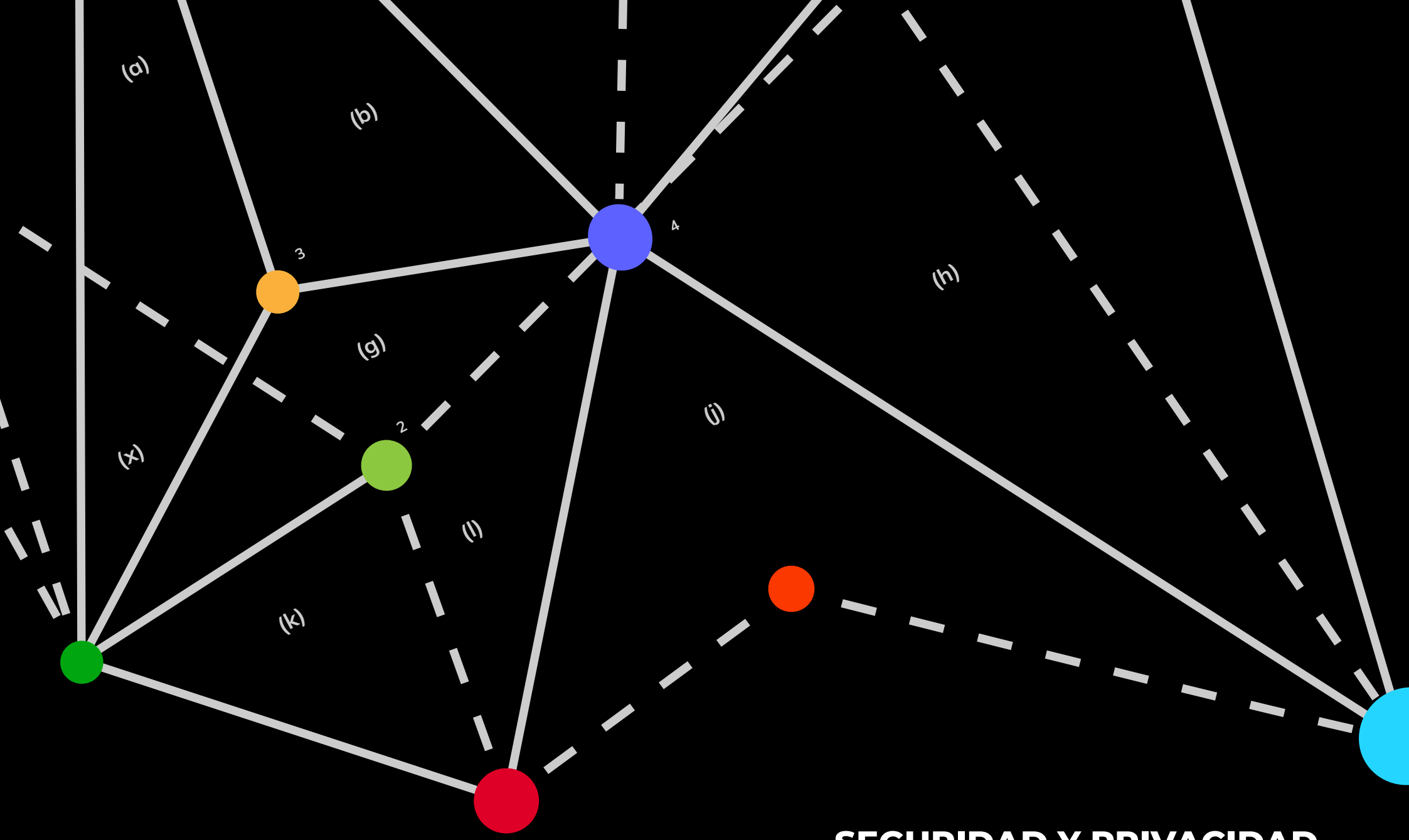


MESH

SEGURIDAD Y PRIVACIDAD DIGITAL BÁSICA

Alex Hache

ÍNDICE

Fuente: *Project Utopia*

PRIVACIDAD Y SEGURIDAD DIGITAL, CUIDADOS DIGITALES PARA TODAS

1. CONCEPTOS FUNDAMENTALES

Es probable que ya te hayas preguntado: **¿Cuánta información digital o "datos" existen acerca tuyo?** ¿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 móvil o un ordenador? ¿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 (TICs) generan huellas y señas personales que te pueden identificar en la vida material y física.

No obstante, en los inicios de internet (70 - 90s), este 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 normal usar avatares o seudónimos y navegar combinando identidades variadas. Por todo ello, **muchas personas vislumbraron en internet nuevas formas de empoderamiento para las mujeres, las disidentes del género y en general para las comunidades discriminadas, excluidas o silenciadas.**

En paralelo, una vorágine de inversores y startups intentaban ver cómo generar dinero con internet. Aunque muchas no sobrevivieron al crash de las puntocom, algunas sí **entendieron que el modelo de negocio radicaba en la recolección y venta de nuestros datos (y el rastreo de nuestras sombras digitales)**

Fuente: wikimedia commons

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.

Ese cambio de rumbo quedó patente en 2010 cuando **Mark Zuckerberg (fundador de Facebook) declaró que la era de la privacidad se había acabado**, mientras compraba las casas particulares situadas alrededor de su propia casa para garantizar su privacidad. Esta perspectiva señalaba una nueva orientación de la agepersonnda mundial neoliberal (buscando la "transparencia" 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 que se quedaría seguramente para siempre flotando en servidores bajo el control de otras personas. Resulta útil pensar en todos los datos digitales que existen acerca tuyo como tus rastros digitales. Estos componen una especie de «**sombra digital**» a la cual vamos agregando más datos cuando usamos herramientas y servicios digitales.

Sabemos que las empresas los recogen con la finalidad de analizar nuestro comportamiento y hábitos con el objeto de vendernos productos y servicios. También sabemos que los gobiernos quieren tener acceso a la mayor cantidad de información acerca nuestro para **controlar, vigilar y/o castigar**. Finalmente, personas malintencionadas pueden desear esa información para **acosar, chantajear, o espiar** a miembros de su familia o simplemente personas cuyo estilo de vida o opiniones no les gusta.

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.

En general resulta difícil ver y entender cómo las corporaciones, gobiernos e individuos pueden conocer los detalles personales e íntimos de la vida de millones de personas. Frente a este contexto en el cual la privacidad es un valor en vías de extinción, cabe preguntarnos cuáles son actualmente las estrategias y tácticas de mitigación y resistencia.

Si no podemos sencillamente apagar el ordenador, puede que 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 posibles adversarios listados anteriormente.

2. BLOQUE 1. ENTENDER LA SEGURIDAD INTEGRAL Y CÓMO ESTA SE RELACIONA CON LAS INFRAESTRUCTURAS DE INFORMACIÓN Y COMUNICACIÓN

En esta primera parte, profundizamos acerca de nuestras percepciones sobre qué es la seguridad y la privacidad. Para ello hablamos de las características de la seguridad integral o seguridad holística. Tradicionalmente la noción de seguridad se ha asociado a la seguridad “dura”, es decir, cómo proteger nuestro cuerpo, nuestros dispositivos y los espacios en los que nos movemos o vivimos.

Más adelante, gracias a los aportes de los movimientos sociales se ha añadido otra dimensión de la seguridad que trata del bienestar psicosocial, emocional y, en general, de los cuidados. Con el auge de Internet y las TIC, **la seguridad ha pasado a integrar una tercera arista que lidia con la seguridad digital y con la protección de nuestros datos y nuestras comunicaciones.** Finalmente, los movimientos feministas han aportado a la seguridad holística una perspectiva de género interseccional que tiene en cuenta las violencias de género relacionadas con los usos de las TIC y las relaciones asimétricas de poder y oportunidades a la hora de acceder a conocimientos y prácticas sobre privacidad y seguridad digital.

Vemos que la implementación de prácticas de protección dependen de la seguridad que podemos negociar con nuestro entorno, familiares, colectivos, pero que también depende de un contexto externo que no controlamos. Además, las necesidades de seguridad también dependen de nuestra subjetividad y de nuestro contexto y suelen evolucionar en el tiempo (no es fija, hay que revisitarla). Por todo ello, **la seguridad es un pastel de milhojas que se articula en capas y redes.**

Una vez que hemos explorado estas características, pasaremos a analizar la infraestructura de Internet y la infraestructura de telefonía móvil para entender por **dónde circulan nuestros datos, quién puede verlos y/o modificarlos en cada momento**. Esta etapa es fundamental para entender que los espacios conectados no son virtuales si no que se basan en unas infraestructuras materiales muy reales que permiten múltiples formas de control y vigilancia sobre las usuarias de Internet y la telefonía móvil, y por descontando, de las plataformas de redes sociales en Internet.

Todo ello nos permitirá entender cómo operan nuestras “sombras digitales”, qué las compone y cómo podemos influenciar o alterarlas.

Estos rastros digitales incluye datos que has creado y ves de manera intencional - como los tuits que compartes públicamente o una entrada de blog en tu sitio web, así como el contenido que otras personas crean acerca de ti cuando te etiquetan en fotos, te mencionan, o simplemente se comunican contigo a través de un correo electrónico o una sesión de chat. El ‘contenido’ son los datos que produces de forma activa: tus correos electrónicos, mensajes de texto, entrada de blog, tuits, llamadas telefónicas, compras en línea, fotos, y vídeos.

Estos rastros digitales también incluyen piezas de datos que se crean acerca de tu contenido y que en su mayoría resultan invisibles, comúnmente llamados ‘metadatos’. Son datos acerca de tus datos, incluyendo cómo y cuándo se crearon, dónde se han almacenado, desde dónde se han enviado, o cuándo y dónde te conectaste para subirlos a Internet. La mayoría de los metadatos son información necesaria para que funcione la infraestructura básica de Internet y nuestros móviles. **Los metadatos se crean casi siempre de forma pasiva, sin que te des cuenta necesariamente, o sin que lo consientas expresamente.**

Por ejemplo, tus hábitos de navegación y dirección IP son compartidas entre los sitios web que visitas y los servicios que utilizas para realizar un seguimiento de tu comportamiento. También se encuentran miles de millones de trozos de metadatos relativamente pequeños que se van creando y almacenando cada vez que envías un correo electrónico, navegas por la web, o cuando tu celular o cualquier otro dispositivo digital se conecta y envía información a Internet.

Estos “rastros digitales” pueden incluir tu nombre, ubicación, contactos, fotos, mensajes, y similares, pero también puede tratarse de la marca de tu computador, la duración de tus llamadas telefónicas o información acerca de las páginas web que visitas.

Finalmente y partiendo de estos elementos de análisis, pasamos a desarrollar ejercicios para llevar a cabo unos análisis de riesgos individuales y colectivos. Para ello mapeamos nuestros dispositivos y nuestra producción de datos (cuentas, perfiles, apps, etc) para entender qué tipo de datos creamos y manejamos, donde están alojados y qué tipo de información confidencial y/o sensible contienen. Esto nos permite identificar posibles áreas de riesgo y pensar cómo reducir o contrarrestar esos riesgos (copias de

seguridad, revisión configuraciones seguridad y privacidad de las plataformas, activar Verificación en dos pasos (2FA), crear contraseñas más seguras y prácticas acerca de su uso, instalar herramientas que permitan cifrado punta a punta, etc).

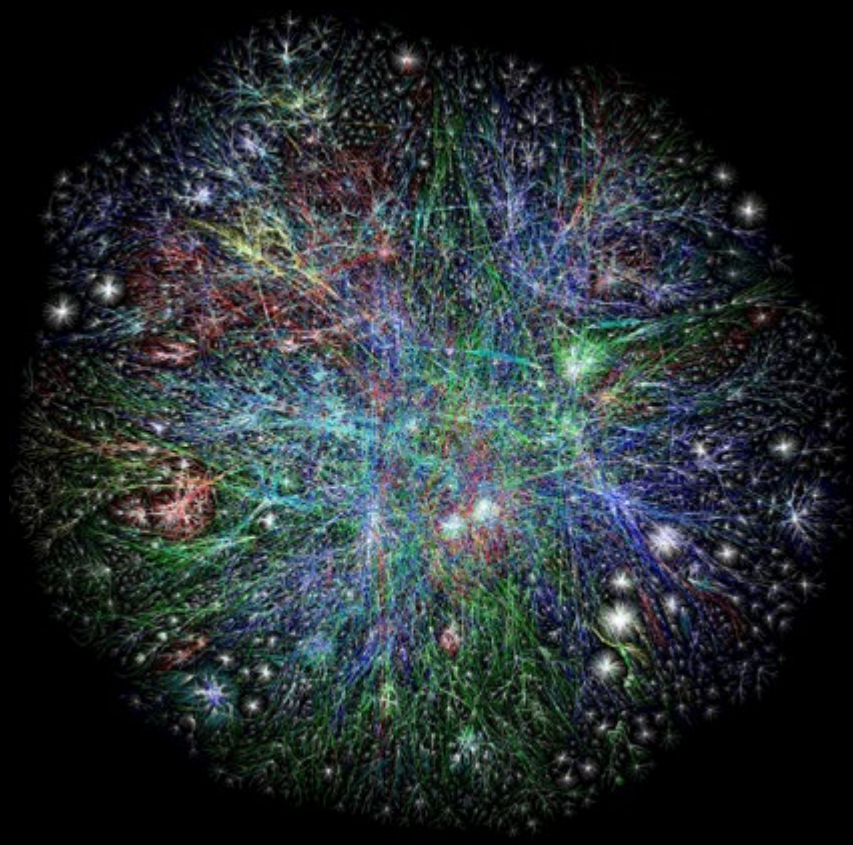
3. BLOQUE 2: GESTIÓN DE IDENTIDADES Y ESTRATEGIAS DE RESISTENCIA

Muchas de nosotras nos hemos encontrado con decisiones difíciles sobre cómo manejar nuestros 'yoes' personales, profesionales, activistas y demás, con nuestras identidades y perfiles en línea. Puede que tengamos una sola identidad que utilicemos para conectarnos a través de nuestras diferentes redes sociales, o puede que hayamos tomado medidas para 'separar' nuestras identidades en línea.

Cada tipo de identidad conectada presenta ventajas e inconvenientes que vale la pena sopesar con atención a la hora de decidir cómo una quiere presentarse, construirse, expresarse en Internet y en los medios sociales. Las identidades conectadas más apropiadas son las que tienen en cuenta el contexto, los riesgos y deseos específicos de las personas que las desarrollan.

El uso de tu **nombre "real"** 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 ganas 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



OPTE Project Map of the Internet 2005

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 afectará el tipo de estrategias de mitigación que puedas poner en funcionamiento.

También puedes optar por el uso de **identidades anónimas** que permiten formas de expresión y opinión para temas silenciados, criminalizados o peligrosos. Por ejemplo, si huyes de la violencia machista, si combates el narco-gobierno o animas una plataforma de medios independiente, es probable que el anonimato sea una opción conveniente para ti. Esa opción es también la más difícil de mantener y donde puedes cometer más fácilmente errores. 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.

Puedes elegir una opción intermedia 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 lo que te ayuda a 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.

Finalmente, también puedes usar una identidad colectiva como sería, por ejemplo, Anonymous 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 veremos que la construcción y manejo de las identidades conectadas puede realizarse en combinación con otras 4 posibles estrategias para alterar nuestras huellas digitales. 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.

Podemos optar por la **estrategia de la "fortificación",** creando barreras, restringiendo el acceso y la visibilidad, monitorizando a quien nos sigue o pública acerca de nosotras, detectando ataques e invasiones de nuestra privacidad, poniendo barreras al uso de nuestro nombre o nuestras identidades por otras personas.

La fortificación también conlleva poner el hardware y los programas en cuarentena, tener un antivirus y spyware siempre al día, encriptar nuestros dispositivos y comunicaciones, guardar nuestro móvil en una bolsa de Faraday, tapar nuestra webcam cuando no la usamos o migrar hacia sistemas operativos más seguros como Gnu/Linux.

Podemos también optar por la **"reducción" de nuestra sombra digital**. Bajo el lema de "menos es más" podemos combinar una serie de tácticas para generar una escasez de datos e información sobre nosotras.

Podemos, por ejemplo, limpiar o borrar perfiles o cuentas que no usamos, ignorar o bloquear nuevas aplicaciones o servicios digitales innecesarios, resistir la tentación de publicar imágenes y contenidos acerca nuestro o de nuestros conocidos, ordenar y organizar las cuentas e identidades asociadas que nos resultan imprescindibles para existir en línea. La estrategia de la reducción

también se aplica activamente a nuestros dispositivos electrónicos a través de tácticas de reciclaje así como de dotar a las tecnologías viejas de nuevos usos.

La tercera estrategia es la **"ofuscación" (o camuflaje)** que funciona a la inversa de la estrategia de la reducción ya que en este modelo cuantos más datos generamos mejor, ya que lo que se busca es una inflación de datos que permita devaluar su valor.

Algunas de las tácticas implicadas consisten en romper nuestras rutinas de navegación, publicación y comunicación, producir pistas e informaciones falsas, generar ruido disonante alrededor de nuestras identidades, usar la multitud o las identidades colectivas para escondernos y enmascarar nuestros verdaderos objetivos y motivaciones. Todas estas tácticas contribuyen a alterar la veracidad o grados de confianza que se pueden depositar en nuestros datos, en su agregación y análisis correspondientes.

Finalmente, podemos optar por la "compartimentación" de nuestros datos, perfiles e identidades conectadas. Esta estrategia incluye separar y disociar nuestras identidades de las redes sociales relacionadas para que no se contaminen y relacionen entre ellas.

Al clasificarlas y mantenerlas separadas, conseguimos reducir los posibles puntos de ataque ya que si un adversario consigue acceder a una de nuestras identidades no conseguirá relacionarlas con nuestras otras identidades y con los posibles datos personales identificables. Esta estrategia apuesta por la combinación de una diversidad de perfiles, cada uno contando con su valor propio.

4. EJERCICIOS PRÁCTICOS, DINÁMICAS GRUPALES Y EJERCICIO DE EVALUACIÓN

Se recomienda para el diseño de sesiones formativas acerca de privacidad y seguridad digital orientada a jóvenes **basarse en la metodología ADIDS.** Esta proporciona un marco para estructurar sesiones de aprendizaje en cinco momentos diferenciados (Actividad / Discusión / Input / Profundización / Síntesis) que deben tener coherencia entre ellos.

Por otra parte, este tipo de metodología orientada a la participación presume que todas las personas tienen experiencia en su propio uso de las TICs, así como reconoce y hace visible sus propias percepciones y estrategias de privacidad y seguridad digital.

Por ello, trabajaremos en todo momento con las participantes para incentivar su participación y aprendizaje a partir de sus conocimientos y experiencias propias así como estimular en ellas la búsqueda autónoma del conocimiento y la colaboración en la materia.

Además, recomendamos en la medida de lo posible **alejarnos de los dispositivos (ordenadores y móviles) mientras se generan dinámicas grupales de reflexión.** Una apropiación crítica y ciudadana de las tecnologías puede empezar cuando las personas quieren compartir acerca de sus experiencias con las TIC sin estar invadidas por ellas.
Se pueden reservar momentos concretos para proyectar herramientas, ver cómo se instalan y dejar las participantes instalar

Fuente: Ken Bauer

una herramienta concreta. Si se dispone de tiempo, también se recomienda crear espacios de aprendizaje informales tipo hacklab en el cual todas aprenden y enseñan a las otras acerca de herramientas de privacidad y seguridad digital que usan o que han descubierto en el taller.

La formación también propicia la utilización de herramientas de privacidad y seguridad para adquirir un **punto de vista crítico y práctico**, así como para fomentar la capacidad de seleccionar entre las herramientas existentes y poder incorporarlas a su propio contexto.

En cualquier caso no se fomenta una acercamiento a la seguridad y a la privacidad empezando por las herramientas, si no que solo se llega a ellas partiendo de los análisis de riesgo individuales y colectivos desarrollados con las participantes, y de cómo estos informan la búsqueda de las herramientas y buenas prácticas relacionadas.

Para poner en práctica y evaluar los conocimientos adquiridos durante la formación se puede diseñar una actividad final con los siguientes objetivos:

- Identificar riesgos, ataques digitales y/o violencias de género que están ocurriendo en el contexto de la experiencia de Internet y las TIC por parte de las estudiantes.
- Aplicar los contenidos aprendidos a un caso concreto que afecta directa o indirectamente a las participantes (se tienen que consensuar estos temas en grupos de trabajo).
- Incidir en la construcción de una solución en base a unos objetivos y resultados estratégicos y medibles. La actividad está dividida en los siguientes apartados:

Parte 1: Detectar uno o varios riesgos, ataques digitales y/o violencias de género que afectan a su comunidad o a una comunidad que conozcan.

Parte 2: Describir de manera detallada esas violencias. ¿Cuándo surgen? ¿Por qué? ¿A cuántas personas afecta? ¿De qué maneras les afectan, qué impacto tienen? ¿Qué consecuencias tiene para la sociedad y la democracia?

Parte 3: Desarrollar un diagnóstico de riesgo para las personas afectadas por estas violencias apuntando los posibles impactos y la probabilidad de que estos acontezcan.

Parte 4: Desarrollar una estrategia de mitigación que implique tácticas proactivas y reactivas que tengan en cuenta la seguridad, los cuidados y el bienestar psicosocial así como la privacidad y la seguridad digital.

Parte 5: Identificar herramientas de privacidad y seguridad de licencia libre que puedan ayudarnos en la consecución de esas acciones.

1.5. RECURSOS

Finalmente, listamos una serie de currículos de capacitación que se pueden usar y adaptar para trabajar los temas de privacidad y seguridad digital – Cuidados Digitales para todas. Estos contenidos están licenciados como CC BY SA NC, pueden usarlos y adaptarlos mientras citen su autoría, compartan bajo mismas condiciones y los usen sin ánimo de lucro.

Currículo de capacitación sobre privacidad y participación política para Decidim Barcelona:

Estas sesiones han sido diseñadas específicamente para las personas que trabajan como formadoras, capacitadoras y facilitadoras en temas de formación a las TIC pero también en temas de participación política y educación a la ciudadanía, no obstante, también pueden resultar útiles para personas que quieren crear conciencia sobre estos temas en su propio ámbito de actuación e influencia.

El repositorio incluye 10 actividades formativas en castellano y catalán con sus materiales didácticos relacionados incluyendo temas como, Cuida los Datos, Soberanía Tecnológica y Cómo Elegir Alternativas, ¿Cómo ganan dinero los servicios que usas en internet, ¿Cómo funciona la comunicación móvil? O Comunicación Móviles.

Enlace: training.decidim.org

Créditos: https://github.com/decidim/training/blob/master/content/README

Currículo de capacitación sobre privacidad por MyShadow:
Con 31 actividades y materiales relacionados en castellano. Ya no está en mantenimiento pero sigue siendo referencia.

https://myshadow.org/train
https://myshadow.org/materials

Créditos: Tactical Technology Collective

Currículo de capacitación Gendersec:

Es un recurso que introduce una perspectiva holística y feminista en las capacitaciones sobre privacidad y seguridad digital. Se basa en nuestra experiencia organizando Institutos de Género y Tecnología para mujeres y activistas trans de todo el mundo.

Es un recurso de acceso libre, disponible en inglés y español, que cubre más de 20 temas desde Hackear el discurso de odio, Riesgos y estrategias de las plataformas de citas, Usos creativos de las redes sociales, Mapeo de riesgos, Manejo del estrés, Soberanía tecnológica y Estrategias de resistencia.

Capacitadoras, facilitadoras y defensoras pueden acceder a estos talleres y adaptarlos a sus comunidades para apoyar las Defensoras de Derechos Humanos en protegerse de amenazas en línea y fuera de línea.

https://es.gendersec.train.tacticaltech.org/
https://en.gendersec.train.tacticaltech.org/

Créditos: https://gendersec.tacticaltech.org/wiki/index.php/Gendersec_training_curricula#Creditos

Manuales

Recomendamos a las personas lectoras visitar las guías de Tactical Technology Collective. Muchas ya no están mantenidas pero siguen siendo recursos de mucho interés para aprender y profundizar en privacidad y seguridad digital:

Data Detox

¿Te has inundado de aplicaciones(apps), hecho clic en “Estoy de acuerdo” demasiadas veces, perdido la pista de todas las cuentas que has creado?

Quizás no estés controlando tu vida digital tanto como quisieras. Pero no te desanimes: esta desintoxicación (“detox”) de datos es para ti. Al final de los siguientes 8 días estarás dando los pasos hacia una vida digital más sana y en tus manos.

https://datadetoxkit.org/es/detox

La página web de **MyShadow** para leer y aprender acerca de herramientas y metodologías para entender y alterar tu sombra digital.

https://myshadow.org/es

“Zen y el arte de que la tecnología funcione para ti” para leer más acerca de la **creación y gestión de identidades en línea** así como acerca de la construcción y mantenimiento de espacios seguros en línea y en la vida física:

https://ttc.io/zen

Caja de herramientas de seguridad disponible para aprender acerca de las **herramientas** que te puedes instalar y configurar **para mejorar tu privacidad y seguridad digital.**

https://securityinabox.org/es/

Otros manuales y recursos didácticos sobre privacidad y seguridad digital con perspectiva de género:

KIT contra las violencias machistas on-line – Donestech

Desde una posición crítica y feminista, hacemos una introducción a las violencias machistas online y, sobretodo, ponemos a vuestra disposición una serie de propuestas, recursos e iniciativas para que nos cuidemos, nos defendamos, contrarrestemos y alteractuemos frente a estas violencias.

Creemos que este KIT resultará muy útil para las mujeres y personas LGTBIQ, especialmente para aquellas mujeres violentadas, pero también para las destacadas, las feministas y disidentes sexuales y de género que se ven afectadas por violencias on-line de forma creciente. Os animamos a utilizar este KIT tanto de manera preventiva como reactiva y esperamos q ue les sea de utilidad.

Cat: https://donestech.net/files/kitcontraviolenciesmasclistesonline2018.pdf

Cast: https://donestech.net/files/kitviolencies2019_cast.pdf

Redes Sociales en perspectiva de género: Guía para conocer y contrarrestar las violencias de género on-line' – Donestech

Esta publicación está pensada para que pueda utilizarse también como guía y manual para entender mejor cuáles 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.

https://donestech.net/files/redessociales.pdf

Formación en violencias de género, privacidad y seguridad digital desde una perspectiva crítica y feminista – Donestech

Relato y ejemplo de formación sobre temas privacidad y seguridad digital orientado a detectar y contrarrestar violencias de género online:

Lista de recursos de privacidad y seguridad digital con perspectiva de género: https://donestech.net/noticia/formacio-en-violencies-de-genere-privacitat-i-seguretat-digital-des-de-una-perspectiva

Ciberseguras: https://ciberseguras.org/

La clicka/Libres en línea: http://www.libresenlinea.mx/

Coding Rights: https://www.codingrights.org/

Safer Sisters: https://giphy.com/codingrights

Chupadados: https://chupadados.codingrights.org/es/introducao

Acoso.online: https://acoso.online/

Guía práctica para tratar casos de pornografía no consentida en recintos educacionales bajo estándares de derechos humanos y equidad de género por Acoso.online: https://acoso.online/wp-content/uploads/2018/12/Guia-Practica-Establecimientos-Educacionales_AcosoOnline_2018.pdf

Señoras de internet podcast: https://soundcloud.com/tristanaproducciones/hacemos-sexting-senoras-de-internet

6. ARTISTAS DE REFERENCIA

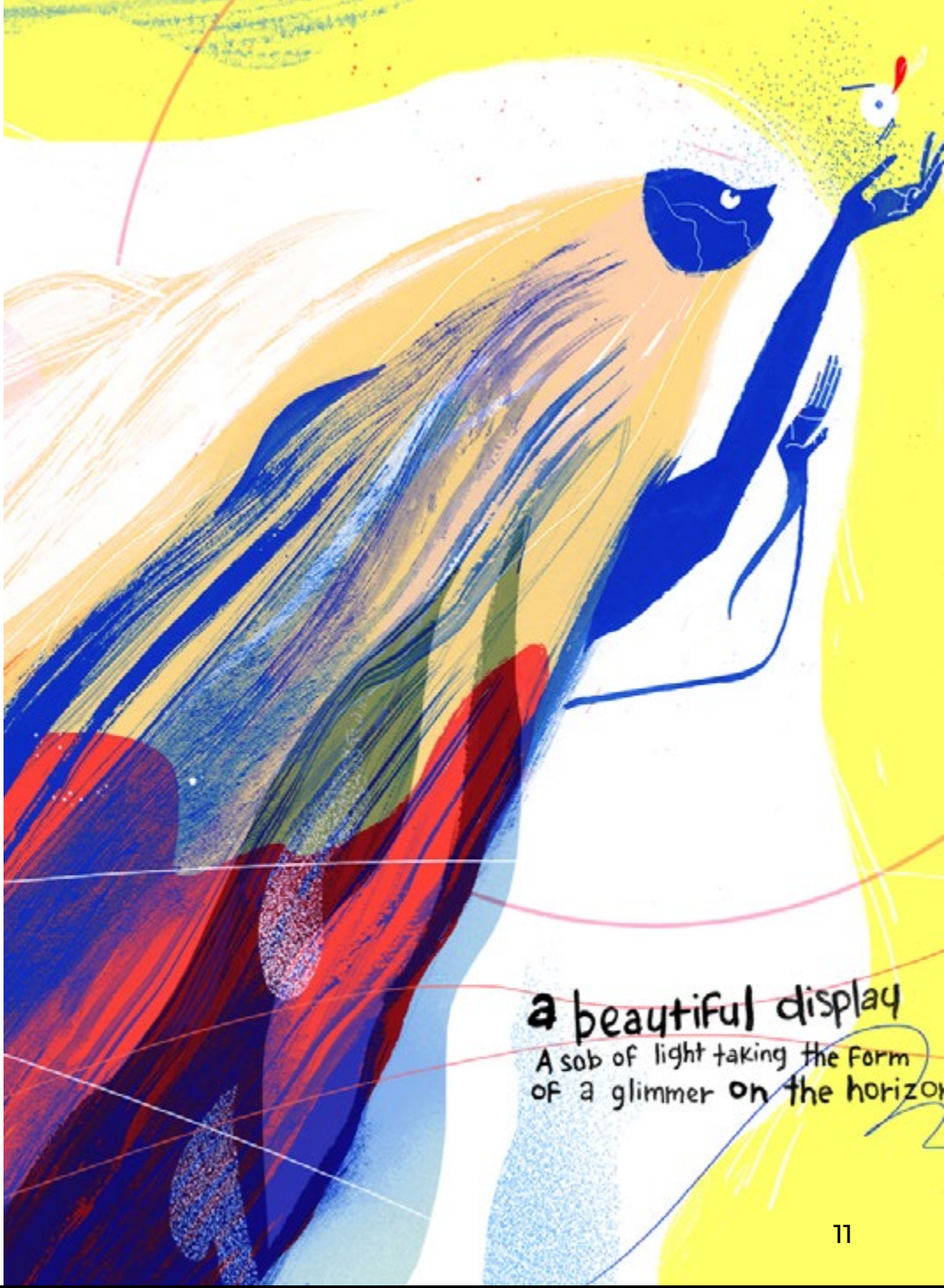
No puedo hacer referencia a un solo artista. Creo que para referirse a la parte creativa y estética de los movimientos y colectivos que trabajan la privacidad y seguridad me interesa mucho más señalar la producción realizada por compañeras ciberfeministas.

Los carteles, memes, fanzines, imagenes, gifs, que generan alrededor de los talleres y eventos que organizan me parecen fascinantes, bellos, inspiradores. Por ello, no puedo hacer referencia a una sola artista.

https://repository.anarchaserver.org/index.php?/category/18

https://repository.anarchaserver.org/index.php?/category/6/start-100#content

Menciones especiales a Anamhoo de Acción Directa Autogestiva / Constanza Figueroa de Derechos Digitales / Nymeria de EnRedadas Nicaragua por su obras artísticas



Fuente: *Molly Mendoza - Voyage*

ALEX HACHE

Ciberfeminista, amante de las tecnologías libres. Es editora de dos volúmenes sobre el panorama de las iniciativas de soberanía tecnológica y le gusta hacer talleres de ficción especulativa (futurotopías feministas) con amigas y activistas.

Es parte del colectivo Donestech que explora la relación entre género y tecnologías desarrollando investigación acción, documentales y formación. Ha coordinado una red internacional para Tactical Tech llamada los institutos de género y tecnología que desarrolla formaciones y contenidos para incluir el género en la privacidad y la seguridad digital.

Fuente: signage of event: Das ist Netzpolitik!

MESH

SEGURIDAD Y PRIVACIDAD DIGITAL BÁSICA

Alex Hache

2019

Technology of love by

Fundació PARE MANEL

SOKO TECH

Amb el suport de l'Ajuntament de Barcelona

Ajuntament de Barcelona

Barcelona Activa