¿Qué es la cultura de seguridad?[1]

La cultura de seguridad es un conjunto de costumbres compartidas por una comunidad, los miembros de la cual pueden ser objetivo del gobierno, diseñadas para minimizar el riesgo. Tener una cultura de la seguridad ahorra a todo el grupo la molestia de tener que elaborar medidas de seguridad continuamente desde cero, y puede ayudar a deshacerse de la paranoia y el pánico en situaciones estresantes — joder, podría incluso mantenerte fuera de prisión. La diferencia entre protocolo y cultura es que la cultura se vuelve inconsciente, instintiva y, por lo tanto, sin esfuerzo; una vez el comportamiento más seguro posible se ha vuelto habitual para todas las personas de los círculos en los que te mueves, puedes dedicar menos tiempo y energía enfatizando la necesidad de ello, o sufriendo las consecuencias de no tenerlo, o preocupándote por el peligro en el que te encuentras, ya que ya sabrás que estás haciendo todo lo posible para ir con cuidado. Si tienes el hábito de no decir nada comprometido sobre ti, puedes colaborar con desconocidos sin tener que preocuparte de si son o no son informadores; si todo el mundo sabe sobre qué no hablar por teléfono, tus enemigos pueden pinchar la línea todo lo que quieran que no les servirá de nada.[2]

El principio central de toda cultura de seguridad, que no se puede enfatizar lo suficiente, es que las personas nunca deberían estar al tanto de ninguna información que no necesitan saber.

Cuanta más gente sepa algo que puede poner a individuos o proyectos en riesgo —ya sea la identidad de una persona que ha cometido un acto ilegal, la ubicación de una reunión privada, o el

1. Extraído de: https://es.crimethinc.com/2004/11/01/que-es-la-cultura-de-seguridad

2. «¿Pero ¿qué pasa con los infiltrados y los informadores?» preguntó un agente de CrimethInc. Hace tiempo en su primera gran movilización. «Los pondremos a pelar patatas» respondió casualmente un organizador experimentado.

plan de una actividad futura— mayor será la probabilidad de que este conocimiento llegue a las manos equivocadas. Compartir tal información con gente que no la necesita les perjudica y les pone en riesgo: les coloca en la incómoda situación de poder arruinar la vida de otras personas con un simple paso en falso. Si son interrogados, por ejemplo, tendrán algo que ocultar, en vez de poder decir honestamente que no saben nada.

No preguntes, no cuentes.

No pidas a otros que compartan información confidencial que no necesitas saber. No vayas fardando de cosas ilegales que tú u otros hayáis hecho, ni menciones cosas que pueden o que van a suceder, ni siquiera hagas referencia al interés de cualquier persona en participar en tales actividades. Mantente alerta cuando hables; no dejes que ciertas alusiones se te escapen sin querer.

Puedes decir no en cualquier momento a cualquier persona sobre cualquier cosa.

No respondas ninguna pregunta que no quieras responder — no solo con la policía, sino que tampoco con otros activistas o incluso con amigos cercanos: si hay algo que no te sientes seguro de compartir, no lo hagas. Esto también significa sentirse cómodo con que otros no respondan preguntas: si hay una conversación que quieren mantener para sí mismos, o te piden que no formes parte de una reunión o proyecto, no deberías tomártelo personalmente — es por el bien de todos que sean libre de hacerlo. Del mismo modo, no participes en ningún proyecto con el que no te sientas bien, ni colabores con nadie con quien te sientas incómodo, ni ignores tu instinto; si algo sale mal y os metéis en problemas, no quieres tener remordimientos. Tu eres responsable de no dejar que nadie te convenza de asumir riesgos a los que no estás dispuesto.

Nunca entregues a tus amigos a tus enemigos.

Si te capturan, nunca, nunca des ninguna información que pudiera poner en peligro a alguien más. Hay gente que recomienda hacer un voto explícito a todos los participantes de un grupo de acción directa: de esta manera, en el peor de los casos, cuando la presión pueda hacer difícil la distinción entre dar algunos detalles inofensivos y venderse totalmente, todos sabrán exactamente el compromiso que han tomado con los demás miembros del grupo.

No le pongas fácil a tus enemigos descubrir lo que estás planeando.

No seas demasiado predictible en los métodos que utilizas, en los objetivos que eliges, o en las horas y lugares en el que os reunís para organizar. No seas muy visible en los aspectos públicos de la lucha en la que haces las acciones directas más serias: mantén tu nombre fuera de listas de correo y fuera de la prensa, tal vez incluso evita asociarte con organizaciones y campañas públicas por completo. Si estás involucrado en actividades clandestinas realmente serias con algunos compañeros, tal vez quieras limitar tus interacciones en público, si no evitaros mutuamente por completo. Los agentes federales pueden acceder fácilmente a los números de teléfono marcados desde tu teléfono, y utilizarán esas listas para establecer conexiones entre individuos; lo mismo pasa con tu correo electrónico, y con los libros que consultas en la biblioteca, y especialmente con las redes sociales como MySpace.

No dejes rastro: el uso de tarjetas de crédito, tarjetas de gasolina, las llamadas de teléfono dejan siempre un registro de tus movimientos, compras y contactos. Ten preparada una coartada, respaldada por hechos verificables, en caso de que necesites una. ¡Ten cuidado con lo que tu basura podría revelar sobre ti — los mendigos no son los únicos que buscan en la basura! Lleva un registro de todo documento escrito y fotocopia incriminatoria — mantenlo todo en un mismo

sitio, para que no te olvides de algo accidentalmente — y destrúyelo tan pronto como no los necesites. Cuantos menos haya en primer lugar, mejor; acostúmbrate a usar tu propia memoria. Asegúrate de que no quedan marcas de escritura en las superficies sobre las que has escrito algo, ya sean mesas de madera u otros papeles. Asume que cualquier uso de ordenadores también deja rastro.

No sueltes en público ideas sobre acciones directas que crees que podrías llevar a cabo algún día.

Al proponer una idea, espera hasta tener un grupo de individuos que esperas que van a estar todos interesados en probarla; la excepción es el compañero íntimo con el que vas a hacer lluvia de ideas y preparar los detalles con antelación — de una manera segura, fuera de tu casa y fuera de otras compañías, por supuesto. No propongas tu idea hasta que creas que es el momento adecuado para llevarla a cabo. Invita solo a esas personas que estás seguro de que van a querer participar — cualquier persona que invites y acabe no participando es un riesgo de seguridad innecesario, y esto puede ser doblemente problemático si resulta que creen que tu actividad propuesta es ridículamente tonta o moralmente incorrecta. Invita solo a gente que puede mantener secretos —esto es crítico acaben o no participando en la acción.

Desarrolla un código secreto para comunicarte con tus camaradas en público.

Es importante encontrar una manera de comunicarse subrepticiamente con la gente de confianza sobre problemas de seguridad y niveles de confort en situaciones públicas, como en una reunión convocada para discutir sobre una posible acción directa. Saber medir los sentimientos de los demás sin que otros se den cuenta de que estás enviando mensajes de ida y vuelta te ahorrará el dolor de cabeza de tener que adivinar los pensamientos

respecto a una situación o individuo, y te ayudará a evitar actuar de manera extraña cuando no puedas llevar a tu colega a un rincón para compartir opiniones. Para cuando hayas convocado a un grupo más grande para proponer un plan de acción, tú y tus amigos deberíais tener claras las intenciones de los demás, su predisposición a correr riesgos, nivel de compromiso, y cuáles son sus opiniones de los demás, para ahorrar tiempo y evitar ambigüedad innecesaria. Si nunca antes has formado parte de un grupo de planificación de acción directa, te sorprenderá lo complicadas que se pueden volver las cosas incluso cuando todo el mundo llega preparado.

Desarrolla métodos para establecer el nivel de seguridad del grupo o situación.

Un método rápido que podéis utilizar al principio de una reunión más grande en la que no todos están familiarizados entre sí es el juego de «garantizar»: cuando cada persona se presenta, cada cual que pueda garantizar a esa persona levanta la mano. Garantiza sólo a esa persona que consideras digna de tu confianza. Con suerte, cada persona estará conectada con los demás a través de algún enlace en la cadena; de cualquier modo, al menos todo el grupo sabrá cómo están las cosas. Un activista que entienda la importancia de la buena seguridad no se sentirá insultado en la situación de que no haya nadie presente que pueda garantizarle y los demás le pidan que se vaya.

El sitio de reunión es un factor importante en la seguridad.

No quieres un sitio que pueda ser monitoreado (no una residencia privada), no quieres un sitio en el que podáis ser observados en grupo (no el parque delante de donde haréis la acción del día siguiente), no quieres un sitio donde puedas ser observado entrando y saliendo o donde alguien pudiera entrar inesperadamente — coloca exploradores, bloquea la puerta una vez se haya empezado,

estate pendiente de cualquier cosa sospechosa.[3] Los grupos pequeños pueden dar paseos y charlar; grupos más grandes pueden reunirse en sitios tranquilos al aire libre — puedes ir de excursión o de campin, si hay tiempo — o en habitaciones privadas en edificios públicos, como en un aula de estudio de la biblioteca o clases vacías. En el mejor de los casos: aunque no tenga ni idea de que estás involucrado en la acción directa, tienes cierta relación con el viejo encargado del café al otro lado de la ciudad, y no le importa dejarte la habitación trasera una tarde para una fiesta privada, sin hacer preguntas.

Ten en cuenta la fiabilidad de quienes están a tu alrededor, especialmente aquellas personas con las que podrías colaborar en actividades clandestinas.

Se consciente del tiempo que hace que conoces a cada persona, cuánto tiempo atrás se puede trazar su actividad dentro de la comunidad y en su vida fuera del círculo de activismo, y cuales han sido las experiencias de los demás con esta persona. Las amistades con las que has crecido, si aún tienes alguna de ellas en tu vida, pueden ser los mejores compañeros de acción directa, ya que estás familiarizado con sus fortalezas y sus debilidades y sus maneras de gestionar la presión — y sabes a ciencia cierta que son quien dicen ser. Asegúrate de confiar tu seguridad y la de tus proyectos solo a gente de nivel que comparten las mismas prioridades y compromiso y que no tienen nada que demostrar. A largo plazo, esfuérzate por construir una comunidad de gente con amistades duraderas y experiencia trabajando juntos, con vínculos con otras comunidades similares.

---

3. Una célula de CrimethInc. nunca olvidará salir de una reunión de alta seguridad en el sótano de una universidad para justo descubrir que mientras estaban encerrados, una multitud de estudiantes manifestantes liberales inundaron la sala contigua para ver una presentación de diapositivas que todos los organizadores del bloque negro militante del día siguiente tuvieron que tragarse con vergüenza.

No te distraigas demasiado preocupándote de si las personas son infiltradas o no; si tus medidas de seguridad son efectivas, no debería importar.

No malgastes energía en volverte paranoico y antisocial sospechando de todos a quienes conoces. Si mantienes toda información sensible dentro del círculo de gente a quien concierne, colaboras solo con amigos de confianza y con experiencia cuya historia puedes verificar, y nunca sueltas información sobre tus actividades privadas, la policía y los informadores serán incapaces de recopilar ninguna evidencia para usar en tu contra. Una buena cultura de seguridad debería hacer que fuera prácticamente irrelevante que esta escoria actúe o no en tu comunidad. Lo importante no es si una persona está trabajando o no con la policía, sino si constituye o no un riesgo de seguridad; si se le considera insegura (doble sentido intencionado), nunca se le debería permitir acabar en una situación en la que la seguridad de alguien dependa de ella.

Entérate y cumple las expectativas de seguridad de cada persona con la que interactúas, y respeta las diferencias de estilo.

Para colaborar con otras personas, tienes que asegurarte de que se sienten como en casa contigo; incluso cuando no estás colaborando con ellas, no quieres incomodarles o ignorar un peligro que entienden mejor que tú. Cuando se trata de planear una acción directa, no respetar la cultura de seguridad aceptada en cierta comunidad puede arruinar no solo las posibilidades de cooperar con otros en un proyecto, sino la posibilidad de que el proyecto llegue a suceder — por ejemplo, si mencionas una idea que otros estaban planeando en un ambiente que consideran inseguro, pueden verse obligados a abandonar el plan, ya que ahora puede estar asociado con ellos. Pídele a la gente que te describa sus necesidades de seguridad específicas antes de siquiera sacar el tema de la acción directa.

Haz saber a los demás exactamente cuáles son tus necesidades en cuanto a seguridad.

El corolario de cumplir con las expectativas de los demás es que tienes que hacer fácil para otros el cumplir las tuyas. Al principio de cualquier relación en la que tu vida política privada pueda ser un problema, enfatiza que hay detalles de tus actividades que necesitas guardarte para ti mismo. Esto puede ahorrarte muchos dramas en situaciones que ya son suficientemente estresantes de por sí; lo último que necesitas al volver de una misión secreta que ha salido mal es acabar en una pelea con tu pareja : «¡Pero si confiaras en mí, me contarías algo de esto! ¿Cómo sé que no estás por ahí acostándote con alguien?» No es una cuestión de confianza — la información sensible no es una recompensa que se pueda ganar o merecer.

Estate atento a las otras personas.

Haz explícito a la gente de tu alrededor qué riesgos puede presentarles tu presencia[4] o qué acciones has planeado, al menos tanto como

---

4. Un ejemplo gracioso de porque esto es importante ocurrió cuando los agentes de CrimethInc. Paul F. Maul y Nick F. Adams intentaban volver a los Estados Unidos continentales después de pasar una temporada escondiéndose en Alaska. Estaban preocupados por lo que pensarían los agentes fronterizos sobre la masiva cantidad de balas de rifle de asalto que llevaban, así que quitaron los paneles de las puertas de su coche y escondieron dentro las balas. De camino a la frontera recogieron a un autoestopista, de aspecto normal y corriente, que parecía inofensivo. En el control de aduanas, ambos trabajadores de CrimethInc aguantaron la respiración mientras los agentes aduaneros comprobaban su identificación, pero se quedaron tranquilos cuando se las devolvieron sin más. Pensaron que iban a poder cruzar la frontera sin problemas hasta que el agente aduanero comprobó la identificación del autoestopista; de repente rodearon el coche oficial armados y les ordenaron salir del coche a punta de pistola. ¡El autoestopista resultó ser un clásico activista de Greenpeace que tenía orden de arresto en treinta países! Los oficiales registraron minuciosamente

sea posible sin violar otros acuerdos de cultura de seguridad. Hazles saber en la medida de lo posible qué riesgos corres tú mismo: por ejemplo, si puedes permitirte ser arrestado o no (si tienes órdenes de arresto encima, si eres un inmigrante indocumentado, etc.), qué responsabilidades tienes que mantener, si tienes alguna alergia. No pongas en peligro a los demás con tus decisiones, especialmente si no podrás ofrecer apoyo concreto si acaban siendo arrestados y acusados por tu comportamiento. Si alguien deja caer un cartel en un sitio cercano de donde has provocado un incendio, la policía podría acusarles de incendio premeditado; incluso si los cargos no se sostienen, no quieres poner a prueba su mala voluntad, o bloquear accidentalmente su vía de escape. Si ayudas a iniciar una marcha separatista que abandona la zona permitida, intenta asegurarte de mantener tu cuerpo entre la policía y las demás personas que han venido pero que no necesariamente entienden los riesgos involucrados; si se intensifica un desfile espontáneo a través de destrucción de la propiedad, asegúrate que las demás personas que no estaban preparadas para ello no se quedan quietas y confundidas cuando aparezca la policía. Sean cuales sean los proyectos arriesgados que emprendas, asegúrate de estar preparado para hacerlo inteligentemente, para que nadie más tenga que correr riesgos inesperados para ayudarte cuando cometas errores.

La cultura de seguridad es un tipo de etiqueta, una manera de evitar malentendidos innecesarios y potenciales conflictos desastrosos.

---

el coche, finalmente quitando los paneles de las puertas, y las balas tintinearon al caer al suelo. Nuestros héroes pasaron las siguientes cuatro horas encerrados en una sala de interrogatorios, policías Canadienses gritando, «¿Dónde están las pistolas? ¡Sabemos que las tenéis, decidnos dónde están!», y haciendo caso omiso a sus quejas: «Esto es un gran malentendido, no tenemos ningún arma. Somos diseñadores gráficos; tenemos las balas para un proyecto de diseño. ¡De verdad, agente!».

¡Las preocupaciones de seguridad nunca deben ser una excusa para hacer sentir apartada o inferior a otra persona — aunque puede requerir cierta finura evitar eso! — al igual que nadie debería sentirse con el «derecho» a entrometerse en algo que otros prefieren quedarse para sí mismos. Aquellas personas que violan la cultura de seguridad de sus comunidades no deberían ser desacreditadas con demasiada dureza la primera vez — esto no trata de ser suficientemente espabilado para poder unirse al grupo interno, sino de establecer expectativas grupales y ayudar amablemente a la gente a entender su importancia; además, la gente es más reacia a aceptar las críticas constructivas cuando se pone a la defensiva. Sin embargo, a esta gente hay que decirle inmediatamente de qué forma están poniendo a los demás en riesgo, y qué consecuencias habrá si siguen igual. Quienes no comprendan esto tienen que ser apartados de cualquier situación de riesgo, con tacto, pero con eficacia.

La cultura de seguridad no es paranoia institucionalizada, sino una manera de evitar la paranoia enfermiza minimizando los riesgos antes de tiempo.

Es contraproducente gastar más energía preocupándote de bajo cuanta vigilancia estás que la que es útil para reducir el peligro que presenta, así como es debilitante tener que estar constantemente cuestionando tus precauciones y dudando de la autenticidad de los camaradas potenciales. Una buena cultura de seguridad debería hacer sentir a todo el mundo más seguro y relajado, no menos. Al mismo tiempo, es igualmente contraproducente acusar a aquellas personas que se adhieren a medidas de seguridad más estrictas que las tuyas de ser paranoicas. Recuerda, nuestros enemigos están tratando de atraparnos.

No permitas que la sospecha juegue en tu contra.

Si vuestros enemigos no pueden descubrir vuestros secretos, se

conformarán con volveros los unos contra los otros. Los agentes infiltrados pueden difundir rumores o lanzar acusaciones para crear disensión, desconfianza y resentimiento dentro o entre grupos. Pueden falsificar cartas o tomar medidas parecidas para incriminar a activistas. Los medios de comunicación convencionales pueden participar en esto comunicando que hay un informador en un grupo cuando no lo hay, o tergiversando la política o la historia de un individuo o grupo para alienar potenciales aliados, o enfatizando una y otra vez que hay un conflicto entre dos ramas de un movimiento hasta que realmente lleguen a desconfiar el uno del otro. Otra vez, una cultura de seguridad astuta que fomente un nivel de confianza apropiadamente alto debería hacer prácticamente imposibles estas provocaciones a nivel personal; cuando se trata de relaciones entre partidarios de tácticas diferentes y organizaciones con diferentes enfoques, recuerda la importancia de la solidaridad y la diversidad de tácticas, y confía en que los demás también lo hacen, incluso si la prensa sugiere lo contrario. No aceptes rumores o informes como ciertos: ves siempre a la fuente original para tener confirmación, y se diplomático al respecto.

No te dejes intimidar con faroles.

La atención y la vigilancia de la policía no son necesariamente un indicador de que saben algo específico sobre tus planes y actividades: a menudo eso indica que no lo saben, y que están intentando asustarte para que abandones. Desarrolla un instinto con el cual poder detectar cuando realmente has sido descubierto y cuando tus enemigos solo están intentando asustarte para que les facilites su trabajo.

Estate siempre preparado por la posibilidad de estar bajo vigilancia, pero no confundas ser vigilado con ser efectivo.

Incluso si todo lo que estás haciendo es perfectamente legal, puedes

recibir atención y acoso de las organizaciones de inteligencia si creen que supones un inconveniente para sus jefes. En ciertos aspectos, esto puede ser algo bueno; cuanto más tengan que monitorear, más dispersas estarán sus energías, y más difícil será para ellos identificar y neutralizar a los subversivos. Al mismo tiempo, no te dejes atrapar por la emoción de estar bajo vigilancia y empieces a asumir que cuanta más atención te prestan las autoridades, más peligroso tienes que ser para ellos; no son tan listos. Tienden a preocuparse por las organizaciones de resistencia cuyos enfoques se parecen más a los suyos; aprovéchate de ello. Las mejores tácticas son aquellas que alcanzan a las personas, presentan argumentos, y ejercen influencia mientras no aparecen en el radar de los poderes existentes, al menos no hasta que sea demasiado tarde. Idealmente, tus actividades deberían ser bien conocidas por todo el mundo excepto por las autoridades.

La cultura de seguridad implica un código de silencio, pero no es un código de «falta de voz».

Las historias de nuestras audaces hazañas en la lucha contra el capitalismo tienen que contarse de alguna manera, para que se sepa que la resistencia es una posibilidad real llevada a cabo por personas reales; deben hacerse incitaciones abiertas a la insurrección, para que los aspirantes a revolucionarios puedan encontrarse y los sentimientos revolucionarios enterrados en los corazones de las masas encuentren su camino a la superficie. Una buena cultura de seguridad debería mantener tanto secreto como sea necesario para que las personas estén seguras en sus actividades clandestinas, mientras que siga proporcionando visibilidad para las perspectivas radicales. La mayoría de la tradición de seguridad en el mundo del activismo hoy en día es derivada de los últimos treinta años de actividades de liberación animal y de la tierra; como tales, son perfectas para las necesidades de pequeños grupos que lleven a cabo acciones ilegales aisladas, pero no siempre son apropiadas

para grupos enfocados de cara al público, pensados en incitar a la insubordinación generalizada. En algunos casos puede tener sentido infringir la ley abiertamente, para provocar la participación de un grupo grande de gente que supondrá más seguridad en los números.

Equilibra la necesidad de evitar la detección por parte de tus enemigos con la necesidad de ser accesible a potenciales aliados.

A la larga, el secretismo de por si no puede protegernos, tarde o temprano van a acabar descubriéndonos, y si nadie más entiende lo que estamos haciendo y lo que queremos, podrán liquidarnos con impunidad. Solo el poder de un público informado y simpatizante (y con suerte equipado similarmente) podrá ayudarnos entonces. Siempre debería haber maneras de entrar en las comunidades en las que se practica la acción directa, para que más y más gente pueda unirse. Aquellos que estén llevando a cabo acciones realmente serias deberían mantenerlo en secreto/privado, por supuesto, pero cada comunidad debería también tener una persona o dos que abiertamente sean partidarias y eduquen sobre la acción directa, y que pueda ayudar discretamente a los novatos de confianza entrar en contacto con otros para empezar.

Cuando estés planeando una acción, empieza por establecer el nivel de seguridad apropiado, y actúa en consecuencia a partir de ahí.

Aprender a evaluar los riesgos que plantea una actividad o situación y cómo lidiar con ellos adecuadamente no es solo una parte crucial de mantenerse fuera de prisión; también ayuda saber qué es lo que no te preocupa, para no desperdiciar energía en medidas de seguridad innecesarias y engorrosas. Ten en cuenta que una acción concreta puede tener diferentes aspectos que exigen diferentes grados de seguridad; asegúrate de mantenerlos diferenciados. Aquí hay un ejemplo de un posible sistema de calificación para niveles de

seguridad:

1. Solo quienes están directamente involucrados en la acción saben de su existencia.

2. Personas de confianza también conocen la existencia de la acción, pero el grupo decide conjuntamente qué personas serán estas.

3.Se permite al grupo invitar a personas que podrían decidir no participar; es decir, gente fuera del grupo sabrá que existe la acción, pero se espera que la mantengan en secreto.

4. El grupo no tiene una lista estricta de quien está invitado; los participantes son libres de invitar a otros y animarlos a hacer lo mismo, enfatizando que el conocimiento de la acción debería mantenerse en círculos de gente en quien se puede confiar para guardar un secreto.

5. «Rumores» sobre la acción pueden correr a lo largo de la comunidad, pero las identidades de quienes están en el centro de la organización se mantienen en secreto.

6. La acción se anuncia abiertamente, pero con al menos cierto grado de discreción, para no alertar a las autoridades más perezosas.

7. La acción es anunciada públicamente por todas partes y de todas las maneras posibles.

Para mostrar ejemplos, el nivel de seguridad #1 sería apropiado para un grupo planeando incendiar un concesionario, mientras que el nivel #2 sería aceptable para aquellos planeando acciones de destrucción de propiedad menores, como hacer pintadas con spray. El nivel #3 y #4 serían apropiados para llamar al consejo de portavoces precedente a un Black Bloc en una gran manifestación o para un grupo planeando enviar un comunicado anónimo a un periódico, dependiendo en la ratio de riesgo frente la necesidad de números. El nivel #5 sería perfecto parar un proyecto como empezar

una marcha sorpresa no permitida: por ejemplo, todo el mundo oye con antelación que la actuación de Ani DiFranco va a acabar en una «espontánea» marcha antiguerra, así que la gente puede prepararse para ello, pero como nadie sabe de quien es la idea, nadie puede ser señalado como organizador. El nivel #6 sería apropiado para anunciar una pedalada de Masa Crítica (evento ciclista): se enganchan panfletos informativos en los manillares de las bicicletas de todas las bicicletas de la calle, pero no se comunica nada a la prensa, para que la policía no esté ahí des del principio mientras la masa aún es vulnerable. El nivel #7 es apropiado para una marcha antiguerra permitida o una proyección de videos independiente, a no ser que seas tan disfuncionalmente paranoico como para querer mantener tus proyectos de acercamiento a la comunidad en secreto.

También tiene sentido elegir el medio de comunicación que usaréis de acuerdo con el nivel de seguridad requerido. Este es un ejemplo de los diferentes niveles de seguridad en la comunicación, correspondientes al sistema descrito más arriba:

1. Ninguna comunicación sobre la acción excepto en persona, fuera de las casas de las personas involucradas, en espacios libres de vigilancia (ejemplo: el grupo se va de camping para planearla); no se habla de la acción excepto cuando sea absolutamente necesario.

2. Fuera de las reuniones del grupo, las personas involucradas son libres de hablar de la acción en espacios libres de vigilancia.

3. Se permite hablar en casas que con seguridad no estén bajo vigilancia.

4. Se acepta la comunicación a través de correo electrónico encriptado o con teléfonos neutrales.

5. La gente puede hablar de la acción por teléfono, correo electrónico, etc. teniendo cuidado de no revelar ciertos detalles: quién, qué, cuándo, dónde.

5. Los teléfonos, correo electrónico, etc. están bien; listas de correo, flyers en espacios públicos, anuncios en periódicos, etc. pueden o no ser aceptables, en función de cada caso concreto.

7. Se recomienda la comunicación y la proclamación por todos los medios posibles.

Si mantienes la información peligrosa fuera de circulación y sigues las medidas de seguridad adecuadas en cada proyecto que emprendas, estarás bien encaminado para conseguir lo que el agente de los inicios de CrimethInc. Abbie Hoffman describió como el principal deber del revolucionario: que no te pillen. Te deseamos lo mejor en tus aventuras y desventuras, y recuerda — ¡Nosotros no te hemos contado nada!

¿Qué es el Doxxeo?[1]

Doxxear significa publicar la información privada de una persona con el objetivo de exponerla e intimidarla. Esto puede provocarle un daño físico, emocional y económico. Se hace con la intención de disuadir al objetivo de actuar y humillarlo por sus ideas y valores. Por ello, es importante plantearnos seriamente la cultura de la seguridad antes de que nos doxeen — antes de que tengas motivos para temer de un posible doxxeo. Normalmente el doxxeador esperará a recolectar la información necesaria antes de exponerla. Es posible que ya estés siendo vigilado sin saberlo hasta que ya sea demasiado tarde.

Seas un activista público bastante reconocido, o alguien que no se entromete mucho, deberías proteger todas tus redes sociales y otras esferas de tu vida — incluso si crees que no estás haciendo nada que merezca atención. Mantener una buena práctica protege a tus amigos, tu familia y tu comunidad. Es común que grupos derechistas incluyan en sus teorías aquellos que son queer o trans, que «parece un izquierdista», tocan en bandas, van a eventos o frecuentan espacios radicales. La información no debe ser correcta o justificada para que alguien te tenga como objetivo. Lo único que necesita un acosador es una sola pieza de información para empezar a indagar más detalles en la red.

Ser consciente de los rastros de información que dejas en internet puede protegerte tanto de las fuerzas del orden como de los acosadores. Ahora que la vigilancia impuesta por el Estado es cada vez más sofisticada, y que los directos en redes sociales se han normalizado en las protestas, ya no basta con llevar un simple tapabocas. En Junio de 2020 en Philadelphia, los investigadores identificaron a una mujer con tan sólo una imagen difuminada de ella. Siguieron un rastro de migas, aparentemente minucioso, que incluía una compra en Etsy, su cuenta de Twitter y su

1. Extraído de: https://es.crimethinc.com/2020/08/26/doxcare-prevention-and-aftercare-for-those-targeted-by-doxxing-and-political-harassment

página de trabajo profesional. El Servicio de Aduanas y Protección de Fronteras ha empezado a rastrear las redes sociales públicas. Proteger tu presencia en internet puede hacerte sentir más seguro al actuar fuera de estas redes.

MÁS VALE PREVENIR QUE CURAR

El mejor momento para empezar es ahora, pues después de haber sido doxxeado, probablemente, seas incapaz de eliminar la información expuesta incluso tratando de quitarla de la red.

Hay muchas maneras de tratar este tema. Obviamente, la mejor forma de asegurarnos de que nadie pueda encontrar información sobre ti es no tener nada al alcance de nadie — pero no todo el mundo puede eliminar su presencia de internet, sea por trabajo, familia, u otras responsabilidades. En algunos casos, existen razones estratégicas para mantener cierto tipo de persona online; por ejemplo, tener un perfil en alguna red social de hace mucho tiempo, creíble pero innocuo, **puede ser útil** para los no-ciudadanos estadounidenses que tratan de **cruzar la frontera**. Afortunadamente, hay muchas formas de compartimentar las distintas esferas de tu vida, de crear un perfil público si lo necesitas y de adoptar prácticas que te ayuden a ti y a tus amigos a sentiros capacitados para seguir actuando en tu comunidad. Este proceso puede resultar tedioso. Requiere tiempo y energía. Recomiendo realizar esto con amigos, compañeros de piso o familiares para que te ayuden en algunos de los aspectos difíciles o aburridos.

MANTENER ESFERAS SEPARADAS

Si no puedes borrar tu huella digital por completo de Internet, aún puedes preservarse una relativa privacidad manteniendo distintas

esferas[2] de actividad online y limpiando las cuentas olvidadas o de uso poco frecuente.

Es probable que tengas más de una presencia online. Esto incluye redes sociales, tableros de mensajes, sitios de trabajo, cuentas de correo electrónico — cualquier cosa en la que necesites entrar. A menudo, en el doxxeo, la información se triangula a partir de muchas fuentes distintas. Una forma de reducir la cantidad de información disponible para los doxxeadores es compartimentar estas esferas para que no estén conectadas entre sí. Este es un proceso completamente individualizado; tómate un tiempo para considerar las siguientes preguntas y mapear tu propia esfera online.

¿Pasas las horas mirando foros como r/politics o debatiendo en el muro de un conocido de Facebook? ¿Interaccionas con alguna cuenta radical de Instagram o Twitter? ¿Tienes imágenes o información personal en tableros de ofertas laborales? ¿Compras por Etsy o eBay? ¿Uno de tus amigos publica una foto tuya en su cuenta de Instagram? ¿Tienes que promocionarte online para el tipo de trabajo al que te dedicas? ¿Hablas con tus compañeros de trabajo, familiares, y amigos activistas con la misma cuenta? ¿Utilizas parte de tu nombre real o tu fecha de nacimiento para los nombres de usuario o los correos electrónicos?

Cada uno de estos no tiene porqué ser un problema como tal, pero juntos pueden crear vínculos entre las diferentes esferas de tu vida.

Pregúntate:

-¿Cuán separadas están cada una de estas cuentas/identidades?

-¿Qué es público? ¿Qué es privado?

-¿Qué significa público-privado en el contexto de cada sitio?

-¿Qué puede encontrarse al buscar tu nombre legal?

---

2. El concepto de esferas aquí empleado se lo debemos a Smiling faces collective: https://smilingfacecollective.github.io/guide-to-preventing-doxxing/

-¿Utilizas el mismo nombre de usuario o correo electrónico en múltiples cuentas? ¿Se cruzan en tus distintas esferas de vida? Tómate tu tiempo para pensar en la forma en que todas estas esferas se superponen fuera de Internet.

-¿Tu trabajo te permite hablar abiertamente de tu política?

-¿Cuán público es tu activismo? ¿Hablas con periodistas? ¿Trabajas en una infoshop?

-¿Filtras parte o todo el contenido de tus redes sociales de tus familiares?

-¿Hay referencias a actividades ilegales o controvertidas en un perfil determinado?

He aquí algunos ejemplos de cómo tu presencia online puede superponerse en distintos sitios:

Familiares

¿Hasta qué punto es abierta la relación entre tú y tus familiares de sangre/legales? Si un extraño tuviera información sobre una sola persona de esta red, ¿qué podría descubrir sobre las demás?

Política

¿Discutes o publicas sobre tus pensamientos políticos online? Si es así, ¿en qué redes sociales?

Amigos y Comunidad

Si tienes redes sociales, ¿quiénes son tus amigos? ¿Tus seguidores? ¿De qué formas tus comunidades online reflejan tus comunidades en la vida real?

Hobbies

¿Qué hobbies tienes? ¿Tienes amigos y comunidad a través de ellos? ¿Eres parte de alguna comunidad de Internet dedicada a esos hobbies?

Legal

¿Quién eres en papel? ¿A qué nombres, números de teléfono, direcciones estás vinculado? ¿Alguna de tus cuentas incluye esta información? ¿Lo hace algún otro sitio (probablemente sin tu permiso)?

Profesión

¿Tu trabajo implica una presencia online, un sitio web o una cuenta en alguna red social? ¿Habría algún problema si tus políticas se superpusieran con tu profesión? O, ¿tu profesión está de alguna forma vinculada a tu identidad política?

Tómate el tiempo necesario para considerar el punto donde se cruzan, cuáles son tus objetivos online y dónde puedes separar estas esferas.

TÁCTICAS

Hablemos de cómo descubrir qué tipo de información nuestra está disponible, cómo identificar y eliminar los rastros, y qué herramientas online existen para eliminarlos.

Empieza con lo que esté disponible públicamente. Búscate en Google y haz una lista de todas tus redes sociales. Elimina las cuentas antiguas que ya no utilices. También es un buen momento de descargarse un *password manager* como 1Password o LastPass para facilitarte en manejar nombres de usuario, correos electrónicos y contraseñas concretas.

ELIMINA LOS SITIOS DE ESPIONAJE/BRÓKERS DE INFORMACIÓN

Averigua qué información puede encontrar la gente sobre ti utilizando un motor de búsqueda. Búscate a ti mismo en DuckDuckGo y Google. Intenta hacerlo en modo incógnito. Prueba con distintas versiones de tu nombre, con o sin tu segundo nombre y entre comillas. Puedes configurar Google Alerts para que te envíe un correo cada vez que tu nombre sea publicado en Internet. Esto te dará una perspectiva de cuanta información sobre ti hay disponible online a la gente que no es de tu red (de confianza).

Después de esta búsqueda inicial, dales una ojeada a todos los sitios de brókers de información (Data Brokers) que se benefician del comercio de datos personales. También te animo a que elimines al mismo tiempo a tus familiares más cercanos. Este proceso puede ser arduo; estos sitios intentan dificultar al máximo la eliminación de información sobre uno mismo. Hay algunas de las que no puedes borrarte — por ejemplo, si te has registrado para votar y aún vives en esa dirección. (Este es otro motivo por el que la gente decide no votar).

Los sitios de alojamiento con más tráfico incluyen: Been-verified, CheckPeople, Instant Checkmate, Intelius, PeekYou, PeopleFinders, PeopleSmart, Pipl, PrivateEye, PublicRecords360, Radaris, Spokeo, USA People Search, TruthFinder.com, Nuwber, OneRep, y FamilyTreeNow. Recomiendo empezar por estos buscando cada uno de ellos en esta **página web**[3], que tiene una guía para excluirse de prácticamente todos los DataBrokers. Si tienes más dinero que tiempo, puedes pagar por un servicio llamado **Just Delete Me**[4] para que eliminen tu información, aunque normalmente recomiendo este servicio si ya has sido doxxeado.

---

3. https://joindeleteme.com/help/diy-free-opt-out-guide/
4. https://onlinesos.org/blog/i-tried-abine-delete-me-to-get-my-info-off-data-broker-websites

ELIMINA TUS ANTIGUAS CUENTAS

Cuando te buscas a ti mismo en un motor de búsqueda online, es probable que también te encuentres con cuentas antiguas. Puede ser beneficioso realizar una búsqueda inversa utilizando todos los nombres de usuario y alias antiguos que puedas recordar. Cuentas que no hayas utilizado en mucho tiempo pueden hacerte vulnerable porque si utilizaste en ellas una antigua contraseña, pueden probar el soporte técnico de esa cuenta para obtener más información sobre ti, y que pueden usar para otras cuentas. Descarga todo el material que tengas con valor sentimental y cierra indefinidamente todas las cuentas que ya no utilices. Éstas pueden estar llenas de pistas sobre tu vida.

Primero, entra en esta **página web**[5], que busca en cientos de plataformas nombres de usuario específicos, y busca todos los posibles nombres de usuario y correos electrónicos que hayas utilizado. Esto te dirá qué plataformas tienen cuentas con ese nombre.

Segundo, entra en esta **página**[6] y escribe el dominio del sitio web. Esta página web archiva una gran variedad de sitios webs existentes, clasificando por cuán sencillo o difícil puede ser borrar una cuenta, además de proporcionar el enlace a la página de «eliminar perfil» de cada sitio.

Haveibeenpwned.com[7] facilitará averiguar si hay alguna brecha de información en alguna de tus cuentas. Si la hay, toma medidas inmediatas para cambiar las contraseñas. [NdT: realizar este proceso de revisión de forma trimestral, cada dos semanas, cada mes, o las que consideres necesarios, pero nunca confiar en una simple y única revisión.]

---

5. https://namechk.com/
6. https://backgroundchecks.org/justdeleteme/
7. https://haveibeenpwned.com/

CAMBIA NOMBRES DE USUARIO, DIRECCIONES DE CORREO ELECTRÓNICO Y CONTRASEÑAS

El método más sencillo de que alguien encuentre más información sobre ti es buscar tu nombre, tus alias y tu nombre de usuario. Con el fin de mantener las esferas de actividad en Internet separadas, utiliza *siempre* un nuevo nombre de usuario cuando crees una cuenta. Si tienes una página web profesional para el trabajo que requiera de tu nombre de usuario, asegúrate que el correo electrónico utilizado para esa cuenta sea destinado para ese único propósito. Es posible que acabes teniendo un sinfín de correos electrónicos y nombres de usuario. Por ejemplo, yo tengo una sola para todas mis cuentas médicas y gubernamentales, otra para mis compras online, otra para mi vida política, otra para mis redes sociales, otra para los sitios de cita, etc. Utilizo alias e información falsa para todos los sitios web que me representan o muestran fotos mías.

Un gestor de contraseñas es una gran ayuda para esto, pues almacenará los inicios de sesión de todas tus cuentas. Recomiendo **LastPass**.[8] que puedes descargar en tu móvil y navegador. Sería tentador dejar la sesión abierta permanentemente, pero asegúrate siempre de cerrar la sesión cuando termines de usarla. En concreto, para no olvidar la contraseña maestra — y también para asegurarte de que incluso si alguien consigue acceder a tu móvil u ordenador, no puedan tener acceso a tus datos personales. Aprovecha este momento para crear nuevos correos electrónicos y cambiar los nombres de usuario de todas las cuentas que no vayas a eliminar. Puedes crear fácilmente nuevos correos electrónicos utilizando **Protonmail**.[9] Tanto 1Password como LastPass pueden ayudar a generar contraseñas de cadenas aleatorias, que son las más seguras.

---

8. https://www.lastpass.com/es/solutions/business-password-manager
9. https://protonmail.com/

CURA LO QUE ESTÁ DISPONIBLE Y CAMBIA TU CONFIGURACIÓN DE PRIVACIDAD

Una vez que hayas eliminado todos los cabos sueltos, ojea lo que decidiste conservar y lo que se puede encontrar de ahí. Si conservas alguna cuenta en las redes sociales, revisa tu perfil y anota lo que la gente puede encontrar sobre ti. Puedes elegir una entre una serie de estrategias sobre cómo enfocar esto, dependiendo lo cauteloso que quieras ser y lo seguro que estés de que es posible mantener tus diferentes esferas de actividad en Internet diferenciadas.

Algunas de las opciones incluyen:

-Eliminando todas las fotos en las que salgas tú y tus mascotas, tu buzón, tus tatuajes, y todo aquello que incluya información innecesaria pero identificatoria — especialmente de tu foto de perfil pública.

-Borrando o falsificando cualquier detalle personas de tu perfil — proporciona una fecha de nacimiento falsa o, directamente, no la des, elige una localización falsa de tu ciudad natal, de las escuelas a las que fuiste, y más información por el estilo.

-Eliminando seguidores o amigos dudosos. Si cambias toda la configuración de tus redes sociales a privado y te sientes seguro con tu depurada lista de seguidores, hay menos motivos para esconder tu cara. Sigo recomendando mantener los detalles de tu localización y tu vida personal íntima fuera de Internet. Recuerda que sólo estás tan seguro como la persona más abierta de tu vida. Si decides ser más público, mantén a tus amigos y familiares por separado, sin publicar fotos de ellos o información personal suya sin su consentimiento, y recuerda que las conexiones sociales son visibles a través de las redes sociales y los sitios web de recopilación de datos.

El **C.O.A.C.H**[10] de Crash Override Network es una guía útil paso a

10. http://www.crashoverridenetwork.com/coach.html

paso que te enlaza directamente con la página de configuración de la privacidad de muchas redes sociales. Haz click en «Let's Get Started» y en «Strengthen the security of my online accounts so people can't break into them as easily», y sigue sus guías para todas las principales compañías de redes sociales. Esta guía también puede ayudar con otros aspectos de la seguridad online, así que después de hacer eso, te recomiendo que termines las ayudas del Coach y compruebes qué otros recursos ofrecen.

Cuando creas haber terminado, pídele a un amigo que se haga pasar por un «doxxeador» y que intente crear un perfil basado en la información que pueda encontrar sobre ti para comprobar que no se te haya escapado algo por alto. Puede ser importante comprobar periódicamente lo que se puede encontrar buscando tu nombre cada pocos meses.

SI HAS SIDO DOXXEADO

No recomendamos dirigirse a la policía cuando hayas sido (alguna vez) doxxeado. La policía puede utilizar esta información proporcionada sobre los acosadores, pero también utilizará esta información obtenida sobre ti y otros individuos y grupos en los que hayas estado asociado públicamente. Una vez que esta información está archivada, estará permanentemente en sus manos, y no hay garantía de que no la utilicen para atacarte a ti o a otros mediante la represión del Estado.

Si decides implicar a la policía, por favor sé transparente y no preguntes a ningún grupo radical que te apoye. Asegúrate de informar de tu decisión a cualquier grupo en el que estés involucrado. Generalmente, la policía no hará nada o empeorará de más la situación. La idea de esta guía es proporcionarte alternativas basadas en el apoyo de la comunidad y el empoderamiento.

¿DEBERÍA HACERLO PÚBLICO?

Respuesta breve: No reacciones inmediatamente en público. Tómate tu tiempo para asegurarte y alertar a tus redes en privado antes de reaccionar públicamente.

Tu primer impulso puede ser alertar a tanta gente como sea posible de inmediato con un anuncio público, o cerrar todas tus redes. Hacerlo público puede proporcionarte un apoyo inmediato si tienes una audiencia solidaria, pero conlleva el riesgo de que aumenten las agresiones de los acosadores. Hay buenos argumentos para ser cuidadosos con la información al principio. Lo más importante es tomar medidas para protegerte a ti y a tus redes contra un mayor daño.

Los anuncios inmediatos pueden complicar tus esfuerzos de seguridad. Tanto si la información publicada sobre ti es cierta o no, es probable que nadie la utilice para causarte un daño grave sin confirmar primero al menos parte de ella. Publicar en una de tus cuentas confirmando tu doxxeo aprueba inmediatamente que la información sobre ti es exacta; también indica que has visto dónde se ha publicado y sugiere que estás aterrorizado. Esto favorece los objetivos de tus acosadores. Quieren intimidarte y aislarte.

No confirmes ni niegues ninguna de las informaciones que han desenterrado sobre ti, independientemente de que sean falsas o embarazosas. Buscan una reacción. Si les haces saber que lo que están publicando es incorrecto, pueden llegar a la conclusión de que van por buen camino y que sólo tienen que seguir indagando. A veces, una de las respuestas públicas más efectivas es no responder a nada — no hagas ningún cambio importante en tus hábitos de publicación ni muestres miedo. Esto puede enviar la señal a tu doxxeador de que no dio en el blanco, y que el ataque fue un fracaso.

Una vez que hayas tenido tiempo para procesar tus sentimientos y asegurar tu posición, sería estratégico hacerlo público y quizás unirte a otras personas que estén en una situación similar. Puedes

aprovechar la indagación pública (por los supremacistas blancos) para crear una campaña que disuada el uso del doxxeo — por ejemplo, ¡haz una campaña de financiación con promesas de dar dinero por cada correo electrónico de acoso que tú u otras personas de tu comunidad hayáis recibido! Dado que tus acosadores quieren aislarte, un apoyo público como éste puede disuadir de una mayor intimidación. Intenta ser creativo, resistente y estratégico. Sé cuidadoso de no poner en peligro a nadie más en este proceso.

Al hacer declaraciones públicas, si presumes o alardeas de tus habilidades, de tu capacidad para emplear violencia, de las armas que dispones para defenderte, o exageras tu ferocidad, puedes morder más de lo que puedes masticar. Por norma general, no es buena idea tergiversar la información sobre ti. Hablar directa o indirectamente con los acosadores no suele mejorar las cosas. Recomiendo hacer una declaración positiva afirmando tu ética y tus creencias, describiendo cómo tu identidad o tus ideales te han convertido en un objetivo, pero manteniendo que, aunque estas campañas de acoso pretenden acobardarte, no lo harás, porque no tienes razón alguna para ocultar tu política. Evita hablar de acciones o grupos concretos, estés o no involucrados con ellos.

INMEDIATAMENTE DESPUÉS DE SER DOXXEADO

No temas. Llama a un amigo cercano para que venga a darte apoyo.

Crea un registro de incidentes y mantén un registro de las provocaciones tanto online como fuera de Internet. Esto es crucial para identificar los patrones de los ataques. Puede ser útil compararlos con los de otros organizadores para identificar patrones más amplios y así poder identificar a tus adversarios y sus organizaciones.

Avisa a tus amigos, familiares y redes políticas sensible por privado. Encarga a algunos amigos en los que confíes tu información

personal a que te ayuden a denunciar las publicaciones en redes sociales y blogs que te doxxen, identificándolas como acoso. Repite este proceso las veces que sean necesarias. Algunas plataformas carecen de políticas que te protejan, incluso si estas publicaciones incluyen información personal precisa, incluso si te ponen en peligro. A veces, los doxxeadores usarán tus fotos e información para crear cuentas impostoras. Suele ser más sencillo reportarlas como falsas; intenta hacerlo rápidamente para evitar que obtengan más información de tus redes haciéndose pasar por ti. Es posible que tú, tu familia y tus compañeros de trabajo comiencen a recibir llamadas telefónicas amenazantes o de acoso. Hazles saber lo que está ocurriendo tan pronto como puedas para que no se relacionen con los acosadores.

Detén el flujo de información. Si estás leyendo este apartado sin haber hecho los cuidados preventivos expuestos, comienza este proceso. Descarga un gestor de contraseñas como 1Password o LastPass y cambia de inmediato todas tus contraseñas. También puedes pagar por un servicio llamado **Delete Me**[11] que eliminará gran parte de tu huella digital de los sitios de espionaje [Snoop Sites] que recogen y monitorean información personal. Este servicio se encargará de la información agregada por los brókers de datos [Data Brokers], pero no de las redes sociales, las cuentas web, los artículos de noticias o los registros de arresto que pueda tener — estos deberán ser manejados por uno mismo. Es importante equilibrar la hemorragia de información mientras, al mismo tiempo, no se alerta a los acosadores de que el doxxeo fue efectivo o hizo diana. Intenta asegurar tus cuentas en las redes sociales haciendo que las listas de amigos y la información sean privadas para proteger tus redes hasta que estés seguro de que no ofrecen información personal vulnerable a quienes estén dispuestos a indagar en ella. Cómo reaccionas públicamente es una situación muy delicada y debe manejarse con cuidado durante todo este proceso.

---

11. https://onlinesos.org/blog/i-tried-abine-delete-me-to-get-my-info-off-data-broker-websites

Establece un plan de seguridad. Recluta a amigos y familiares para que te den soporte. Hazles saber qué está pasando; el doxxeo puede ser traumático y debes priorizar tu salud mental y física para poder superar estos ataques. Estas conversaciones pueden ser difíciles — especialmente si no entienden los matices de este momento político, si es la primera vez que oyen hablar de un grupo de odio en particular, o si tus relaciones son tensas debido a diferencias políticas o personales. Si no te sientes capaz de hacerlo, puedes pedir a un amigo que tenga experiencia en estos asuntos que mantenga las conversaciones más difíciles por ti.

Si la dirección de tu casa está incluida en el doxxeo, a ser posible, busca un nuevo lugar en el que puedas quedarte. Si no puedes salir de tu casa, invita a tus amigos o a un grupo de seguridad local a quedarse contigo. Haz una «mochila de emergencia» (Go-Bag) con todo lo necesario si tienes que hacer las maletas e irte con poco margen de tiempo.[12]

EVALUANDO LAS AMENAZAS

Si no sientes que corres ningún gran riesgo, especialmente si tu doxxeo se compone de información de libre acceso o simplemente te lo envían directamente con la intención de ponerte nervioso, puede que te sientas bien desechándolo como una táctica de intimidación barata, bloqueando y denunciando al acosador, y pasando página. Es posible que sólo se trate de alguien intentando sacarte de quicio. Sin embargo, si el doxxeo incluye información personal sensible, con detalles específicos que son difíciles de encontrar sin un buen

---

12. Nota añadida de traducción: en motores de búsqueda como Google, ofrecen un servicio de atención a la privacidad de petición a eliminar todo contenido que involucre una vulnerabilidad a tu intimidad, apelando al Derecho al Olvido, sin necesidad de otorgar información adicional que no sea tu nombre y correo electrónico: https://support.google.com/legal/troubleshooter/1114905

método de espionaje, o aparece en un foro público donde la gente distribuye información con la esperanza de que otros actúen sobre ella, es posible que quieras tomar precauciones más serias. Esto es especialmente cierto si ya formas parte de un grupo (demográfico) señalado.

Cuando sepas que has sido doxxeado, es importante establecer qué información podría traducirse en amenazas creíbles. A menudo, el doxxeo es un precursor de un acoso más intrusivo fuera de Internet, o está relacionado con amenazas de actuar en base a la información. Esto podría significar cualquier cosa, desde llamadas telefónicas a tu familia o puesto de trabajo hasta amenazas de muerte o una llamada a los SWAT.

A veces es complicado determinar qué hace que una amenaza sea «creíble». La táctica más común de los doxxeadores ordinarios es enviar mensajes extraños o intimidantes allí donde creen que pueden llegar a ti — redes sociales, correos electrónicos, familiares, etc. A menudo insinúan que tienen más información de la que en realidad poseen; es común en ellos que digan que han proporcionado esta información a las fuerzas de seguridad locales. Su objetivo es intimidarte para que no actúes; a menudo, la información que publican es la única que tienen.

La empresa en la que trabajas puede recibir llamadas exigiendo que te despidan. Hasta ahora, es raro que los objetivos del doxxeo hayan sido atacados físicamente, pero *ha pasado*, y es posible que quienes te doxeen se esfuercen por hacer llegar tu información en manos de quienes no actúan de forma racional o ética. Es importante ser cauteloso, no entrar en pánico ni sumergirse en la ansiedad.

Pregúntate:

-¿Es esta información cierta? ¿Tienen la dirección de tu casa, trabajo o familiares? ¿Conocen los lugares que sueles frecuentar? ¿De quiénes eres amigo?

-¿Estás en riesgo de perder tu trabajo si encuentran cierta

información tuya?

-¿Sabes dónde vive el acosador? ¿Son cercanos a tu comunidad física o son meros trolls de Internet en un foro descentralizado? ¿Tienes motivos para creer que los cuerpos de policía estén interesados en esta información?

-¿La información que se comparte proviene de fuentes locales de noticias de la derecha, poniendo tu cara frente a una multitud de extraños hostiles que ahora tienen tu información?

-¿Tienen alguna foto tuya embarazosa o especialmente íntima?

-¿Existe información que te vincule a una actividad criminal que pueda provocar tu detención?

SOLUCIONES

He aquí algunas cosas que puedes hacer en respuesta a los peligros que pueden surgir por ser doxxeado:

-Crea un plan de autodefensa, contacta un grupo de defensa comunitario de tu zona.

-Informa a la gente y grupos mencionados en el doxxeo — puestos de trabajo, camaradas, compañeros de piso, familia.

-Habla de tus miedos con la gente que confías.

-Contacta con la gente que ya haya pasado por este proceso para pedirles consejo.

-Planea tener un abogado disponible si te preocupa que la información sobre ti pueda ser de interés para los agentes del Estado.

-Contacta con grupos antifascistas de tu zona — puede que te ayuden a identificar a los doxxeadores en caso de que haya sido publicado desde una cuenta falsa.

MANTÉN CONVERSACIONES CON EL TRABAJO Y LA FAMILIA

Esta conversación puede ser muy difícil, especialmente si tu relación con tu familia no es favorable. Ten a mano un amigo con la cabeza fría para que te ayude a mediar o te apoye después si es necesario.

Piensa en la frecuencia con la que estás dispuesto a ser vulnerable con tu familia y en las oportunidades que se te avecinan para seguir la conversación. Si es necesario hablar con la familia, pero crees que sólo tendrás una sola oportunidad, puedes ensayar con un amigo y prepararte para sus reacciones. Si tienes una relación estable, conversacional y de confianza, puedes explicarles la situación en una serie de pequeñas conversaciones, en vez de una larga sentada. Evalúa cuánto tiempo y cuánta atención vas a tener.

Siempre me ha ayudado enmarcar esto como si «tuviera un acosador» a las personas con las que no quiero tener una conversación política — eso puede ser suficiente para explicarles la gravedad del asunto y el por qué necesitas privacidad. Esto puede ser de ayuda para construir relaciones más sólidas y desmitificar este hecho tan común, a la vez que anima a otras personas que quizás no se hayan planteado que pueda ocurrirles a ellos, o a alguien cercano, a tomarse en serio la privacidad online. La mayoría de la gente responderá con miedo y simpatía, aunque a veces sugerirán, e incluso insistirán, en que llames a la policía.

No hay un enfoque exclusivo para todos. En mi caso, tuve que obligar a mi conservadora madre a prometer que no involucraría a la policía. Lo hice apelando a mi derecho a la seguridad personal y a mi autonomía como víctima de la situación, pidiéndole que respetara mis deseos y recordándole que la policía puede hacer muy poco para responder a un acoso selectivo como éste — y que lo único que conseguiría acudiendo a ellos sería exponerme a su escrutinio, pues se me acusaba de actividad criminal. Recuerda a tus amigos y familiares que no deben reaccionar ni responder a las

llamadas telefónicas, los correos electrónicos o las solicitudes de las redes sociales.

Puedes leer una guía sobre cómo discutir esto con tu empresa/ compañeros de trabajo **aquí.**[13]

Cosas que debes recordar cuando hables con tus amigos y familiares:

-El objetivo del acusador es aislarte de tus relaciones y arruinar tu vida. No permitas que se salga con la suya. Dile a tu familia que la mejor forma de apoyarte es evitando caer en sus tácticas.

-No vendas a los anarquistas y antifascistas o afirmes que estás siendo atacado sin razón. Esto no te servirá si surgen razones — y sólo deslegitimará y pondrá en peligro a aquellos que no pueden distanciarse de la política anarquista.

-No dejes que nadie te culpe de lo que está pasando, ya sea por la política a la que te adhieres o por tu supuesta irresponsabilidad por haberte metido «en esta situación». Luchar por un mundo mejor implica desafíos. En cualquier caso, tiene el mérito de haber provocado esta respuesta por tus esfuerzos.

-Sugiere formas concretas en las que puedas ayudarles a entender la situación y a protegerse. Envíales este artículo o una lista de recursos; ofrécete a ayudarles a bloquear sus redes sociales si no tienen experiencia con la tecnología.

-Háblales de a lo que pueden prepararse — llamadas de teléfono amenazantes, correos electrónicos, quizás los vecinos reciban mensajes sobre ti. Prepáralos para el peor de los casos, pero haz hincapié en que es poco probable.

-Sé claro sobre lo que necesitas de ellos.

---

13. http://www.crashoverridenetwork.com/employers.pdf

VIVE TU VIDA, AVANZA

Respira profundamente. No te martirices. Emocionalmente esto puede ser verdaderamente inquietante y perturbador, con un toque de estrés agudo en tu vida. Es posible que haya gente que sepa cómo eres y no tengas ni idea de quiénes son. A veces, la información de los doxxeadores se convierte en una parte permanente en Internet si tu nombre es googleado; esto puede afectar a tus perspectivas de trabajo. En ocasiones, nada ocurre con la atención — pero la constante posibilidad de que alguien intente continuar donde lo dejó el último doxxeador existe.

Hasta que estés seguro de que tu tiempo en el punto haya finalizado, puede que tengas que modificar algunos aspectos de tu vida. Pregúntate, «¿Qué tipo de vida quiero llevar? ¿Cómo puedo paliar mi ansiedad? ¿Hay formas de aceptar ser una figura más pública? ¿Cómo puedo volverme a sentir seguro al asumir riesgos y volver a ser activo?». Especialmente, a medida que se intensifican las tensiones políticas, puede ser importante extremar las medidas de seguridad.

He aquí algunas de las medidas que puedes emplear:

-No dejes que nadie te fotografíe, a menos que confíes en que manejará las imágenes de la manera que necesitas. Esto puede acarrear conversaciones incómodas, especialmente en eventos familiares o en situaciones laborales. Sé consciente de quién aparece en las fotos contigo; informales de que aparecer en una foto contigo puede atraer una atención no deseada. Puede ser útil ensayar las conversaciones que puedas necesitar.

-Instala cámaras de seguimiento en tu casa.

-Lleva un registro de todo el acoso que experimentas.

-Si te mudas, no actualices tu dirección. No te registres para votar, pues esto hace pública tu dirección. Intenta conservar tu antiguo carné de conducir o documento de identidad y recibe el correo en un apartado de correos. Considera cuándo utilizar tu

dirección real y cuándo usar una falsa u omitir tu dirección en sitios web.

-Si es necesario, utiliza pseudónimos online y en persona. No utilices el mismo constantemente.

-Cuando vayas a acciones, y más si no te cubres la cara, presta atención de qué grupos, lugares o individuos podrían estar implicados a ser vistos o fotografiados en tus alrededores.

-Invierte tiempo en clases de defensa personal. Esto puede incluir el entrenamiento con armas, pero debería ser suficiente el entrenamiento defensivo y de desarme.

-Visita un terapeuta para trabajar cualquier trauma que hayas experimentado.

-Ayuda a tus amigos y familiares a entender la importancia de la seguridad online.

-Ten conversaciones honestas con personas fuera de tus círculos de afinidad política. Puede sorprenderte cuánta empatía pueden mostrar.

No importa la intensidad con la que tus acosadores traten de aislarte, no estás solo. Como comunidad, debemos protegernos los unos a los otros y a nuestras redes online del acoso, el encarcelamiento, la violencia política y la intimidación. Juntos, podemos hacerlo.

La Paranoia Maquínica

[varias compas nos hemos reunido con la finalidad de exponer nuestras ideas de eventos que recién afectan con gravedad en nuestras comunidades con la intención de mezclar nuestras voces y distorsionar la melodía rítmica del capitalismo][1]

Despertar en esta ensordecedora calamidad presente suma un día menos en la continuidad del vacío organizado. Prolongamos la tortuosidad de la vida en la cáscara transitada, comúnmente dictada «ciudad», desplazando el cuerpo de semáforo en semáforo, de tienda en tienda, de metro en metro… del trabajo a casa. «Sin Esperanza, Sin Futuro», aquello que decían unos, «¡Estáis locos!», les respondían otros. Cada generación es el resultado de un proceso incestuoso entre el individuo y la ciudad. No impresiona pues la cantidad de cuerpos errantes a la deriva al latido colectivo del civismo. El ciudadano es un sin sentido, carece de alma. Sólo le impulsa el miedo, si bien canalizado como responsabilidad. Viste con el exo-esqueleto proporcionado al salir del útero: la moral. Desnudarse, hoy, como ayer, en medio de la ciudad, es un acto incívico, por ende, criminal. Gestionar que todo cuerpo tenga la indumentaria reglamentaria implica un largo proceso de sometimiento, bien lo saben los cultistas de la civilización. Las ciudades cumplen el rol fundamental de esta vigilancia —que se lo pregunten sino a las víctimas Vagas y Maleantes—, la arquitectura se alza simulando una omni-presencia panóptica. Pero estas, como si de un ser vivo tratase, evolucionan. Más preciso, metamorfosean. No es que el individuo perdiera sus sentidos, sino que, como una ofrenda, les fueron otorgados a la ciudad. Cada ciudadano conforma un panóptico. La macrovigilancia estatal se convierte en una microvigilancia que, a su vez, es una macrovigilancia, pues cada individuo no es sino un elemento constitutivo de la sociedad.

---

1. Extraído de https://refractarixscxlectixs.wordpress.com/2020/06/18/la-paranoia-maquinica/

La arquitectura panóptica de las ciudades se inutiliza, caduca, deja de tener la eficacia que se creía tener ante la evolución de la tecnología. Quienes creían que la mejora de los elementos tecnológicos traería la automatización, la liberación del hombre del trabajo por las máquinas, no comprendían que, al contrario de lo que deseaban, la tecnología automatizaría la naturalización del trabajo en la vida. Nace un nuevo milagro civilizatorio: las Smart-Cities. En ellas, el algoritmo será el nuevo carcelero. Detecta, controla, clasifica, monitoriza todo lo que su lente capta. Sin descansos, ni turnos, ni rotaciones de puestos. No hay puntos ciegos, allá donde creas que exista uno, estará el ciudadano-panóptico [bien podría abreviarse en paco] para controlar-te.

En la ecografía de la ciudad el modelo principal es la centralización, la focalización en un punto que irradia externamente; una visión en escala muestra el pico más alto en el centro y una disminución al llegar a los márgenes, la periferia. En la Smart-City el resultado es todo lo contrario pues presenta un modelo descentralizado, requiriendo de un campo de cuatro dimensiones para comprender la funcionalidad de este sistema. Digamos, si el panoptismo de la ciudad era una estructura centralizada, con la acelerada aparición tecnológica de las Smart-Cities lo importante es la descentralización. Descentralizar para expandir, sin perder calidad, fuerza, intensidad, forma. El ciudadano hace de efecto espora. Vaya donde vaya segrega organismos invasivos. A este ritmo constante, las smart-cities no darán siquiera margen de tiempo a la desertificación de las metrópolis.

Es costumbre en los revolucionarios lanzar una mirada nostálgica ante cualquier elemento histórico. Confunden la consideración para el aprendizaje con la idolatría en un altar de las formas dominantes de entonces. Los ojos le tintinean cuando habla de las barricadas formadas en cualquier calle, que deja de ser calle para ser un nuevo altar —véase cómo la Plaza Baquedano devino Plaza de la Dignidad, en un rebautizamiento popular en el que formalizar toda asamblea. Sus voces claman «Saber levantar una barricada no quiere decir

mucho si al mismo tiempo no se sabe cómo vivir detrás de ella», pero olvidan, igual que olvidaron los promulgadores de la automatización tecnológica. Y será demasiado tarde, cuando vean que las barricadas forman parte de las Smart-Cities, como un complemento de más. «Saber cómo vivir detrás de una barricada no quiere decir mucho si al mismo tiempo no se sabe cómo hackearla.», dicen los refractarios.

La cuestión que florece de este infértil terreno tiene como semilla la incertidumbre de una nada autoritaria en el horizonte: ¿existe alguna posibilidad de resistencia? Y, sobre todo, ¿resistencia a qué? Los revolucionarios suponían ser los que se oponían al sistema establecido, pero incluso ellos forman parte del entramado de subjetividades del poder. Mientras, los enjuiciamientos a hermanas siguen. Las condenas nos persiguen. La represión nos intimida. Las torturas nos trauman. La muerte es el último bastión. No hay tiempo para la reflexión. El constante ritmo de las smart-cities incapacita todo proceso mental de recapacitación hacia un esquema mental inmóvil.

Ante este paradigma, la paranoia se instaura en nuestro sistema nervioso como un no-sentido. Similar a la araña que se sitúa en el núcleo de su telaraña —convirtiéndose en una extensión somática de sí, capaz de percibir a sus presas clasificando las percepciones según su criterio—, la paranoia puede ser una herramienta que construya redes con nuestro entorno, estableciendo contactos afectivos, discernir la hostilidad mediante la vibración única de cada individuo que se nos aproxima. Siguiendo con el símil. La telaraña converge desde su centro hilos maquínicos para semiotizar la fuente externa de la araña, como medio de transcripción que facilite la detección fuera de sí. El individuo se aposenta en su centro, tejiendo hilos [sociales] entre sí y otro extremo con el que intercambiar información, mapeando su entorno con la intención de crear una imagen mental de los puntos de fuga viables para su acción, evaluando la peligrosidad de cada situación con anticipación. Esto, claro, ocurre si la paranoia del individuo es proactiva. Es decir, el individuo domina la paranoia y la utiliza en beneficio propio y

mutuo. En caso contrario, la paranoia resulta ser un nuevo elemento hostil ajeno a nuestra semiótica significante, pues no hay que olvidar que el agravamiento de la paranoia es consecuencia de la anulación de nuestro instinto neuronal de cazadores-recolectores, de la lobectomización civilizatoria.

Poco a poco dentro de las comunidades se da a conocer la importancia de la Cultura de la Seguridad, un aspecto esencial si queremos generar conexiones firmes basadas en la confianza mutua y en la afectividad que plante cara a la mercantilización de toda forma de vida. Sin embargo, el estigma de la paranoia permanece intenso, provocando incluso un efecto opuesto al esperado: la desconfianza. La causa de este pre-juicio tiene su origen en la constante sensación de guerra, de vigilancia, de posiciones y hostilidades; la única forma de combatirla sin ser vistos como enemigos —pues incrementaría exponencialmente los efectos adversos— es considerando toda estrategia de autodefensa un peligro, una extrañeza, algo a evitar. Hay que batir el duelo, enfrentarse al miedo, pactar con la muerte, aceptar la paranoia como instrumento favorable y no como un tabú a evitar.

En algún rincón de _____, 2020.

¿Es un/a confidente?[1]

Un grupo de gente que ha sido afectado de forma directa por agitadores confidentes ha compilado esta lista, utilizando tanto experiencias personales como información filtrada sobre los agitadores. Esperamos que el daño sufrido pueda utilizarse con la finalidad de evitar que estas personas sufran consecuencias tardías.

He aquí diez señales de advertencia:

1. Algo se siente «fuera de lugar». Algo en ellos no encaja. Sus historias sobre su activismo o su vida suenan a patraña. En este punto, tienes que hacer una comprobación de antecedentes y criminal. Si esperas a otras señales, puede ser demasiado tarde. La causa más evidente de preocupación es cuando alguien aparece de la nada en una comunidad activista, pareciendo no haber existido anteriormente. Esto debería ser un factor de ruptura ipso facto.

2. A pesar de las dudas de algunos miembros, el individuo en cuestión asciende rápidamente a una posición de liderazgo. Se atribuye vigorosamente el mérito de las acciones frente los medios de comunicación, promocionándose a sí mismo/a. Se esfuerza por convertirse en la «cara» de la organización y, claramente, quiere ser el símbolo del grupo, intentando «marcar» su identidad con el nombre del grupo, así como el imaginario y la identidad. Le gusta que le fotografíen, incluso realizando acciones ilegales.

3. Fotografía acciones, reuniones y a gente que no debe ser fotografiada. Publica fotos de las acciones y reuniones en redes sociales como Facebook, incluso etiquetando a los activistas sin su permiso (en consecuencia, facilitando la vigilancia estatal).

4. Es un/a mentiroso/a. Muestra signos de falta de ética y falta de transparencia con el resto del grupo.

---

1. Extraído de: https://es.crimethinc.com/2013/07/06/is-she-an-informant-a-ten-point-checklist

5. Aboga por una acción ilegal de alto riesgo ante gente que no debería confiar, mientras afirma comprender la importancia de la cultura de la seguridad. Incita a otros a realizar acciones violentas, por ejemplo, diciéndoles que deben ser «guerreros». Considerando las acciones ilegales propuestas uno ve que no tienen ningún propósito real y no harán avanzar los objetivos del grupo de ninguna manera significativa. La persona suele tener una percepción muy retorcida de lo que significa ser un guerrero.

Busca grietas internas en la comunidad para poder explotarlas. Tiene un ciclo de abuso con el grupo y los individuos: un periodo de luna de miel, seguido de un comportamiento manipulador y abusivo, seguido de disculpas y promesas de hacerlo mejor. Entonces el ciclo se repite.

6. Siempre tiene dinero para todo tipo de gastos, pero ni tiene un trabajo real y, aunque lo tuviera, no podría permitirse tantos gastos. Puede dar a entender que tiene acceso a un fondo fiduciario o a recursos similares, pero esto debe ser comprobado. De alguna manera siempre tiene la libertad económica de estar en cualquier acción que atraiga la atención de los medios de comunicación, o cualquier acción clandestina que pueda implicar una actividad ilegal.

7. Se descubre que miente sobre cosas tan graves como la identidad, la familia, el origen, la raza o la etnia.

8. Tiene órdenes de detención, pero no tiene miedo de anunciar y promover acciones ilegales, utilizando su nombre real, anunciando públicamente su paradero y, de nuevo, chupando cámara cada vez que se hace una acción ilegal. Cuando se le detiene, siempre tiene que pagar una fianza para quedar en libertad, a veces bajo caución juratoria incluso cuando los cargos son muy graves. Esto ocurre a menudo. Entonces el individuo vuelve a las reuniones, a tomar fotos y a chupar cámara. Tiene un ciclo de captura-liberación con la policía. Puede tener un historial de salidas muy tempranas de la cárcel, para luego ir

directamente a las reuniones políticas, a veces de grupos que dice odiar en privado, o que habrían sido prohibidas, como condición de la libertad condicional normal.

9. La información con sustancia, que sólo se da al confidente sospechoso, surge del lado de las fuerzas del orden. Para asegurarnos de que esto es así, la información debe ser inconfundible y haber sido compartida cara a cara, de tú a tú, con cero posibilidades de vigilancia (digamos, susurrada al oído del confidente en medio del campo).

10. Confesión completa: «Mi nombre es _____ y fui contratado por la [agencia] para infiltrarme en [organización].» Una confesión completa de la condición del confidente y/o agitador puede incluir detalles de lo que el confidente-agitador recibió a cambio de su trabajo: ya sea la cantidad de dinero que se le pagó, o el trato que obtuvo al salir de la cárcel, o evitar el enjuiciamiento por determinados delitos. En algunos casos, el trato incluye un enchufe en las fuerzas del orden o en las agencias de inteligencia que los contrató. En la improbable posibilidad de que uno de ellos sea un enfermo mental [sic], esta información puede cotejarse con el precio de los confidentes-agitadores; pero si el resto de criterios cumplen, hay que suponer que están diciendo la verdad, incluso si son enfermos mentales. Si bien los enfermos mentales no son considerados informadores fiables, pueden ser excelentes agitadores, y su historial de inestabilidad puede citarse como evidencia cuando las fuerzas del orden niegan que el individuo haya sido contratado como agitador.

Si una persona cumple cualquiera de los criterios más allá del primer punto al tercero, no deberías cooperar con ellos. Con suerte, todos los puntos más allá del primero no tendrán relevancia alguna en tanto que ya habrás cortado lazos con ellos desde la primera advertencia [red-flag]. A pesar de que podamos demostrar que alguien es un infiltrado, si muestra alguno de los comportamientos problemáticos expuestos, no debería formar parte de nada sensible. Incluso si

aún no son un infiltrado, ofrece motivos para creer que podrían convertirse o agrietarse en un interrogatorio.

He aquí otras señales de advertencia a las que prestar atención. Cuando se trata del comportamiento cotidiano de las personas, fuera de las reuniones y las acciones, ¿se comporta la persona sospechosa inapropiadamente con los niños? ¿Lastiman a sus parejas? ¿No pueden mantener las manos alejadas de los niños? O, ¿están intentando tener relaciones íntimas con múltiples personas del grupo (o con alguno de los líderes)? Asegúrate de que no haya un pedófilo recién liberado a cambio de la alteración, o un violador en serio o un maltratador al que se le haya encomendado entrar en una comunidad activista para causar estragos. Hay que considerar cómo estas personas nunca se enfrentan a las consecuencias de las fuerzas del orden, incluso cuando las víctimas presentan cargos. Si hay un caso sólido contra un acosador, y este se le permite huir para ir a reuniones políticas en otra jurisdicción mientras los federales se niegan a extraditarlo para ser juzgado… bingo.

En nuestra experiencia reciente, un acosador que cumplía nueve de los diez criterios expuestos (incluido el décimo: la confesión a otros activistas a los que intentaba convertir) nunca fue condenado por las fuerzas del orden. En lugar de ello, se le asignó infiltrarse en una serie de comunidades activistas en las que causar estragos y destrucción. Sólo su muerte puso fin a ello. Pero hay muchos más como él, deseosos de ocupar su lugar. Algunos de ellos pueden estar en tu lista de amigos de Facebook. Algunos pueden haberse salido literalmente con la suya.

Cuando se trata de la espinosa cuestión de los agentes agitadores y la acción directa, la cuestión no es si es preferible la violencia o la no violencia, sino si alguien ha violado el consenso de su grupo de afinidad y ha puesto a su grupo en peligro sin su consentimiento. Es irresponsable alegar que la violencia es siempre obra de agentes infiltrados; más bien, los agentes infiltrados se proponen instigar una violencia que resulte desventajosa o aislante para los participantes.

He aquí un ejemplo. Alguien que cumplió todos los criterios, salvo el noveno y décimo punto, se presenta en una marcha pública. La marcha se ha planificado como un evento pacífico y legal. Quizás no todas las acciones de este grupo sean pacíficas y legales, pero para este evento, esa es la estrategia acordada. El evento está cubierto mediáticamente, la gente utiliza sus nombres reales y participan ancianos y niños. El agitador ha pasado meses intimando con el grupo, presentándose a cada acción, pagando las facturas, llevando a la gente, diciendo lo que otros quieren oír, incluso comprándoles droga. Pero una vez que la marcha comienza y las cámaras grabando, el agitador procede a no mostrar ninguna consideración por la seguridad o el consenso del grupo. Hace todo lo que puede para cambiar el estado de ánimo de la muchedumbre, para instigar y fomentar las emociones fuertes.

Basta con ver vídeos de acciones en protestas en YouTube para ver cómo algunas personas se graban a sí mismas en acciones infringiendo la ley. Algunos vídeos incluyen este momento álgido. Presta atención a quién hace qué; quién cumple y quién no recibe condena.

Los agentes con experiencia pueden ser difíciles de detectar. Pero la mayoría de los infiltrados no son agentes del orden entrenados. La mayoría son delincuentes a los que se les ha ofrecido un trato si simplemente van a las reuniones y escuchan, o si van a las reuniones y acciones para perturbar.

En nuestra experiencia, ha habido unos pocos casos, aunque significativos, en los que los activistas han errado en sus sospechas. En un caso de hace tiempo que afectó a muchos de nosotros, esta identificación errónea tuvo consecuencias devastadoras. El error fue por la falta de pruebas y de experiencia por parte de quienes realizaron la identificación errónea y a la ausencia de criterios sólidos con los que evaluar la situación — sin mencionar la participación de agentes reales en el chivo expiatorio de una mujer inocente. En consecuencia, de este grave error, muchos activistas lo agravaron

yendo al otro extremo, pasando por alto descaradas señales de peligro e incluso admisiones directas de la condición de infiltrado. Al proporcionar esta lista de comprobación pretendemos ayudar a desarrollar la capacidad para identificar, y priorizar, la verdad en estas situaciones. No es una «mala praxis» [bad-jacketing] cuando es verdad.

Sé seguro, sé eficaz y confía en tu instinto.

UTOPÍAS PIRATAS: REFLEXIONES FINALES HACIA UNA AUTODEFENSA DIGITAL[1]

> «Los piratas y corsarios del siglo XVIII crearon una 'red de información' que envolvía el globo: primitiva y dedicada primordialmente a negocios ilegales, la red funcionaba admirablemente. Repartidas por ella había islas, remotos escondites donde los barcos podían ser aprovisionados y cargados con los frutos del pillaje para satisfacer toda clase de lujos y necesidades. Algunas de estas islas mantenían 'comunidades intencionales', una verdadera red mundial de agrupaciones invisibles que vivían conscientemente fuera de la ley y mostraban determinación a mantenerse así, aunque fuera sólo por una corta -pero alegre- existencia.»[2]

La reciente polémica por la política de privacidad de Whatsapp ha desencadenado una serie de debates sobre la importancia de la ciberseguridad y el rol de las corporaciones en el uso de la tecnología y la información personal. Lo que comenzó como una forma sofisticada de mostrarnos publicidad en internet, se está transformando en una herramienta política sin precedentes para los Estados, que utilizan estas tecnologías para la vigilancia, la represión y el control social.

Esto ocurre en un contexto local de revuelta y pandemia. La vigilancia satelital, la geolocalización vía GPS y la creciente inversión en infraestructura y tecnologías para la vigilancia son la expresión de un estado policial que busca un mayor control social. Las excusas de la gestión de una crisis sanitaria y el mito neoliberal de la «seguridad ciudadana» son utilizadas para vulnerar el principio de inocencia

1. Fragmento extraído del texto completo de Grupo Solepnosis disponible en la siguiente página: https://lapeste.org/2021/01/vigilancia-masiva-tecnocapitalismo-y-estado-policial-analisis-critico-y-estrategias-de-autodefensa-digital/

2. Hakim Bey, *Zona Temporalmente Autónoma*.

del sistema penal al someter a la población a la constante mirada vigilante y omnipresente de la policía, facilitada por la tecnología.

Al mismo tiempo, en la región chilena se impulsan leyes represivas y dispositivos jurídicos para la persecución política y la potencial criminalización de «ciudadanos peligrosos». La modernización de la ANI, la Ley de Delitos informáticos y el TPP-11 buscan sentar bases institucionales para la implementación de sistemas de vigilancia. Estas iniciativas reflejan el rol del Estado como el brazo armado del Capital transnacional, utilizando el monopolio de la fuerza, la diplomacia de los tratados internacionales y el blindaje jurídico para facilitar el saqueo extractivista en la región.

Actualmente avanzamos en todo el mundo hacia sociedades de vigilancia total que nos recuerdan la distopía Orwelliana de 1984. Las grandes potencias se disputan la infraestructura y el control de la información, siendo el 5G la última de sus manifestaciones. Desde dispositivos móviles, micrófonos, cámaras de celulares y notebooks hasta drones y satélites, todos tributan a una red global de información al servicio de las grandes corporaciones y de los Estados más poderosos. El propósito es claro: el control del Big Data y la infraestructura de las comunicaciones permitirá a los gobiernos totalitarios saber virtualmente todo lo que hacen todas las personas en todo momento, en cualquier parte del mundo.

Donde hay poder hay resistencia. Hoy nos encontramos en una etapa de transición en la cual mantenerse informados y desarrollar una posición crítica resulta fundamental para anticiparnos a lo que viene. Las organizaciones civiles con enfoque de derechos han denunciado públicamente el sistema de videovigilancia por reconocimiento facial y la geolocalización como contrario a los derechos humanos, a la ley, a la constitución, y a los pactos internacionales de derechos civiles y políticos. Frente a esto han realizado campañas para solicitar mayor regulación e impulsar una reforma a la normativa sobre protección de datos personales, un debate democrático en el Congreso previo a la implementación de esta tecnología y solicitando aumentar la

fiscalización por parte de autoridades estatales de control, apelando a una reforma de los programas policiales de vigilancia. Sin embargo, estas iniciativas parten de la premisa de que el propósito del estado es protegernos.

Desde una perspectiva ácrata, apuntamos a la organización y a la autodefensa digital como la mejor forma de enfrentar el asedio de vigilancia masiva por parte de los estados totalitaristas. Millones de personas alrededor del mundo están desarrollando colaborativamente sistemas operativos, navegadores y softwares que protegen nuestros datos de los gobiernos y las empresas, utilizando código abierto y los principios del software libre.

Colectivos como RiseUp ofrecen aplicaciones y servicios de correo, VPN y almacenamiento seguro de datos, sustentados en los principios del software libre y el establecimiento de una red internacional de colaboración y comunicación entre experiencias y proyectos antiautoritarios. En la región chilena, grupos como el Colectivo Disonancia proporcionan información y material educativo totalmente gratuito sobre criptografía digital o cómo cifrar nuestras comunicaciones.[3]

Existe una larga lista de aplicaciones y sistemas operativos disponibles para organización y comunicación cifrada. Motores de búsqueda como DuckDuckGo que no almacenan la información del usuario. Redes sociales como Mastodon y Diaspora o Jitsi son alternativas a Facebook, Twitter y Zoom. Aplicaciones de mensajería cifrada y de código abierto como Signal, Telegram o Briar se han vuelto cada vez más populares. El principal problema es el monopolio de las redes sociales y aplicaciones de mensajería de las grandes empresas transnacionales. Una red social no funciona sin personas. Sin embargo, no debemos subestimar el poder de la contrainformación y la capacidad de las personas de cambiar sus hábitos en el uso de tecnologías cuando alguien se da el tiempo de explicarles las implicancias de esta decisión: luego de la polémica por las políticas

3. https://colectivodisonancia.net/

de privacidad, Telegram tuvo 25 millones de descargas en todo el mundo, en sólo 72 horas.[4]

Al mismo tiempo, artistas y diseñadores han desarrollado técnicas y dispositivos *Do It Yourself* para hackear el reconocimiento facial: maquillajes, joyas y jockeys con luces LED.[5] Otras personas han diseñado vestuario y estuches para celulares que impiden el rastreo satelital de celulares por GPS.[6] Colectivos anarquistas y antidesarrollistas en la región europea están implementando el proyecto *Low Tech Magazine*, realizando tutoriales para implementar una red de internet autónoma con infraestructura de baja tecnología[7], además de redes de pares o P2P, que implican una participación colectiva en cómo se organiza la comunicación en línea.[8] Grupos de economía social y solidaria en distintas regiones están utilizando blockchain y aplicaciones móviles de código abierto para realizar intercambios comerciales con moneda social, una forma de economía comunitaria anticapitalista.[9] En 2018, una empresa de cartografía rusa hizo desaparecer los sitios de operaciones militares sensibles en Turquía e Israel, lo que acabó revelando su existencia e impulsó a algunos usuarios a localizar estos sitios en otros mapas de código abierto.[10] En la región chilena, el grupo Evade la Vigilancia realizó un mapeo de las cámaras de vigilancia en el territorio con

---

4.https://www.technologyreview.es/s/11282/si-no-regulamos-las-imagenes-de-satelite-nos-vigilaran-las-24-horas

5. https://umap.openstreetmap.co/en/map/ubicacion-de-camaras-de-vigilancia-en-chile_2598#4/-38.34/-71.46

6. https://www.dw.com/es/telegram-gana-25-millones-de-usuarios-en-72-horas/a-56211248

7. https://blogs.publico.es/strambotic/2019/10/burlar-reconocimiento-facial/

8. https://cnnespanol.cnn.com/2012/04/29/como-enganar-a-la-tecnologia-de-reconocimiento-facial/

9. https://solar.lowtechmagazine.com/es/2015/10/how-to-build-a-low-tech-internet.html

10. https://colectivodisonancia.net/autonomia/redes-p2p/

la plataforma *uMaps* basada en *Open Street Maps*, una plataforma gratuita, colaborativa y de código abierto.[11]

El capitalismo, en la medida en que adquiere mayores niveles de complejidad y dificultad para administrar sus contradicciones internas y el malestar latente, ha comenzado a implementar mecanismos de control social cada vez más eficientes, utilizando los últimos avances científicos y tecnológicos e impulsando a su vez el desarrollo de nuevas tecnologías con esta finalidad. El Estado chino es hoy la principal manifestación de esta forma de capitalismo, y su camino a controlar la infraestructura de comunicaciones en Abya Yala está pavimentado representando una importante amenaza a la autonomía de la región.

Cuando la empresa de navegación asistida *Waze* de Google prohibió reportar controles policiales en las ciudades, la gente comenzó a reportarlos como "animales muertos". Debemos aprovechar la inteligencia colectiva para utilizar las mismas tecnologías en nuestro beneficio. La adaptabilidad de nuestra especie a estas nuevas formas de represión parece necesaria, y los planteamientos teóricos del transhumanismo parecen coherentes. Sin embargo, tenemos que considerar que no son aplicables en todos los contextos, como en zonas del no-ser, regiones del Sur Global devastadas por la guerra, el totalitarismo y el necrocapitalismo. Aprender nociones básicas sobre *baja* tecnología y computación permitiría fortalecer una red de agrupaciones invisibles como foros y comunidades internacionales compartiendo información de forma invisible a la vigilancia del Capital-estado gracias a plataformas de videollamada como Jitsi desarrolladas por personas anónimas que deciden colaborar en ello como forma de resistencia política pero no es una solución para todos.

Dmytri Kleiner, activista por el software libre, planteaba que los hackers no pueden solucionar el problema de la vigilancia: «La vigilancia masiva y el control social no son un problema técnico

11. https://monedapar.com.ar/funcionamiento-del-sistema/

que requiera más expertos en programación ni en ingeniería: sólo a través de la vinculación con movimientos sociales y su organización podemos enfrentarlo».[12] Esto nos lleva a pensar en lo que Silvia Rivera Cusicanqui planteaba como la necesidad de desarrollar *una ética india y una técnica occidental*.

12. https://colectivodisonancia.net/2020/11/un-desafio-colectivo-para-enfrentar-la-vigilancia/

APLICACIONES Y PRECAUCIONES BÁSICAS PARA AUTODEFENSA DIGITAL EN LA PROTESTA[1]

MENSAJERÍA

SIGNAL: Para una mensajería segura y fácil de usar, es recomendable Signal. Posee cifrado completo, de extremo a extremo, y posibilidad de autodestruir todos sus mensajes. Existen otras opciones aún mejor, como Matrix o XMPP, pero requieren de algunos conocimientos para su adecuada configuración.

Algunos consejos extras para un uso más seguro en Signal:

-Dependiendo del grado de peligrosidad al que estés expuesto, conviene utilizar un teléfono de usar y tirar [burner pone] para registrarte. Puedes utilizar un número VOIP si no dispones de una tarjeta SIM anónima.[2]

-Para evitar cualquier peligro de que la IP se filtre, activar la opción de recibir llamadas únicamente a través del servidor de Signal; en caso de poder evitarlo, mejor.

-Utiliza un PIN para bloquear Signal, no sólo para fortificar tu seguridad, sino para prevenir que alguien intercambie las tarjetas SIM con el objetivo de recibir los mensajes destinados a ti. Si hacía falta mencionarlo, usar un PIN distinto al configurado para el bloqueo de tu móvil es primordial.

-Configura tus notificaciones para que no aparezcan en tu pantalla incluso estando bloqueado.

- Coméntale a la persona correspondiente de borrar antiguos mensajes que consideres vulnerables.

---

1. Extraído de: https://colectivodisonancia.net/protestas-autodefensa-digital/

2. https://mysudo.com/

-Hacer uso de los mensajes de autodestrucción en caso de compartir información sensible.

-A pesar de los mensajes de autodestrucción y la encriptación de Signal, conviene no discutir nada por mensajería. Recuerda, la mejor forma de encriptar es borrando cualquier (meta)rastro.

-Borra regularmente mensajes de tu móvil; nunca se sabe cuándo puedes "perder" tú móvil.

-Como colofón, de nada sirve tener la mejor configuración posible si la principal brecha de seguridad es el mismo usuario. Por poner un ejemplo: En 2018, se filtraron unas conversaciones entre el expresidente de la Generalitat de Catalunya C.Puigdemont con el exconsejero Toni Comín. La información obtenida ocurrió por algo tan simple como tener el brillo de la pantalla de móvil al máximo en un espacio público, facilitando la lectura de los mensajes y vulnerando cualquier muro de seguridad.

FOTOS EN EL MÓVIL

Scrambled Exif: Antes de compartir una fotografía, es necesario borrar sus metadatos (GPS, modelo de móvil, etc) para que no sea identificado quién la comparte. Para usarla, una vez instalada, hay que compartir la foto a esta aplicación, que limpiará los metadatos y luego permitirá volver a compartirla.

ObscuraCam: Para no revelar la identidad de los manifestantes, es necesario pixelar rostros o vestimentas, para eso sirve ObscuraCam. Puede tomar fotografías y editarlas o editar fotos o imágenes que ya has sacado y tienes en tu memoria. Proteger la identidad de los manifestantes es proteger la protesta social.

VPN

RISE-UP VPN: Una VPN es una conexión de internet que permite mantener segura y privada tu comunicación al navegar por internet desde un servidor distante, en este caso del colectivo Riseup. Para usar la app solo hay que descargarla y activarla, haciendo que toda tu conexión a internet esté cifrada y anónima para las empresas de telecomunicaciones.

SIN INTERNET

BRIAR: En el caso de que el internet sea cortado, Briar es una opción de mensajería necesaria. No depende de ningún servidor (P2P). Puede utilizarse con Bluetooth o con Routers encendidos sin internet, permitiendo comunicarse en zonas cercanas, entre vecinos o grupos cercanos.

SILENCE: Al usar SMS, deben estar cifrados, ya que de lo contrario pueden ser leídos por las empresas de telecomunicaciones. Silence soluciona ese problema. Cuando 2 o más usuarios usan Silence para usar SMS, tienen la opción de cifrar sus mensajes y proteger su comunicación. SIGNAL también ofrece esta opción.

PRECAUCIONES

- Bloquea tu móvil con contraseña y cuida que las cámaras no vean tu clave.

- Todas las cámaras pueden potencialmente analizar los rostros con reconocimiento facial. Cubre tu rostro si es necesario.

-Ten en cuenta que mientras estés con un móvil, tu ubicación es rastreable por las antenas de telefonía, información que las empresas guardan.