que se propone criticar la imposición de cánones de belleza y en la que se publican artículos teóricos que analizan las implicaciones de género en la construcción cultural de la gordura y artículos personales sobre la experiencia desde cuerpos gordos. Ver en: http://www.stopgordofobia.com

- FatMicroagressions. El Hashtag en inglés #FatMicroaggressions tiene la intención de visibilizar los comentarios hirientes e inapropiados que reciben las mujeres gordas en su día a día; ya que es socialmente aceptado expresar públicamente prejuicios sobre las personas con sobrepeso. Ver en: https://twitter.com/search?q=%23fatmicroaggressions

- We Lover Size. En respuesta a la falta de representaciones de cuerpos gordos en los medios de comunicación tradicionales nace también el proyecto “WeLoverSize”, una revista digital que promueve contenidos dirigidos a las mujeres que no cumplen con los ideales de belleza establecidos. Ver en: http://weloversize.com/

Hacking Feminism - https://wiki.laglab.org/Hacking_Feminism

- Tornillo, Gordofobia. Vídeo del Tornillo sobre la Gordofobia en la que se explica cómo el heteropartiarcado propicia la connotación negativa hacia la gordura, para mantener su control sobre los cuerpos de las mujeres: Ver en: https://www.youtube.com/watch?v=El-R1B_kyzY

2.6.3 Inducir a prácticas dañinas

Aquí nos referimos a la producción de contenidos que buscan provocar estados negativos o letales para tu integridad física, emocional y psicológica como pueden ser la anorexia, la modificación forzada de tu cuerpo a través de operaciones invasivas o el suicidio.

El sistema patriarcal amplifica los ataques machistas porque les otorga una posición dominante en la producción de tropos y narrativas acerca de lo que es socialmente aceptable y lo que no lo es. Resaltamos que de manera difusa y pervasiva internet y las redes sociales vehiculan en prioridad una visión del mundo sesgada en la cual se espera de las mujeres en particular corresponder a ciertos patrones de belleza y de comportamiento. Todo ello implica un conjunto de violencias simbólicas que llevan mujeres, adolescentes y niñas a sentir una baja autoestima y poner en riesgo su bienestar e integridad física y psicológica traduciéndose en alteraciones de alimentación, sueño, así como desear operaciones para modificar su cuerpo. No discutimos aquí el derecho de cada una a cambiar su aspecto físico, más bien denunciamos las presiones que se ejercen y que pueden llevar personas a imponerse modificaciones que no desean verdaderamente.

2.6.4 La ballena azul

Se trata de una práctica que se presenta como un juego cuya meta es el suicidio y que incita a sus participantes a un reto diario durante 50 días. Se dice que se inició en Rusia en 2013 y el primer suicidio fue reportado en 2015. A día de hoy se han reportado casos en 19 países. La inducción al suicidio se hace explotando vulnerabilidades como los sentimientos de rechazo, soledad o abandono de las personas. Este fenómeno forma parte de una tendencia reciente por generar pactos suicidas en internet y que, a diferencia de sus equivalentes analógicos, se da por lo general entre gente muy joven y que no se conoce.

Este fenómeno ha crecido en los últimos años en todo el mundo y aunque algunos estudios han mostrado la relación entre ambientes violentos y el suicidio entre jóvenes, sigue faltando mucha información para tratar de entender el efecto que podría darse entre la manipulación al suicidio y la violencia de género.

2.6.4.1 Acciones e iniciativas de autodefensa:

- Proyecto life. En España existen iniciativas como el Proyecto Life! de la Universidad de Alicante que busca detectar tendencias suicidas en las redes sociales: Ver en: https://gplsi.dlsi.ua.es/gplsi13/es/node/245

- La ballena rosa. "La baleia rosa" es una iniciativa desarrollada en Brasil para hacer frente a los casos de la ballena azul y, con ello, mostrar que internet también se puede usar para el bién. Consiste en un juego de 50 retos para tener una actitud positiva. Ver en: http://baleiarosa.com.br/index.php?lang=es

2.7 Ataques basados en el chantaje y la extorsión

2.7.1 Sextorsión

Se trata de un chantaje basado en amenazar hacer público material fotográfico o de vídeo íntimo o sexual. Se puede pedir a cambio dinero, contenido íntimo, actos sexuales contra su voluntad. Dominemos la Tecnología afirma que los "chantajistas buscan castigar o controlar a la mujer mediante la censura y/o vergüenza que nuestras sociedades patriarcales hacen recaer sobre las mujeres y sus cuerpos desnudos"1. Se dan muchos casos de sextorsión en las parejas para que la mujer no termine una relación. A veces la amenaza puede no ser únicamente la publicación de los contenidos, sino enviárselos a familiares, compañeros de trabajo, amigas etc.

2.7.1.1 Acciones e iniciativas de autodefensa:

- Take back the tech-chantaje. Dependiendo de quién sea el agresor Dominemos la tecnología recomienda "cubrir la webcam con cinta2", y "cambiar todas tus contraseñas por códigos alfanuméricos sólidos y únicos, si se cree que han sido crackeadas". Ver en: https://www.takebackthetech.net/es/be-safe/chantaje-estrategias y https://www.takebackthetech.net/es/be-safe/chantaje-derechos-relacionados

- Safer Nudes. Otra iniciativa de interés es la "guía sensual de seguridad digital Safe nudes" de la colectiva Coding Rights (s.f). En este fanzine disponible en portugués, español y inglés, se comentan buenas practicas para compartir imágenes desnudas y se muestra porque los selfies y otras formas de auto-representación pueden ser gestos políticos de empoderamiento feminista y LGTIQ. Ver en: https://www.codingrights.org/safernudes/

Hackmitin Mexico - http://hackmitin.espora.org/2017/

2.7.2 Pornografía no consentida

Se entiende como la "divulgación de material gráfico y audiovisual de tono erótico o explícitamente sexual sin consentimiento y sin propósito legítimo (a menudo con la intención de humillar, intimidar o extorsionar a la víctima)" (Peña y Vera, 2017). Pueden haber sido obtenidos por medio del sexting, grabados con el consentimiento de las partes para mantenerse en sus dispositivos, o haber sido grabados o registrados sin que la mujer se diera cuenta. La "pornografía no consentida" es un concepto que se distingue de lo que mucha gente llama "pornografía de venganza" (revenge porn) (Eikren y Ingram-Waters, 2016).

Esta plantea que el "acto de revelar una imagen privada y sexualmente explícita a un tercero podría describirse como pornográfico, en tanto transforma una imagen privada en el entretenimiento sexual público". No obstante no tiene en cuenta la intención de la víctima que de ninguna manera ha creado estas imágenes con esa finalidad pública. Además otro argumento en contra del término "porno venganza" es que este sigue culpando a la víctima en vez de poner la responsabilidad de estos ataques en el agresor que ha violado la privacidad, la intimidad y los acuerdos pactados. El concepto de venganza justifica un pensamiento en el cual la difusión sin consentimiento se acepta socialmente al ser una respuesta de revancha o venganza hacia una acción ejercida por la mujer. El amor romántico, los celos y los chicos siempre serán chicos son algunos de los argumentos que dan pie a que se justifiquen estos ataques.

La difusión de este tipo de contenidos puede llevarse a cabo con la finalidad de desacreditar, así como de mostrar el poder que tienen los agresores sobre ellas. A veces la publicación de los contenidos viene acompañada de datos personales lo que puede generar también acoso por parte de quienes han tenido acceso a estos contenidos, buscando, por ejemplo, contactar a la mujer que ha sido expuesta. En otros casos el agresor crea perfiles en sitios pornográficos donde publica las fotografías o vídeos, haciéndolas públicas a través de grupos en redes sociales, en servicios de mensajería instantánea o en sitios web o foros.

Para muchas personas agredidas es difícil poder hablar y compartir su situación en sus entornos más cercanos, como sus familias y amigos. En varios países, personas victimas de pornografía no consentida, así como organizaciones de mujeres y ciberfeministas han ejercido presión hacia las instituciones públicas para que cambiaran los marcos legislativos y tipificaran este tipo de ataque. También se ejerce presión hacia las empresas y plataformas en internet para que mejoren sus términos de uso y sus actuaciones respecto a estos contenidos (Peña y Vera, 2017).

Lelacoders Donestech - https://donestech.net/lelacoders

2.7.2.1 Acciones e iniciativas de autodefensa:

- Dominemos la Tecnología. Se recomienda, por ejemplo, de diversificar los idiomas para reportar y denunciar contenidos en internet ya que muchas empresas siguen privilegiando el inglés y sólo usan ese idioma para entablar una comunicación más profundizada y cuando piden datos para tumbar esos contenidos. También piden que se puedan marcar los contenidos protagonizados por menores de edad para facilitar su borrado más rápidamente. Ver en: http://dominemoslatecnologia.org/
- Acoso online. En el contexto de los países latino americanos Acoso.online se constituye como un espacio de referencia con recursos, análisis y recomendaciones practicas para hacer frente a este tipo de violencia. Ver en: https://acoso.online/pornovenganza/

2.7.3 Packs

Se denomina "pack" a un paquete de fotografías o vídeos sexuales o eróticos de una mujer. Se trata también de la dinámica de incitar hombres a que "consigan" el "pack" de alguna mujer o que compartan los contenidos íntimos de los cuales disponen con un grupo más amplio de hombres. La frase "pasa el pack" puede encontrarse en en foros, páginas de Facebook, grupos de chat, e incluso en memes. También se pueden encontrar foros donde se dan consejos sobre los tipos de engaños bajo los cuales se pueden obtener los contenidos íntimos de las mujeres.

Como en el caso de la pornografía no consentida estas fotografías o vídeos en ocasiones son tomadas con el consentimiento de la mujer para su registro pero no para su difusión abierta. Estas se pasan en plataformas como VivaAnuncios, Megaupload, Media fire, Google Play Store así como en páginas de Facebook que promocionan "los packs" o que sextorsionan a las mujeres bajo amenaza de difundir las imágenes. Este tipo de difusión de contenidos sin consentimiento ha sufrido un grave aumento en México donde la mayoría de los casos son de mujeres en edad escolar en secundaria, preparatoria, o universitaria (Morones, 2017).

2.7.4 Ciberacoso infantil (Grooming)

Hablamos de grooming cuando una persona mayor de edad establece contacto a través de medios digitales con una niña, niño o adolescente con el objetivo de crear una relación de confianza que sirva de preámbulo para un abuso sexual, explotación sexual o tráfico de personas. UNICEF lo define como "la acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de Internet."(UNICEF Argentina, 2014)

Little Red Riding Hood Lora Zombie - http://lorazombie.com/

El atacante, en la mayoría de los casos, finge ser también menor de edad (Gray, 2010). Al presentarse como un par, se muestra como entendedor de las problemáticas y necesidades de las criaturas con las que se comunica, incluso puede manipularlas para hacerles creer que es la única persona que las quiere y las entiende. De esta manera les resulta más fácil concretar un encuentro presencial o presionar para participar en actividades sexuales en línea. Al crear un perfil falso y enviar solicitudes de amistad a menores de edad, entra dentro de un círculo de contactos y tiene acceso a más información para manipular sus percepciones y sentimientos.

El abusador también puede entrar en una dinámica de extorsión una vez haya logrado su propósito; para mantener el control sobre su víctima puede amenazar con hacer público el abuso creando una narrativa en la que la niña, niño o adolescente se sienta culpable del abuso.

Para prevenir el grooming se recomiendan acciones colectivas, que involucren a la familia y la estructura educativa, promoviendo ideas y practicas básicas de privacidad y seguridad digital a través de la toda la institución escolar así como en los espacios de trabajo y la sociedad civil. En vez de pensar en acciones de censura y aislamiento se tienen que brindar herramientas y saberes que permitan la identificación de estas posibles amenazas así como un uso informado, crítico y ciudadano de las tecnologías.

Para contrarrestar el grooming, se recomienda establecer canales de información y acuerdos compartidos entre los adultos y los menores, hablar de las prácticas y dudas respectivas y de cómo establecer mecanismos de vigilancia y seguridad que no sean invasivos y se muestren respetuosos con los espacios de ambas partes. Por otra parte se recomienda investigar con atención nuevos contactos o amistades en las redes sociales, así como comprobar que nuestras "amistades" son personas reales a través de una revisión de sus publicaciones y fotografías.

2.7.4.1 Acciones e iniciativas de autodefensa:

- Campañas antigrooming. Se han desarrollado diversas iniciativas para la prevención y mitigación del grooming alrededor del mundo. Algunos países como Australia, Argentina y Chile han aprobado leyes anti-grooming, y otros han optado por promover campañas de comunicación que, en su mayoría, tienen un enfoque adultista y de censura a la participación de las niñas, niños y adolescentes en Internet. Organizaciones internacionales como UNICEF y Save the Children han implementado diversas iniciativas como por ejemplo guías para capacitar a padres y madres de familia, investigando la temática y creando espacios de coordinación multisectorial para la creación de políticas públicas preventivas. Ver en: https://www.unicef.org/argentina/spanish/guiagrooming_2014.pdf

- COLNODO. Una organización colombiana que forma parte de la red de Dominemos la Tecnología en países hispanohablantes, ha desarrollado una lista de 6 recomendaciones básicas para prevenir el grooming. Ver en: http://dominemoslatecnologia.org/es/formas-violencias/grooming

- Asociación nacional por la prevención de la crueldad contra la niñez. Ha elaborado una guía para conocer e identificar el grooming, así como proteger a la niñez. https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/

- Groomingclick. Blog dedicado a conocer y dar pautas para prevenir el grooming. Abuso a un click. http://groomingclick.blogspot.com/

2.7.5 Reclutamiento con fines de abuso sexual

ONU Mujeres (2015) describe esta práctica como el "uso de las tecnologías para atraer víctimas potenciales a situaciones violentas". Las redes de trata, el crimen organizado y organizaciones terroristas han incursionado en la internet para captar niñxs, adolescentes y mujeres a través de engaños y promesas falsas.

Estas organizaciones crean perfiles en foros, salas de chat y redes sociales donde se presentan como empleadores potenciales, amistades comprensivas o como hombres solitarios buscando pareja. Una vez establecida la comunicación, pueden secuestrarles, forzarles en contra de su voluntad o convencerles, a través del engaño y la manipulación, para que entren a una situación de violencia y abuso. Los abusadores pueden aprovecharse del condicionamiento de género del amor romántico. Al establecer lazos de afecto, "amor" y dependencia emocional pueden "presionar y persuadir a las mujeres" (Patrick, 2014) a aceptar situaciones de prostitución, transporte de sustancias ilegales o auto-inmolación.

Por ejemplo, en Latinoamérica es bastante común que redes de reclutamiento internacionales publiquen anuncios en sitios de búsqueda de empleo dirigidos a mujeres entre los 18 y 35 años ofreciendo trabajo como niñera o mucama para familias en España u otros países con mayor desarrollo económico. Sigue siendo un reto compilar cifras sobre el funcionamiento de estas redes ya que el riesgo y estigma social derivado de la denuncia pública hace que muchas prefieran callar. Por otra parte muchas legislaciones en contra de estas redes criminales no contemplan la posibilidad de que las mujeres sean manipuladas para salir de sus países de manera voluntaria, lo que invisibiliza este crimen.

2.7.5.1 Acciones e iniciativas de autodefensa:

Redes sociales y trata. En el artículo "Relación entre redes sociales y la trata" de Sheila Aarvik (2013), publicado en GenderIT.org explica que en el reclutamiento "convergen fatalmente, por un lado, una de las mejores herramientas de la comunicación y por otro la peor pesadilla de la humanidad: la esclavitud moderna". Ver en: http://www.genderit.org/sites/default/upload/trata_de_personas_y_redes_sociales.pdf

2.8 Ataques con un fuerte componente tecnológico

2.8.1 Programa espía (Spyware)

Los programas espías son una categoría de lo que se denomina software malicioso (en inglés ''malware'' como contracción de ''malicious software''). De manera general el software malicioso se refiere a cualquier programa computacional que opera de forma no legítima con la intención de hacer daño. En el caso

de los programas espías la finalidad es mantener el acecho a su objetivo, explotar los recursos de su sistema y/o enviar información a terceros.

Es común que los programas espías se instalen a partir de otro tipo de programas maliciosos, por ejemplo los gusanos (Kralicek, 2016), que al ejecutarse instalan el programa espía y pueden así mismo actuar junto con otros tipos de malware. Existen 4 categorías de spyware: los que monitorean sistemas, los llamados caballos de Troya, los adware y los cookies de rastreo.

Pueden tener funcionalidades como capturar contraseñas, copiar contenidos, grabar pantallas, activar y grabar audio y vídeo. Dos métodos comunes para infectar con estos programas es el envío por correo electrónico de un enlace para descargar el software aparentando otro programa, o realizando intromisiones en conexiones de red o inalámbricas (p. ej. wifi o bluetooth).

Existe una amplia variedad de programas espías. Algunos requieren de pocos conocimientos técnicos para poder usarlos. Se pueden obtener gratuitamente, comprarse e incluso contratarse servicios de espionaje mediante software. Algunos programas espías conocidos son: Spyware Quake, Security toolbar, WhenUSave, PuritySCANVirtumonde, Pegasus, CoolWebSearch, FinFisher, HuntBar, WinTools, DyFuCa, Look2Me, Movieland, WeatherStudio, Zango, Zlob Trojan.

Se han documentado ampliamente casos de programas espía usados a niveles gubernamentales y de control a disidencias y movimientos sociales (por ejemplo ‘’octubre Rojo’’,’’Pegasus’’ o el caso de la empresa “hacking team”) o como parte de ciberguerras (http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464_pf.html), pero también hay muchos casos documentados para obtener información personal de usuarios en general.

Su uso como parte de la violencia contra las mujeres suele consistir en la instalación de herramientas de administración remotas mediante las cuales se obtiene acceso a la pantalla, webcam, archivos, micrófono de una computadora infectada para obtener imágenes (Campbell, 2016; Bansal and Ahmad, 2016) (https://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/). También se dan usos dentro de parejas o exparejas para dar seguimiento a las actividades de una mujer cuando se conecta pero también para saber cuando esté en casa y cuándo no.

Debido a que los programas espía pueden no alterar visiblemente las actividades en un equipo infectado, se dificulta mucho su detección. Sin embargo hay dos estrategias importantes para evitar estos ataques. Por una parte, limitar el acceso a la computadora personal y no abrir enlaces o archivos que puedan contener malware. Por otra parte, se recomienda mantener tu computadora, móviles y otros dispositivos

limpios y saludables. Actualiza tus programas, corre un firewall, y cuenta con un antivirus y un antispyware en tus dispositivos (https://securityinabox.org/en/guide/malware).

2.8.2 Crackeo de cuentas

Conocido como "hackeo de cuentas", preferimos usar el termindo "crackeo de cuentas" (Coleman, 2013) ya que nos referimos a actividades maliciosas.

En su origen, el término "hack" proviene del inglés y significa cortar o alterar. Hackear tiene un uso muy extenso en los entornos tecnológicos que incluye la capacidad de acceder a sistemas informáticos y modificarlos pero también abarca actividades como curiosear y compartir conocimiento libre (para más detalles ver hackstory.es, https://es.wikipedia.org/wiki/Hacker, Coleman 2013).

Algunas hackers son personas con gran dominio de las redes y la informática que exploran, ponen a prueba y construyen estos medios. Sus acciones están motivadas por la defensa de valores como la libertad de expresión, información, comunicación y colaboración así como se basan sobre valores éticos compartidos que no incluyen llevar a cabo acciones criminales (Coleman, 2013; Rahalkar, 2016). Por todo ello, en algunas comunidades se propuso cambiar la palabra hack por la de crack cuando se hace referencia a actividades maliciosas como la de quebrantar contraseñas mediante programas.

El crackeo de cuentas es la acción de forzar, mediante herramientas tecnológicas o de ingeniería social, el acceso a una cuenta que requiere una autenticación de usuario y una contraseña. En la actualidad muchos dispositivos (software y hardware) permiten lograr el acceso a contraseñas de redes sociales, sitios webs, redes inalámbricas, móviles, objetos conectados etc. También se pueden contratar servicios o aprender con cursos on-line cómo crackear cuentas para obtener el acceso a espacios conectados.

Se reportan numerosos casos de ataques a cuentas y sitios web feministas para lograr obtener su control, comúnmente después de ello se cambian las contraseñas para que las propietarias no puedan recuperar el acceso. El crackeo de cuentas de redes sociales es común como parte de la violencia entre parejas (por ejemplo para tener acceso de manera escondida o forzada a las conversaciones privadas) y también lo usan acosadores o machitrolls para robar información de usuarias, por ejemplo datos personales y fotografías íntimas. El crackeo de cuentas puede implicar el robo de identidad, la extorsión o difamación.

Algunas de las técnicas más usuales para el crackeo de cuentas son:

- Ataque de contraseñas: Consiste en probar una a una la coincidencia de los caracteres de una contraseña con palabras de un diccionario (o de varios diccionarios de diferentes lenguas).

- Ataque de fuerza bruta: Consiste en la prueba aleatoria de combinar los diferentes tipos de caracteres (letras, números, caracteres especiales).

- Ataques híbridos: Consiste en probar con palabras de diccionario y agregar información que usuarios suelen añadir cpm frecuencia como por ejemplo combinaciones de números.

- Ataques no técnicos: Seguramente una de las maneras más comunes consiste en usar técnicas de ingeniería social sin apenas recursos tecnológicos, como buscar contraseñas anotadas en papel, mirar sobre el hombro de la persona cuando escribe su contraseña, adivinar o sonsacar información con preguntas indirectas, o aventajarse de información cuando el crackeo proviene de seres conocidos.

Un aspecto que dificulta la recuperación de cuentas, e impide la mitigación de las consecuencias en estos casos de robo o intromisión, es la falta de responsabilidad de las empresas que brindan servicios como cuentas de correo electrónico o redes sociales. Resulta difícil reportar y probar estos robos de cuentas a las plataformas que las detienen porque estas invierten recursos humanos limitados en el tratamiento de los casos reportados, porque privilegian interfaces y canales de reporte con poca inclusividad cultural y de género y porque a menudo las usuarias bajo ataque se encuentran en la imposibilidad de proveer los datos o pruebas que les piden para poder retomar el control de sus cuentas.

Para evitar el crackeo es recomendable proteger el acceso a tus cuentas y perfiles cuidando y haciendo fuertes tus contraseñas. Mantén una contraseña diferente por cada una de tus cuentas. Cámbialas con cierta frecuencia aun mas si crees que pueden estar comprometidas. Evita guardarlas por defecto en sistemas poco seguros, trata de no abrir tus cuentas en computadoras ajenas, borra tu historial de contraseñas y cuídate de programas espías así como de personas espiándote cuando entras tus contraseñas.

También puedes inventar un sistema mnemotécnico para recordarlas si es que manejas pocas cuentas o usar un gestionador de contraseñas quien se encargara de crearlas y recordarlas para ti. Finalmente se recomienda que actives la doble autentificacion para todas las cuentas que ofrecen esta opción.

2.8.3 Ataque a servidores

Este ataque es conocido como pharming o DNS hijacking. Tiene como objetivo suplantar un sitio web mediante el redireccionamiento de un dominio a una dirección IP que no corresponde al sitio original. Tradicionalmente los sitios web utilizan un nombre que forma parte del sistema DNS (acrónimo de Domain Name Server). Un ataque de pharming intentará que

la IP asociada a un dominio cambie, explotando las vulnerabilidades del software de servicios DNS o alterando los archivos asociados en la computadora de cada usuario.

Una de las posibles consecuencias de este tipo de ataque es obtener información de las personas que son engañadas para entrar en sitios falsos. Por ejemplo para obtener sus contraseñas y después direccionar al sitio correcto para evitar que la irrupción sea detectada.

2.8.3.1 Acciones e iniciativas de autodefensa:

- Security in a box. Este tipo de ataque puede prevenirse limitando el acceso a la computadora personal y no abriendo enlaces que puedan contener malware. Para ello mantén tu computadora y otros dispositivos limpios y saludables: actualiza tus programas, corre un firewall, y protégete contra infecciones de virus y spyware. Ver en: https://securityinabox.org/en/guide/malware.

- Fundación Fronteras Electrónicas. También se recomienda conectarte de forma segura a la internet cuando estés en línea, especialmente si estás transmitiendo datos personales y contraseñas. Es crucial que siempre uses una conexión cifrada que te asegura que tus datos no pueden ser vistos por nadie mientras viajan de tu computadora al sitio web que estás visitando o el servicio que estés usando. Para asegurarte que siempre estás conectándote de forma segura a sitios web cuando hay disponible una conexión cifrada, puedes instalarte HTTPS Everywhere, una extensión para Firefox, Chrome y Opera, desarrollada por la Fundación Fronteras Electrónicas. Ver en: https://www.eff.org/https-everywhere.

2.8.4 Ataques a sitios web y perfiles feministas

Si bien el análisis de ataques a sitios web se ha enfocado mucho en los servicios comerciales también se sabe de ataques a sitios feministas que tienen como característica la voluntad de censurar e intimidar a las propietarias de estos sitios.

Comúnmente estos tipos de ataques consisten en evitar la disponibilidad de los sitios haciendo ataques de denegación de servicios (DOS) o su versión distribuida (DDOS) o lograr accesos autorizados a los servidores en los que se hospeda el sitio web y cambiar su contenido, en algunos casos poniendo imágenes de pornografía comercial o haciendo público el "crackeo" del sitio.

Los ataques de denegación de servicios (DOS) basan su estrategia en:

- Enviar de forma irregular paquetes de datos.

Foockinho - https://www.behance.net/foockinho

- Generar un flujo de datos que sobrepasa las capacidades destinadas a la memoria (búfer https://es.wikipedia.org/wiki/B%C3%BAfer_de_datos) .
- Usar el tráfico de entrada y salida a los servidores para responder a peticiones falsas saturando el sistema.
- Interrumpir físicamente las conexiones (por ejemplo las fuentes de alimentación eléctricas).

Los ataques DDOS usan las mismas estrategias pero de manera distribuida a partir de múltiples sistemas de computo.

En 2016 mayfirst.org reportó una serie de ataques DDOS con el objetivo de imposibilitar el acceso a webs feministas y alertaban del correspondiente riesgo de censura así como de la necesidad de infraestructura para combatir este tipo de ataques. Ese mismo año la pagina web Laquearde.org recibió una serie de ataques DDOS que le obligaron a cambiar de servidor varias veces. Varias empresas de hosting comerciales rescindieron su contrato debido a que los ataques les reportaban una perdida económica y también afrontaron actitudes patriarcales por parte de los administradores de los servicios ante estos ataques. Otras organizaciones que trabajan con feminismo, lesbofeminismo o derecho a decidir recibieron ataques de defacement que consiste en cambiar el aspecto de una web maliciosamente (Ayala, 2016).

2.8.4.1 Acciones e iniciativas de autodefensa:

Algunas prácticas de mitigación para este tipo de ataque consisten en evaluar y conocer los principios éticos y políticos de los proveedores y plataformas de hosting y alojamiento de nuestros contenidos on-line.

- Onlinecensorship.org: Si tu publicación, contenido o tuit ha sido bloqueado o borrado de medios sociales puedes denunciar su censura en el portal Onlinecensorship.org: Ver en: https://onlinecensorship.org/es
- Project Shield. Para paginas y sitios webs podemos apoyar y usar servidores éticos o aliados para alojarlas. En casos extremos existen iniciativas como el Project Shield de Google. Ver en: https://projectshield.withgoogle.com/public/
- Greenhost.net. Son los fondos de respuesta urgente del proveedor de internet Greenhost para ofrecer alojamiento con altos niveles de seguridad e infraestructura a las iniciativas que ven peligrar su libertad de expresión en internet por culpa de estos ataques. Ver en: https://greenhost.net/products/rapid-response-services/

2.8.5 Bombeo en Google (Google bombing)

En la actualidad el buscador de Google se ha popularizado y probablemente es el principal motor de búsqueda que usa la gente en todo el mundo. En 2016

se reportó que dominaba el 64% del mercado (Lella, 2016). Lograr posicionar un sitio o contenido on-line entre los primeros resultados que aparecen se ha vuelto muy a menudo necesario para tener algo de visibilidad en la internet. El bombeo de google tiene como objetivo estar en los mejores lugares de la lista de resultados de una búsqueda disminuyendo el impacto de otros sitios.

Si bien los algoritmos para posicionar sitios en una búsqueda no son públicos los lineamientos generales que utilizan si lo son (https://www.google.com/search/howsearchworks/algorithms/). Posicionar un sitio en los primeros lugares de una búsqueda se puede conseguir mejorando algunas de las características y metadatos de la web, sea pagando por ello, sea engañando los algoritmos de google modificando palabras clave o alterando las estadísticas de visitas de un sitio web.

Este tipo de ataque ha sido asociado a grupos fundamentalistas, ciberarmadas así como grupos anti derechos. En varios países las páginas webs de los grupos anti-abortistas se vuelven los primeros resultados en aparecer cuando alguien busca información sobre aborto. Esta estrategia puede también darse con incluir información falsa presentándola como datos científicos, crear sitios web falsos de clínicas de aborto o de líneas telefónicas de ayuda, y/o pagar para la colocación de anuncios anti-aborto en los sitios donde se provee de información sobre aborto seguro (Skoski, 2017).

Algunas prácticas de mitigación para este tipo de ataque pueden consistir en diseñar estrategias de posicionamiento de sitios web en buscadores, usar servidores aliados para alojar los sitios web e impedir que no se agreguen de manera automática anuncios no deseados.

3. RECOMENDACONES GENERALES

3.1 RECOMENDACIONES TÉCNICAS DE PRIVACIDAD Y SEGURIDAD

1. Mantén tu computadora y otros dispositivos limpios y saludables: actualizar tus programas, correr un firewall y protegerte contra infecciones de virus son piezas claves en la seguridad de tus datos (https://securityinabox.org/es/guide/malware). Deberías también contemplar el tener cifrado de disco completo como un paso básico para la seguridad de tus dispositivos. La mayoría de dispositivos (computadoras y moviles) ofrecen cifrado de disco completo y esto requiere sólo un poco de conocimiento y habilidades. Por ejemplo, MS Windows ofrece cifrado con bitlocker a partir de Windows 7 Ultimate. File Vault es parte de Mac OS X, y el cifrado para celulares está disponible en la mayoría de celulares con Android comenzando con la versión 3.0 (Honeycomb).

2. Mapea tus datos: ¿Qué clase de datos produces y/o gestionas? ¿Con quién? ¿Dónde están almacenados estos datos? ¿Qué dispositivos o plataformas en línea tienen tus datos? Y lo más importante, ¿cómo de sensibles son tus datos y qué podría pasar si estos datos en particular desaparecieran de repente, o fueran vistos y copiados por terceros? Ten también en cuenta que almacenar información en dispositivos y servicios sobre los que no tienes un control completo es siempre un riesgo de seguridad. Esto no significa, sin embargo, que deberías rehuir cualquier servicio de terceros que pueda almacenar tus datos, sino que recomendamos estar atentas o tener en mente qué tipos de información y datos almacenas en estos servicios.

3. Securiza tus datos: Especialmente cuando tus datos se almacenan en línea, es crucial elegir contraseñas fuertes, o mejores frases de contraseña, y usar una diferente para cada una de tus cuentas. Para más información sobre la importancia de las contraseñas fuertes, cómo crear una y cómo almacenarlas, lee el capítulo sobre contraseñas de Security in a Box (SIAB) (https://securityinabox.org/es/guide/passwords). Si estás almacenando información en tu computadora y otros dispositivos, puedes usar cifrado para evitar que otros accedan a tus archivos. Para más información acerca de qué herramientas puedes usar para hacer esto, mira el capítulo de SIAB sobre almacenamiento seguro de archivos (https://www.securityinabox.org/es/guide/secure-file-storage).

4. Conoce las reglas de los espacios conectados en los cuales te mueves: Todas las plataformas cuentan con términos de uso y políticas de privacidad que establecen una relación contractual entre tú y las empresas que te ofrecen estos servicios. Es importante entender cuáles son tus derechos y que opciones te ofrecen para configurar tus opciones de visibilidad, privacidad pero también de reporte, bloqueo y denuncia de contenidos y perfiles. Ten en cuenta que

estos términos suelen cambiar con frecuencia y que suele ser responsabilidad de la usuaria estar informada de estos cambios.

5. Conéctate de forma segura a la internet: cuando estés en línea, especialmente si estás transmitiendo datos personales y contraseñas, es crucial que siempre uses una conexión cifrada que te asegura que tus datos no pueden ser vistos por nadie mientras viajan de tu computadora al sitio web que estás visitando o el servicio que estés usando. Para asegurarte que siempre estás conectándote de forma segura cuando hay disponible una conexión cifrada, puedes instalarte HTTPS Everywhere, una extensión para Firefox, Chrome y Opera, desarrollada por la Fundación Fronteras Electrónicas: (https://www.eff.org/https-everywhere).

6. Anonimiza tus conexiones: Algunas veces hay buenas razones para esconder tu localización física y tus actividades en internet. El navegador Tor anonimiza tus conexiones cuando estás navegando en internet, escondiendo los sitios que estás visitando de la vista de tu proveedor de servicios, y escondiendo tu localización de la vista de los sitios que visitas. Se consciente, sin embargo, que el uso de Tor puede levantar "banderas rojas", de modo que podría no ser siempre la mejor opción en tu caso. Para más información e instrucciones para usuarios de Windows, puedes visitar: (https://securityinabox.org/es/guide/anonymity-and-circumvention).

7. Securiza tus comunicaciones: Encontrarás algunos consejos particulares en esta guía.- Sin embargo, para ahondar en esta cuestión puedes consultar diferentes guías, entre las cuales destacamos:

- Cuando estés usando dispositivos celulares: https://securityinabox.org/en/guide/mobile-phones
- Teléfonos "inteligentes": https://securityinabox.org/en/guide/smartphones
- Opciones para el correo electrónico y la mensajería instantánea: https://securityinabox.org/en/guide/secure-communication

Te recomendamos encarecidamente que te tomes un tiempo para leer la guía completa "Caja de Herramientas de Seguridad", por el colectivo Tactical Technology y Front Line Defenders, y que está disponible en 15 idiomas (https://securityinabox.org/es). Puedes complementarla con otra guía diseñada por el colectivo Safehub llamada "Una guía casera a la Ciberseguidad Feminista para tomar control de tus espacios digitales"(https://es.hackblossom.org/cybersecurity/).

8. Interésate por las alternativas tecnológicas: Existen muchas alternativas desarrolladas por organizaciones y comunidades sin ánimo de lucro. Puedes de esta manera apoyar y contribuir al desarrollo de infraestructura y herramientas tecnológicas que no

sean patriarcales y que fomenten el respecto y privacidad de sus usuarias (por ejemplo y respecto a seguridad digital https://prism-break.org/es/).

En general las alternativas de software libre, así como de hardware libre, tienen un fundamento ético confiable orientado al uso y conocimiento común sin ánimo de lucro. Su naturaleza permite reforzarse con el apoyo y revisión de la comunidad y, además de ayudarte a aprender y entender mejor las tecnologías que escojas libremente, están más cerca de un planteamiento de la internet y tecnologías feministas, aunque no quedan 'perse' excentas de ello en algunos casos. Si necesitas aumentar tu conocimiento y uso de las tecnologías libres y, con ello, tu nivel de privacidad y seguridad, te recomendamos que te suscribas a listas de correo o comunidades o proyectos online donde su objetivo es el de difundir y ayudar a las personas a integrarse con estas alternativas o, con suerte, participar de algun grupo laboratorio crítico (hacklab) con encuentros presenciales y comunidades ciberfeministas orientadas a hackear la tecnología libre desde una defensa y colaboración feminista.

9. Practica el auto-cuidado: Nada es seguro si sólo pensamos sobre la tecnología y dejamos de lado los aspectos físicos y psico-sociales de nuestro bienestar. Si estás cansada, estresada o quemada, podrías cometer errores que pongan en peligro tu seguridad. Nuestro enfoque de la seguridad debería empoderarnos y no ser una carga; tener conciencia sobre la seguridad y las habilidades necesarias nos hacen más efectivas y nos acercan al zen en el trabajo y las actividades que desarrollamos.

3.2 RECOMENDACIONES RESPECTO A IDENTIDADES CONECTADAS

1. Nombre real. El uso de tu nombre "real" cuando creas un perfil o una cuenta en una red social significa que eres fácilmente identificable por tus familiares, colegas y otros, y que tus actividades se pueden vincular a tu identidad. Eso permite alimentar tu reputación e influencia ya que ganar confianza y credibilidad se hace más fácil. El nivel de esfuerzo es poco ya que las condiciones actuales de internet y sus servicios comerciales buscan alimentar activamente ese modelo. Si eres una periodista o una defensora de derechos humanos conocida es probable que tu cara y nombre real asociado sean ya conocidos y esto afectara el tipo de estrategias de mitigación que puedas poner en funcionamiento.

2. Anónimas. También puedes optar por el uso de identidades anónimas que permiten formas de expresión y opinión para temas mal vistos o criminalizadas. Por ejemplo, si eres una activista por el derecho a decidir, si combates el narco-gobierno o necesitas escapar de una relación de maltrato, es probable que el anonimato sea una opción conveniente para ti. Esa opción es también la más difícil de mantener y donde puedes

cometer mas fácilmente errores sea a nivel técnico así como de procesos sociales. El anonimato también implica pocas oportunidades de conectarte con otros, y por tanto de ganar confianza y reputación. Si nadie sabe quién eres, nadie puede darte apoyo si afrontas una situación de emergencia o alto riesgo.

3. Seudónimo. Puedes elegir una opción intermediaria creando identidades seudónimas. Existe el riesgo de que estas puedan ser vinculadas a tu identidad en el mundo físico pero usar un seudónimo permanente permite que otros puedan identificarte permitiéndote generar reputación y confianza. El mantenimiento de ese tipo de identidad requiere algo de esfuerzo, particularmente si estás utilizando también tu nombre real en otros lugares.

4. Identidades colectivas. También puedes usar una identidad colectiva como seria por ejemplo Guerrilla Girls, Isaac Hacksimov, Donna Hackaway, Hacktivistas o Luther Blisset. Este modelo te expone a posibles riesgos derivados de las acciones de otras personas usando también esa misma identidad. Al mismo tiempo te permite beneficiarte de la reputación del colectivo y contribuir al desarrollo de los imaginarios y acciones relacionados con esa identidad colectiva.

Si desglosamos más en detalle vemos que la construcción y manejo de las identidades conectadas puede realizarse en combinación con otras 4 posibles estrategias para alterarlas. Todas ellas constan de varios niveles posibles de aplicación incluyendo desde la instalación de aplicaciones y programas, la generación de contenidos y metadatos, hasta el uso de dispositivos materiales.

5. Fortificación. Puedes optar por la estrategia de la "fortificación", creando barreras restringiendo el acceso y visibilidad de tus perfiles, monitorizando quién te sigue o pública sobre ti, detectando ataques e invasiones de tu privacidad, poniendo barreras al uso de tu nombre o identidades por otras personas. La fortificación también conlleva poner dispositivos o programas en cuarentena, tener un antivirus y spyware siempre al día, encriptar tus dispositivos y comunicaciones, guardar tu celular en una bolsa de faraday, tapar tu webcam cuando no la usas o migrar hacia sistemas operativos más seguros como Gnu/Linux. Esta estrategia podría definirse como "Mis dispositivos, mis cuentas, mis reglas!".

6. Reducción. Puedes también optar por la "reducción" de tu sombra digital. Bajo el lema de "menos es más" puedes combinar una serie de tácticas para generar una escasez de datos e información sobre ti. Puedes por ejemplo limpiar o borrar perfiles o cuentas que no usas, ignorar o bloquear nuevas aplicaciones o servicios digitales innecesarios, resistir la tentación de publicar imágenes y contenidos acerca tuyo y tus conocidos y ordenar y organizar las cuentas e identidades asociadas que te resultan imprescindibles para existir en línea. La estrategia de la reducción

también puede aplicarse activamente a tus dispositivos electrónicos a través de tácticas de reciclaje, como dotar a tecnologías viejas de nuevos usos.

7. Camuflaje. La tercera estrategia es el "camuflaje" que funciona a la inversa de la reducción, tal que, en este modelo, cuantos mas datos generes mejor, porque lo que se busca es una inflación de datos que permita devaluar su valor. Algunas de las tácticas implicadas consisten en romper tus rutinas de navegación, publicación y comunicación, producir pistas e informaciones falsa, generar ruido disonante alrededor de tus identidades, usar la multitud o las identidades colectivas para esconderte y enmascarar tus verdaderos objetivos y motivaciones. Todas estas tácticas contribuyen en alterar la veracidad o grados de confianza que se pueden depositar en tus datos, su agregación y análisis correspondiente.

8. Compartimentación. Puedes optar por la "compartimentación" de tus datos, perfiles e identidades conectadas. Esta estrategia incluye separar y disociar tus identidades y redes sociales relacionadas para que no se contaminen y relacionen entre ellas. Al clasificarlas y mantenerlas separadas consigues reducir los posibles puntos de ataque ya que si un agresor consigue acceder a una de tus identidades no conseguirá relacionarla con tus otras identidades y posibles datos personales identificables relacionados. Esta estrategia apuesta por la combinación de una diversidad de perfiles, cada uno contando con su valor propio.

En conclusión queremos apuntar que todas estas estrategias y tácticas pueden ser combinadas, remixadas, transformadas. Cada persona y cada colectivo pueden ir desarrollando la combinación que mejor les funcione.

Otras compilaciones de recomendaciones útiles para mujeres y feministas...

Finalmente, si quieres seguir profundizando en cómo llevar a cabo las recomendaciones previas te listamos las siguientes guías que han sido escritas en un lenguaje llano y, algunas de ellas, en clave feminista, para facilitar su comprensión por las personas interesadas en entender qué alternativas existen y qué herramientas pueden mejorar tu privacidad y seguridad digital:

- Caja de Herramientas de Seguridad: El colectivo Tactical Technology y Front Line Defenders desarrolló está guía que es de gran utilidad. Además está disponible en 15 idiomas. Ver en: https://securityinabox.org/es/
- Zen y el arte de que la tecnología funcione para ti. Este manual es la base y precedente de esta publicación y resulta muy útil para poder leer más acerca de la creación y gestión de identidades en linea así como acerca de la construcción y mantenimiento de espacios seguros en linea y en la vida física. Ver en: https://ttc.io/zen
- MyShadow. La pagina web de MyShadow para leer y aprender acerca de herramientas y meto-

dologías para entender y alterar tu sombra digital. Ver en: https://myshadow.org

- Safehub. Una guía casera para la Ciberseguidad Feminista para tomar control de tus espacios digitales diseñada por el colectivo Safehub, requiere ciertos conocimientos técnicos, pero resulta muy clara e útil. Ver en: https://es.hackblossom.org/cybersecurity/
- Ciberseguras. Es un espacio que reúne muchos recursos y herramientas para aprender más sobre Internet y seguridad digital desde una perspectiva feminista. Ver en: http://ciberseguras.org/
- Más info: si quieres ahondar aun más en todo ello, te pasamos una compilación de varias guías de privacidad y seguridad escritas desde una perspectiva de género. Ver en: https://gendersec.tacticaltech.org/wiki/index.php/Manuals_with_a_gender_perspective

3.3 RECOMENDACIONES PARA DAR APOYO A OTRAS PERSONAS

A veces puede ser desalentador ver que alguien está sufriendo violencia en línea y, sin querer, podemos empeorar la situación al intentar dar un apoyo. Saber cómo actuar frente a la violencia es nuestra responsabilidad individual y colectiva para construir espacios más seguros. Si cuentas con ciertos privilegios es importante alzar la voz y decir "no", públicamente, ante la violencia y el acoso. Si no, la cultura de impunidad en torno al acoso y la violencia continuará. Y si eres parte de un grupo marginado, acuérdate de decirles a las personas que te apoyan, y que no pertenecen a dicho grupo, que este es uno de los métodos más poderosos de ayudar, en vez de sentir que no deben —o no pueden— hacer nada porque no son de ese grupo en particular. Cuando amigas o aliadas están siendo acosadas o atacadas en línea, hay buenas prácticas que puedes seguir:

1. Brindar apoyo rápido: Si eres cercana a la persona que está siendo atacada, ofrece asistencia inmediata. Ten en cuenta que esta persona puede sentirse abrumada y puede que no tenga instrucciones claras sobre cómo mejor ser ayudada. Debes permanecer tranquila, con atención activa y con paciencia. Intenta no agregar presiones o estrés. También puedes ofrecer moderar sus redes sociales o los comentarios de su blog para darles un descanso de la gestión. Finalmente, también puedes revisar leyes y políticas nacionales y locales que sirvan para tratar con acoso en línea y fuera de línea, para convertir tu conocimiento en acciones concretas que puedan ayudar a la persona que está siendo atacada.

2. Hazte oír: Si no conoces bien a la persona atacada, puedes alzar la voz en contra de lo que está ocurriendo. No es suficiente simplemente mandar un mensaje o tuit privado a la persona para decirle que ese tipo

de ataque es inaceptable. Incluso, a veces, cuando la persona bajo ataque está sumergida en tuits y mensajes, es mejor ni escribirle. En su lugar, alza la voz en tus redes sobre lo que está ocurriendo y atrévete a hablar sobre este tipo de comportamiento.

3. Organizar colectivamente: Si deseas tener un impacto mayor, piensa en organizar una acción colectiva ya que es mucho más efectivo que las acciones individuales por sí solas. Junta un grupo de amistades —y amistades de amistades— para hacer una enjambre de contra-discurso juntas en Twitter, por ejemplo. Esto le demostrará a la persona bajo ataque que tú y otras personas se preocupan por ella, y que tales ataques son inaceptables.

4. Escribir una declaración de solidaridad: Si eres parte de una organización social o una red de contactos, pueden escribir una carta que haga explicito el rechazo hacia la violencia de género y el acoso en línea. Asegúrense de que la persona que está siendo atacada lee la declaración antes de que se publique. También pueden preparar de antemano un protocolo de actuación para delinear los pasos a seguir en caso de que alguien sea atacada en línea. De esta manera, es posible evitar mayores daños y ser más efectivas en su reacción cuando esta situación ocurra.

En todos los casos ¡Recuerda que esto no se trata de ti: el enfoque es luchar contra la violencia de género y apoyar a las personas que la están sufriendo!

3.4 RECOMENDACIONES ORIENTADAS A ACTUACIONES PÚBLICAS

#InternetEsNuestra (s.f) es una coalición que trabaja por una red libre de violencias, cuyo objetivo es que internet sea un espacio libre donde la lucha contra la violencia en línea hacia las mujeres no tenga como consecuencia la restricción de sus derechos. Para lograrlo, las organizaciones contrapartes que conformamos la coalición realizaremos actividades de monitoreo, análisis y propuestas hacia la búsqueda de soluciones que pongan un alto a la violencia en línea. Desde esta iniciativa se comparten las siguientes preocupaciones respecto a las respuestas institucionales que buscan atender las diferentes formas de violencia en línea contra las mujeres:

1. No culpar a las mujeres y hacerlas responsables por la violencia. Culpar a las agredidas no sólo las revictimiza, además tiene como consecuencia la autocensura: las mujeres optan por dejar de usar las tecnologías y redes sociales. Se limita así no solo su derecho a la libertad de expresión, sino también el derecho de acceso a la información en línea.

2. Ir más allá de la legislación. Se propone como solución una falsa protección al “legislar por legislar”. La respuesta no radica por principio en el derecho penal, sobre todo tratándose de un país con altos niveles de impunidad, derivados de una acción efectiva prácticamente nula por parte de las autoridades en-

cargadas de investigar y sancionar la violencia contra las mujeres.

3. No separar los mundos on-line y lo off-line. Esto contribuye a que la violencia en línea no se considere "real" y a que no se tengan en cuenta los efectos que esta tiene en la vida de las mujeres, a nivel físico y emocional. Lo anterior impacta la toma de decisiones sobre situaciones cotidianas, como su forma de vestir y si salir o no de sus casas.

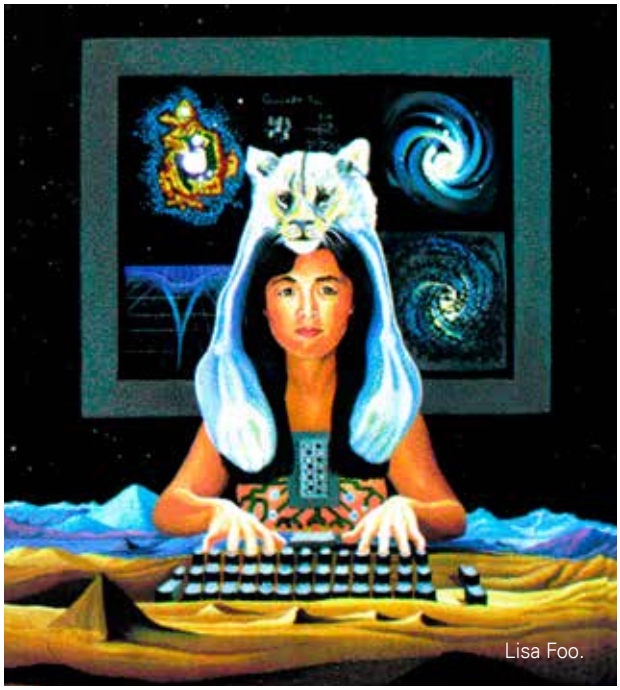
4. No restringir otros derechos a nombre de la protección a las víctimas. Soluciones como la regulación indebida, la vigilancia sin controles o la prohibición del anonimato hacen que internet sea un espacio más limitado en materia de privacidad, acceso a la cultura y libertad de expresión, y difícilmente ofrece mecanismos de reparación y garantías de no repetición.

5. Generar datos sobre violencias de género on-line. No existen datos públicos y oficiales al respecto. Es urgente poder contar con datos públicos, oficiales, sistemáticos y longitudinales sobre la prevalencia de las violencias de género on-line. Ello permitiría visibilizar claramente y con rigor qué está ocurriendo. Contar con datos posibilitaría un mejor diagnóstico e investigación de la situación para poder diseñar políticas públicas adecuadas y bien fundamentadas al respeto. Además, contrarrestaría los discursos y acciones neomachistas que se apoyan, justamente, en la inexistencia de datos e investigaciones, y la impunidad que eso genera, para seguir ejerciendo violencias de género.

3.5 RECOMENDACIONES ORIENTADAS A LAS PLATAFORMAS DE REDES SOCIALES COMERCIALES

Gracias a la investigación de the Guardian sobre las "Facebook Files" (s.f) y la moderación y sus condiciones en Facebook y, sobre todo, a su relectura en clave de género llevada a cabo Take back the Tech (s.f.b), apuntamos un sumario de recomendaciones que pueden resultar útiles para las plataformas de redes sociales comerciales.

1. Diversificar los equipos de moderación y facilitar la coordinación con equipos de igualdad. Diversificar los perfiles de los equipos no sólo mejora su efectividad y actitud ante los riesgos, sino que posibilita llegar a la mejor decisión y solución ante un problema. Es importante que los equipos tengan mujeres y hombres de diferentes perfiles socio-demográficos y, que, además, puedan comunicarse en diferentes lenguas más allá del inglés. Además de establecer equipos diversos cabe que estén coordinados con los equipos de igualdad de las mismas plataformas y/o, en su ausencia, establecer contactos con entidades feministas y/o pro-derechos humanos que puedan darles apoyo.


Lisa Foo.

2. Capacitar en perspectiva de género a los equipos de moderación de las plataformas. Es posible que los equipos de moderación sean aún demasiado escasos y/o pequeños para hacer frente a todas las demandas sobre violencias de género y contra los derechos humanos que se generan a escala global. Tampoco puede resultar suficiente que sean diversos. Cabe asegurar el conocimiento y capacidad de los equipos de diseño y moderación de las plataformas respecto al género y, específicamente, las violencias de género. Para ello es necesario dar formación específica en perspectiva de género y sobre los derechos humanos a los equipos.

3. Revisar los mecanismos de denuncia y acción. Los mecanismos de denuncia y acción deben asegurar su accesibilidad por parte de personas diversas. Debe ser fácil de encontrar, entender y utilizar. En este sentido es necesario que sea especialmente sensible a las dificultades que presentan las colectividades previamente excluidas de las TIC, así como que se entienda en otras lenguas que no sean el inglés. Es necesario que los mecanismos establecidos sean transparentes, fiables, legítimos, justos, claros y abiertos. En este sentido, es importante que el proceso sea previsible y con plazos establecidos para facilitar su seguimiento.

4. Mejorar la transferencia e información responsable respecto la moderación de contenidos. Es importante dotarse de una normativa que tenga en cuenta la normativa internacional sobre derechos humanos y sobre género. También que esta normativa se haga pública, respecto a los límites establecidos en cuanto a contenidos de las plataformas. Esta debería contener el rechazo explícito a las violencias de género on-line y visibilizar los mecanismos para hacerles frente. A su vez, resulta necesario generar y mostrar datos sobre la incidencia de estas violencias y las acciones tomadas al respecto. Además sería útil que facilitara el aprendizaje continuo para ir mejorando a l respecto, por parte de la propia plataforma y para las demás.


Oh, oh, sexualidades digitales!
Facilitado por
María Martha Escobar
¡Taller gratuito!
Reservá tu cupo antes del 10 de junio al correo: enredadas.ni@gmail.com
HACKATÓN FEMINISTA 2016
FemHack 2016: 404 equidad, diversidad no encontrada
¡Súmate a la construcción de mundos ciberfeministas!
Sábado 18 de Junio
TALLERES :- 1: 00 - 5:00 PM / Universidad Centroamericana
AFTER PARTY :- 8:00 - 10:00 PM / Café Mará Mará
Para mayor información, escribir al correo: enredadas.ni@gmail.com
FEMHACK

4. CONCLUSIONES

Actualmente, la mayoría de personas ya somos parte de las redes sociales, al menos en el contexto español y occidental. Las mujeres cada vez estamos más presentes en ellas. Generamos sus contenidos y las utilizamos para trabajar, comunicarnos con amistades, reivindicar o, incluso, para nuestras relaciones sexo-afectivas. Sin embargo, sigue siendo necesaria una mirada crítica respecto a las redes sociales y con perspectiva de género. En esta publicación hemos intentado contribuir a ello.

La aparición de las redes sociales fue celebrada por su potencial de mejora y transformación tecnosocial. Incluso las feministas, especialmente las ciberfeministas en sus inicios, destacaban sus posibilidades para la igualdad y el desarrollo de las mujeres, sus derechos y libertades. Sin embargo, las plataformas y redes sociales donde nos relacionamos en internet no resultaron ser la panacea y presentan también sus limitaciones. Por un lado, son una muestra de la brecha social y de género que aún persiste en nuestras sociedades. Unas personas (sobre todo ellas) sólo usan, dan y generan, mientras otras (sobre todo ellos) además de usar, prácticamente siempre mandan y reciben los beneficios asociados. Por el otro, las redes sociales no resultan tan abiertas y libres como aparentan. El capital social, el efecto mateo y su reverso Matilde, así como los filtros burbuja favorecen que las redes internamente contengan a nuestros similares y privilegien ciertas redes encima de otras. De este modo se mantiene el status quo y se dificultan los cambios, también de género. Finalmente, es imprescindible que reflexionemos en torno a la privacidad, la igualdad y libertad, pues tampoco se distribuye de forma uniforme on-line. No todas las personas resultan igual de libres en internet y las redes sociales. De hecho, las violencias de género, también las que operan on-line, cohartan la libertad de acción y movimento de las mujeres y otras colectividades y tienen graves consecuencias para ellas.

En esta publicación hemos intentado mostrar y desgranar lo que está ocurriendo en internet y las redes sociales si atendemos a las violencias de género. Este asunto es gravísimo y tiene consecuencias potencialmente fatales para más de la mitad de la población. Las agresiones machistas a mujeres y personas LGTBIQ persisten, se multiplican, viralizan y alcanzan una mayor audiencia, tanto a nivel geográfico como a nivel temporal. Además, se agrava por la acción organizada de grupos neomachistas que tienen internet como espacio de acción privilegiado defendiendo y alentando a los agresores de mujeres, también on-line. Ello se constituye pues como uno de los principales problemas de la sociedad de la información actual

y de futuro, aunque, paradójicamente, ni se presente como tal ni se actúe en consecuencia.

Aunque la preocupación y acción feminista al respecto es crucial y consigue sus logros, sus acciones, personas y familiares son extremadamente acosadas on-line. En relación a ello las mujeres y personas LGTBIQ son objeto de control y se limitan sus opciones de libre expresión y exposición en las redes. Sobre todo, las mujeres empoderadas y las feministas están en el punto de mira de los ataques machistas on-line. Sin embargo, es desgarradora la pasividad e incluso, la revictimización de las personas agredidas, por parte de las instituciones públicas y las grandes corporaciones detrás de las principales redes sociales. No sólo dificultan un diagnóstico preciso de las violencias de género on-line al no generar datos públicos al respecto, aún disponiendo de ellos o de la capacidad de generarlos, sino que por acción u omisión controlan y siguen permitiendo estas violencias. Con ello se convierten en reflejo, parte y alimento sustentador del viejo sistema heteropatriarcal y machista que se resiste a desaparecer y se actualiza a través, en, para y con los mundos virtuales.

Las violencias de género on-line las ejercen mayoritariamente hombres. A menudo son parejas o exparejas de las mujeres agredidas, pero también otros hombres contribuyen a ellas y las ejercen, muchas veces en forma de machitrols. Las violencias de género on-line adoptan diferentes formas y tipologías, desde el mansplaning hasta el grooming o la pornografía no consentida. Algunas de ellas, además, implican un elevado componente tecnológico. Todas estas formas de violencia resultan ser dañinas, especialmente para las mujeres y las colectividades LGTBIQ, pero pueden y deben revertirse. En esta publicación hemos intentado facilitar la identificación de los tipos de violencias de género on-line con las que te puedes encontrar o llegar a sufrir, pero también hemos apuntado algunas acciones e iniciativas, sobre todo feministas, que pueden ser útiles para hacerles frente y/o contrarrestarlas. Estas acciones son una muestra de la sororidad entre mujeres, pero también de las estrategias de autodefensa y luchas de género de antaño y del futuro. Por ello, esta publicación se constituye también como una guía-manual sobre las violencias de género on-line y cómo contrarrestarlas.

Queda aún mucho camino por recorrer para conocer el alcance de las violencias de género on-line y, sobre todo, para hacerles frente hasta su erradicación. Las propias mujeres y colectividades LGTBIQ, los responsables de las principales plataformas on-line, los gobiernos, así como y, sobre todo, los hombres deben comprometerse y pasar a la acción para que las relaciones sociales on-line, sean efectivamente libres y seguras para todas las personas.

5 REFERENCIAS

- Aarvik, S. C. (2013). Trata de personas y redes sociales. Disponible en: http://www.genderit.org/sites/default/upload/trata_de_personas_y_redes_sociales.pdf
- ACP (2015). Exploring corporate and legal remedies for technology-related violence against women 2012-2015. Disponible en: http://www.genderit.org/onlinevaw/
- Ayala, L. (2016). Cybersecurity Lexicon. Apress.
- Bansal, P. & Ahmad, T. (2016). Methods and Techniques of Intrusion Detection: A Review. SmartCom pp. 518–529
- Barrena, M. (2016). Convierten en viral la violación de 33 hombres a una adolescente en Brasil. Los replicantes. Disponible en: https://www.losreplicantes.com/articulos/violan-adolescente-brasil-comparten-redes-sociales/
- BBC (2017). Detienen en Suecia a 3 hombres sospechosos de retransmitir en vivo una violación en grupo en Facebook. Disponible en: http://www.bbc.com/mundo/noticias-internacional-38720270
- BeckyGardiner, B. Mansfield, M.; Anderson, I.; Holder, J.; Louter, D. & Ulmanu, M. (2016). The dark side of The Guardian comments. Disponible en: https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments
- Benesch, S. (2013). The Dangerous Speech Project. Dangerous Speech: A Proposal to Prevent Group Violence. Disponible en: http://dangerousspeech.org/guidelines/
- Boix, M. (2006). Hackeando el patriarcado: La lucha contra la violencia hacia las mujeres como nexo. Filosofía y práctica de Mujeres en Red desde el ciberfeminismo social. Revista de Estudios Feministas Labrys, 10.
- Bourdieu, P.(1983). Poder, Derecho y Clases Sociales. Desclée. pp. 131-164
- Burgos, A.; Mandillo, E.; Martínez, Y. (2014). Memes feministas: estrategias ciberfeministas de derribo del heteropatriarcado. Violencias de género 2.0, 5, 57-70.
- Cabello, F., Franco, M. G., & Haché, A. (2012). Hacia una web social libre y federada: el caso de Lorea. Teknokultura. Revista de Cultura Digital y Movimientos Sociales, 9(1), 19-43.
- Campbell, T. (2016). Practical Information Security Management. Apress, 155-165 pp.

- Chemaly, S. (2014). "Hate Crimes in Cyberspace" author: "Everyone is at risk, from powerful celebrities to ordinary people", Salon. Disponible en: http://www.salon.com/2014/09/02/hate_crimes_in_cyberspace_author_everyone_is_at_risk_from_the_most_powerful_celebrity_to_the_ordinary_person/

- Coleman, G. (2013). Coding freedom. Princeton University Press.

- Constantini, L. (2016) . El negocio de las citas 'online': "Ligar en Internet está aceptado por la sociedad". El País. Disponible en: https://economia.elpais.com/economia/2016/01/27/actualidad/1453923530_063999.html

- Crash Override Network (s.f) So you have been doxed: a guide to best practices. Disponible en: https://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices?is_related_post=1

- Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. U. Chi. Legal F., 139.

- Crothers L.M. (2016). Slut Shaming as Bullying in LGBTQ Adolescents: A New Area for Inquiry and Intervention. J Trauma Treat 5:282. doi:10.4172/2167-1222.1000282

- Díaz-Aguado, M.J., Martínez Arias, R.; Martínez Babarro, J. (2014). La evolución de la adolescencia española sobre la igualdad y la prevención de la violencia de género. Colección 19. Delegación del Gobierno para la Violencia de Género. Ministerio de Sanidad, política social e igualdad. Centro de publicaciones. Disponible en: http://www.violenciagenero.msssi.gob.es/violenciaEnCifras/estudios/colecciones/estudio/evolucion2014.html

- Donestech (2008) Descifrando el código Lela. Documental disponible https://www.youtube.com/watch?v=WlyFAaDsugg

- Donoso-Vázquez, T & Pardo, V. (2014). Neomachismos en espacios virtuales. Violencias de género 2.0, 4, 47-55 http://iknowpolitics.org/sites/default/files/completo_violencias_de_genero_2.0.pdf#page=29

- Donoso-Vázquez, T., Rubio, M. J. & Vilà, R. (2014) Investigando sobre violencias de género 2.0. Violencias de género 2.0, 2, 29-34

- Eikren, E. & Ingram-Waters, M. (2016). Dismantling 'You Get What You Deserve': Towards a Fe-

minist Sociology of Revenge Porn. Ada: A Journal of Gender, New Media, and Technology, No. 10. doi:10.7264/N3JW8C5Q

- European Institute for Gender Equality (2017) Cyberviolence against women and girls. Disponible en: http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls

- FRA (2014). Violence Against Women: An EU-Wide Survey. Main Results Report. Disponible en: http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

- Gray, L. (2010). Grooming: How child molesters create willing victims. Cómo abusadores de niños crean victimas. Asociación Nacional de Sobrevivientes de Abuso Infantil. Disponible en: http://www.naasca.org/2012-Articles/040512-GroomingWillingVictims.html

- Hache, A. (Ed.) (2014). Soberanía tecnológica. Dossier sobre Soberanía Tecnológica. Disponible en: gitbook.com/@sobtec

- HACHE, Alex; CRUELS, Eva; VERGÉS BOSCH, Nuria, Ciberfeminismos 2017.In: ¡Feminismos! Eslabones fuertes del cambio social. Disponible: http://www.coredem.info/rubrique77.html , p.127 – 135.2016.

- Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104-118.

- Henson, B., Reyns, B. W. & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. Journal of Contemporary Criminal Justice, 29(4), 475-497.

- Instituto Andaluz de la Mujer (2015) Protocolo de detección e intervención en la atención a víctimas de ciberdelincuencia de género. Disponible en: http://www.juntadeandalucia.es/iam/catalogo/doc/iam/2015/143528391.pdf

- Internet es nuestra (s.f) #FalsaProtección Cuatro errores que se deben evitar al combatir la violencia en línea. Disponible en: http://internetesnuestra.mx/post/158075258118/falsaprotecc-io-n-cuatro-errores-que-se-deben

- Jeong, S. (2015). The internet of Garbage. Conferencia audiovisual. Disponible en: https://www.youtube.com/watch?v=pUSctMLLNUE

- Kralicek, E. (2016). The Accidental SysAdmin Handbook. Apress 219-223 pp.

- LaVanguardia(2017).Investiganlaviolaciónengrupo de una adolescente transmitida en directo por Facebook Live. Disponible en: http://www.lavanguardia.com/sucesos/20170321/421070396548/violacion-en-grupo-adolescente-facebook-live-chicago.html

- Lancheros, L. (2014). La Marcha de las Putas: un golpe a los sexistas del mundo. PubliMetro. Disponible en: https://www.publimetro.cl/cl/mundo/2014/04/16/marcha-putas-golpe-sexistas-mundo.html

- Lella, A. (2016). ComScore Releases February 2016 U.S. Desktop Search Engine Rankings. ComScore.com. Disponible en: https://www.comscore.com/Insights/Rankings/comScore-Releases-February-2016-US-Desktop-Search-Engine-Rankings

- Momoitio, A. (2014) Violencias patriarcales en la red: internet al servicio de la violencia contra las mujeres. Violencias de género 2.0, 5, 13-26.

- Morones, M. (2017). Packs: el nuevo riesgo para menores en la red. El diario mx. Disponible en: http://diario.mx/Local/2017-02-07_2f29460b/packs-el-nuevo-riesgo-para-menores-en-la-red/

- Núñez Puente, S. (2008). Una exploración de la praxis feminista en España: nuevas tecnologías y nuevos espacios de relación desde el ciberfeminism. Feminismo/s, 11, 109-12.

- Obn (s.f) 100 anti.theses. Cyberfeminism is not... Disponible en: http://www.obn.org/reading_room/manifestos/html/anti.html

- ONU Mujeres (2015) Cyber Violence against women and girls: a world-wide wake-up call. Ciberviolencia contra mujeres y niñas: un llamado de atención global. Disponible en: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

- ONU (1993). ONU. Declaración sobre la eliminación de la violencia contra la mujer. Resolución de la Asamblea General 48/104 del 20 de diciembre de 1993.

- O'Toole, L. L., & Schiffman, J. R. (Eds.). (1997). Gender violence: Interdisciplinary perspectives. NYU Press.

- Padilla, M. & Mezquita, R. (2006) Penélope: tejiendo y destejiendo la red, en Reunión de Ovejas Electrónicas (ROE) (2006), Ciberactivismo, Sobre usos políticos y sociales de la Red, Barcelona: Virus.

- Patrick, W. (2014). Human trafficking: psycology of recruitment. Tráfico de personas: la psicología

del reclutamiento. Psycology Today. Disponible en: https://www.psychologytoday.com/blog/why-bad-looks-good/201401/human-trafficking-psychology-recruitment

- Pelton, J., & Singh, I. B. (2015). Digital Defense: A Cybersecurity Primer. Springer.

- Peña, Vera (2017). Pornografía no consentida: Análisis situado a respuestas de plataformas en Internet. Disponible en: https://acoso.online/wp-content/uploads/Informe-N1_Pornografia-No-Consentida-en-Plataformas.pdf

- Pereira, F., & Matos, M. (2016). Cyber-Stalking Victimization: What Predicts Fear Among Portuguese Adolescents?. European Journal on Criminal Policy and Research, 22(2), 253-270.

- Pérez Tejera, F. (2012). Diferencias entre los usuarios de seis parques públicos en Barcelona según el nivel de seguridad percibida en el barrio. Athenea Digital. Revista de pensamiento e investigación social, 12(1).

- Periodicoclm (2017). Detenido por justificar en Twitter el asesinato machista de Mora: "Algo haría la puta para acabar así". Disponible en: http://www.periodicoclm.es/articulo/sociedad/detenido-justificar-tuit-twitter-asesinato-violencia-genero-machista-mora-toledo-algo-haria-puta-acabar-asi/20170216121313006421.html

- Periodista digital (2017). El vídeo del depravado que viola a una mujer inconsciente en la discoteca ¡animado por los clientes! Disponible en: http://www.periodistadigital.com/america/sociedad/2017/04/12/el-video-del-depravado-que-viola-a-una-mujer-inconsciente-en-una-discoteca-animado-por-los-clientes.shtml

- Plant, S. (1997). Zeros and ones. Doubleday books.

- Rahalkar, S. A. (2016). Certified Ethical Hacker (CEH) Foundation Guide. Apress.

- Requena, A. (2013). Los datos que demuestran que Toni Cantó miente sobre la violencia machista. Eldiario.es. Disponible en: http://www.eldiario.es/sociedad/datos-demuestran-Toni-Canto_0_104990017.html

- Salas, E. (2008). XXI Una odissea al ciberespai: un recorregut preliminar pel ciberfeminisme. UOC Papers. Revista sobre la sociedad del conocimiento, (7), 1-12.

- Shephard, N. (2016). Big Data and Sexual Surveillance. Disponible en: https://www.apc.org/en/pubs/big-data-and-sexual-surveillance

- Skoski, E. (2017). How Anti-Choice Fake Clinics Leverage Technology to Trick People Out of Abortion Care. Rewire. Disponible en: https://rewire.news/article/2017/05/12/anti-choice-fake-clinics-leverage-technology-trick-people-abortion-care/

- Stampler, L. (2011). SlutWalks sweep the nation. Huffingtonpost.com. Disponible en: http://www.huffingtonpost.com/2011/04/20/slutwalk-united-states-city_n_851725.html

- Tacticaltech (2017). L. Egaña, F. Goldsman. Usos creativos feministas de las redes sociales. Disponible en: https://gendersec.tacticaltech.org/wiki/index.php/Usos_creativos_feministas_de_las_redes_sociales

- Tacticaltech (2015). Hache, A. (coord). Zen and the art of making tech work for you. Autodoxeo. Disponible en: https:ttc.io/zenmanual

- Take back the tech (s.f). Discurso de odio. Disponible en: https://www.takebackthetech.net/es/know-more/discurso-de-odio

- Take back the Tech (s.f). Joint statement on Facebook's internal guidelines for content moderation. Disponible en: https://www.takebackthetech.net/news/joint-statement-facebooks-internal-guidelines-content-moderation

- Take back the tech (s.f). Violencia contra las mujeres. Conocer más. Disponible en: https://www.takebackthetech.net/es/conocer-m%C3%A1s

- The guardian (s.f.b). Facebook files. Disponible en: https://www.theguardian.com/news/series/facebook-files

- UNICEF Argentina (2014) Grooming. Guía práctica para adultos. Disponible en: https://www.unicef.org/argentina/spanish/guiagrooming_2014.pdf

- Vargas, V. (2015). El fiscal denuncia el juego 'on line' que animaba a matar a gais. El Periódico. Disponible en: http://www.elperiodico.com/es/sociedad/20150529/fiscal-denuncia-juego-on-line-animaba-matar-a-gais-4232014

- Vergés, N. (2012). Una década de feminicidios en el Estado Español: Una aproximación a través de la visualización de información con AREA. Arte y Políticas de Identidad, 6, 145-159.

- Vergés, N., Hache, A., & Cruells, E. (2014). Ciberfeminismo de investigacción con y entre tecnoartistas y hackers. Athenea Digital. Revista de pensamiento e investigación social, 14(4), 153-180.

- Vilà Baños, R. (2016). La juventud ante las violencias de género 2.0. In Comunicació presentada a: XVI Congreso Nacional y VII Congreso Iberoame-

ricano de Pedagogía: Democracia y Educación en el siglo XXI (SEP2016). Madrid, Facultat de Educación. Universidad Complutense de Madrid. 28 al 30 de Junio de 2016.

- Women's media center. (s.f) Speech project. Research and statistics. Disponible en: http://wmcspeechproject.com/research-statistics/#_ftn5
- Zafra, R. (2015). Netianas, N(h) hacer mujer en Internet. Madrid: Lengua de Trapo.

www.juntadeandalucia.es/institutodeadministracionpublica