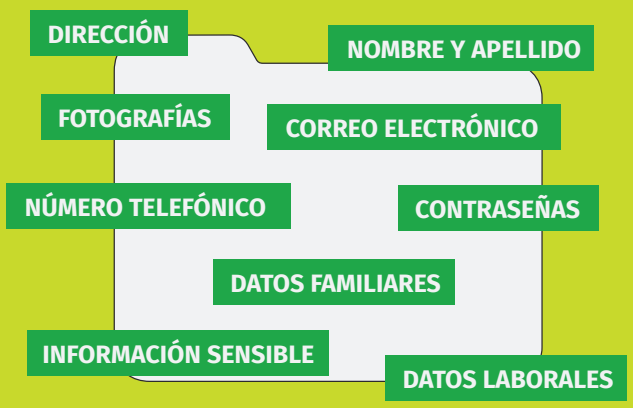
Capítulo 2

¿QUÉ ES EL DOXING Y CÓMO OPERA?

¿Qué es el doxing? Aproximaciones a algunas definiciones

El **doxing** es una práctica que consiste en la **publicación, difusión o exposición de información personal sin el consentimiento de la persona afectada**, con el objetivo de **acosar, intimidar, censurar, extorsionar o generar daños económicos, reputacionales o simbólicos**. En situaciones extremas, estas acciones pueden derivar en **violencia física directa**.

La información expuesta puede incluir



Cada tipo de dato habilita distintos niveles de agresión y riesgos, que pueden incluir hostigamiento digital, robo de identidad, violencia en línea o incluso en la vida cotidiana.

El **doxing** es una forma de **violencia digital** que busca generar miedo, daño emocional, pérdida de privacidad, autocensura y, en algunos casos, riesgos reales para la integridad física y económica de la persona afectada.

En este material adoptamos una **perspectiva de seguridad holística**, entendida como un enfoque que integra de manera inseparable las dimensiones físicas, digitales y psicosociales. Esta mirada no se limita a situaciones excepcionales ni a episodios de violencia puntual, sino que propone una forma de **habitar los entornos digitales** que pueda sostenerse en la vida cotidiana.

Desde esta perspectiva, la seguridad no se reduce al uso correcto de herramientas técnicas ni a la prevención de ataques específicos. Implica también considerar los impactos emocionales, vinculares, laborales y políticos que el uso de tecnologías —y las violencias mediadas por ellas— producen en las personas y los colectivos. Por eso, no analizamos el doxing como un fenómeno meramente tecnológico, sino como una **práctica de violencia** que atraviesa la vida cotidiana, los vínculos sociales, el trabajo, la militancia y la participación pública.

Adoptar una mirada de seguridad holística permite **salir de respuestas fragmentadas** y fortalecer prácticas de cuidado que no se activan solo ante un ataque, sino que se incorporan de manera sostenida en la forma en que nos organizamos, nos comunicamos y participamos en el espacio público digital.

¿Cómo se obtiene la información para hacer doxing?

El doxing puede realizarse a partir de múltiples vías de obtención de información que combinan técnicas tecnológicas y sociales. En la mayoría de los casos, la información que se usa para doxear **no se "hackea"**, sino que se **reconstruye** a partir de muchos datos sueltos. Pequeñas pistas que, juntas, permiten identificar, ubicar o exponer a una persona.

Las formas más comunes son:

Recolección de datos a través de redes sociales

Gran parte de los datos se obtienen de lo que las personas **publicamos sin darnos cuenta**:

- Fotos donde se ve una calle, una casa, un cartel o una patente.
- Historias que muestran rutinas (horarios, lugares, recorridos).
- Perfiles con nombre real, trabajo, ciudad, vínculos familiares.
- Comentarios viejos, publicaciones cruzadas entre plataformas.

Nada de eso parece peligroso por separado, pero **todo junto arma un mapa**.

Filtraciones de datos

A veces la información proviene de:

- Filtraciones de empresas o del Estado.
- Bases de datos vendidas o compartidas ilegalmente.
- Servicios que no protegieron bien la información.

Phishing

Mediante mensajes falsos que buscan engañar para robar accesos, datos o instalar malware. Es un tipo de engaño digital que busca que la persona:

- Ingrese su contraseña en un sitio falso.
- Descargue un archivo malicioso.
- Autorice accesos sin saberlo.

Con una sola cuenta o dispositivo vulnerado, se podría acceder a muchas más y realizar diferentes acciones que compliquen a la persona que está siendo atacada.

Sniffing

Analiza el tráfico de red para captar datos sensibles.
Puede ocurrir cuando:

- Se usan **redes Wi-Fi públicas o abiertas** (bares, aeropuertos, plazas).
- La red no está bien protegida.
- Alguien con conocimientos técnicos está "escuchando" lo que pasa por esa red.

A través del sniffing se pueden obtener:

- Contraseñas.
- Datos de inicio de sesión.
- Mensajes.
- Información sobre los sitios que se visitan.

La persona atacada **no hace nada raro ni incorrecto**: simplemente está conectada a una red insegura.

Búsqueda de información abierta

La búsqueda de información abierta consiste en **recolectar y analizar datos que ya están disponibles públicamente en internet**, sin acceder a información privada ni vulnerar sistemas. Es una práctica habitual en investigaciones periodísticas, académicas y de derechos humanos, pero también es utilizada en contextos de hostigamiento y doxing.

Es la recopilación de datos que ya están disponibles públicamente en internet. Puede incluir:

- **Registros públicos y bases de datos oficiales**.
- **Archivos y contenidos antiguos** (publicaciones, capturas, notas, perfiles ya inactivos).
- **Información técnica básica** asociada a dominios web (WHOIS, fechas de registro, proveedores).
- **Datos publicados en redes sociales** (biografías, fotos, interacciones, ubicaciones).
- **Cruce de información entre plataformas**, a partir de nombres, usuarios, correos, imágenes u otros rastros compartidos.

Ingeniería social

Consiste en **hacerse pasar por alguien confiable** para obtener información:

- Mensajes que parecen de una empresa, un banco o una red social.
- Pedidos "inocentes" de datos por mail, WhatsApp o redes.
- Formularios falsos o links que roban contraseñas.

No explotan fallas técnicas, explotan la **confianza e información** o conocimientos previos que tengan de la persona.

Ataques digitales

En algunos casos, la información utilizada para hacer doxing se obtiene a través de accesos no autorizados a cuentas o dispositivos. Esto puede ocurrir mediante:

- **Malware:** programas maliciosos que se instalan sin que la persona lo note, muchas veces al descargar archivos o hacer clic en enlaces.
- **Exploits:** aprovechamiento de fallas de seguridad en sistemas, aplicaciones o dispositivos que no están actualizados.
- **Descifrado o robo de contraseñas:** uso de contraseñas débiles, repetidas o filtradas previamente en otras plataformas.

Estas técnicas pueden utilizarse de manera aislada o combinada, aumentando la eficacia del ataque.

¿Cómo opera y se despliega el doxing?

El doxing **no ocurre de un día para otro**. Suele desplegarse como un proceso:

- Se juntan datos dispersos.
- Se los cruza y ordena.
- Se publican de forma estratégica.
- Se amplifica a través de redes, grupos o medios.

Las plataformas digitales permiten que un ataque **escale rápido**, incluso cuando empezó con una sola persona o cuenta.

Una vez difundida la información, las **agresiones asociadas al doxing** pueden adoptar diferentes niveles de intensidad, que no siempre se presentan de forma lineal o inmediata.

- Amenazas y hostigamiento en entornos digitales
- Acoso sistemático y campañas de odio coordinadas con uso de bots o cuentas creadas específicamente para hostigar.
- Realización de compras falsas a nombre de las personas a través de plataformas de comercio o mensajería que permiten ubicar las direcciones de las personas (Por ejemplo, Pedidos Ya, Facebook Market, entre otras)
- Extorsión mediante la amenaza de difusión de información
- Robo de identidad y suplantación
- Swatting: es una forma de violencia que consiste en **hacer denuncias falsas y graves ante fuerzas de seguridad** (por ejemplo, avisar de un secuestro, una bomba o una situación armada inexistente) **con el objetivo de que la policía o fuerzas especiales se movilicen hacia el domicilio de una persona**.

La IA como amplificadora del doxing

En el contexto actual, resulta clave **incorporar la inteligencia artificial en los análisis vinculados al doxing**, ya que amplifica y complejiza las amenazas existentes. La IA no crea el doxing, pero **modifica su escala, velocidad y capacidad de daño**, reduciendo las barreras de entrada para quienes atacan y aumentando la dificultad de detección y defensa.

Entre los principales riesgos emergentes se destacan:

- Deepfakes (contenidos falsos), que permiten crear mediante IA imágenes y videos falsos utilizando rostros de personas reales**.
- Audiofakes (audios falsos), mediante la imitación de voces.
- Optimización de ataques de phishing y malware, a partir del análisis automatizado de sistemas y comportamientos.

En enero de 2026, **Grok**, el sistema de inteligencia artificial desarrollado por **xAI** e integrado a la plataforma **X (ex Twitter)**, facilitó la **difusión masiva de deepfakes íntimos generados sin consentimiento**, incluyendo imágenes sexualizadas de **personas adultas y niñes y adolescentes**. Investigaciones periodísticas y denuncias públicas señalaron que la herramienta permitía editar imágenes de personas reales mediante funciones integradas, con **controles insuficientes y fácilmente eludibles**, lo que derivó en bloqueos, investigaciones regulatorias y debates legislativos en distintos países. La funcionalidad que facilita el despliegue de estas acciones sigue disponible para algunes usuaries.

¿Quiénes son los actores del doxing?

El doxing **no es una práctica aislada ni individual, sino que forma parte de estrategias organizadas de hostigamiento digital**, que se despliega de manera coordinada.

Distintos actores cumplen roles específicos dentro de estas dinámicas, desde quienes impulsan el ataque hasta quienes lo amplifican o lo ejecutan. Entre esos actores se pueden identificar:

Milicias digitales de ultraderecha: grupos organizados que operan en redes sociales con objetivos políticos claros. Funcionan de manera coordinada, se organizan alrededor de liderazgos ideológicos, influencers o figuras públicas. Estas milicias no buscan solo debatir ideas, sino neutralizar adversarios, generar miedo y expulsar voces críticas del espacio público.

Influencers políticos y nodos de amplificación: señalan públicamente a personas (por ejemplo: periodistas, militantes, activistas), difunden información personal o habilitan que otrxs lo hagan. Funcionan como disparadores de campañas de doxing, aun que no siempre publiquen ellxs mismxs directamente los datos. Estos actores cumplen un rol clave porque legitiman el ataque y multiplican su alcance.

Trolls, cuentas anónimas y bots : Cuentas anónimas o pseudónimas, muchas veces creadas específicamente para hostigar, redes de trolls que actúan en masa. En algunos casos se utiliza la automatización (bots) para amplificar ataques, amenazas o datos personales. El anonimato, combinado con la falta de procesos de las plataformas para responder a estos ataques y minimizarlos, permite escalar la violencia con bajo costo personal y alta impunidad.

Simpatizantes y participantes espontáneos: seguidores que replican ataques "por militancia", usuarios que participan del hostigamiento como forma de pertenencia identitaria. Ahi, aplica una lógica de linchamiento digital, donde el ataque se vuelve colectivo. Esto diluye responsabilidades, vuelve difícil identificar un único agresor, complejiza identificar orígenes de los ataques y habilita la idea de "viralización orgánica" como excusa para que no vuelva visible la existencia de una metodología establecida.

••••••••

Vínculos previos: el doxing también puede ser impulsado por **personas individuales**, especialmente cuando existen **vínculos previos o relaciones de cercanía**. Incluye situaciones como ex parejas o vínculos sexoafectivos; conflictos personales, laborales o militantes; disputas dentro de organizaciones o comunidades; personas conocidas que acceden a información sensible.
En estos casos, el doxing suele combinar **información obtenida por cercanía** con lógicas de exposición pública. Aunque el ataque pueda comenzar de manera individual, **rápidamente puede escalar** cuando otros actores (trolls, seguidores, cuentas anónimas) se suman y amplifican la violencia.

¿A quién puede afectar el doxing? Una mirada desde la interseccionalidad

El doxing no impacta a todas las personas de la misma manera. Si bien cualquiera puede ser víctima, **sus efectos se intensifican cuando se combinan distintas desigualdades estructurales**. Desde una **perspectiva interseccional**, entendemos que múltiples factores como géneros, clase social, origen étnico, edad, discapacidad, orientación sexual, diversidad corporal, identidad de género, religión o nacionalidad, entre otras, no actúan por separado, sino que se **entraman** y producen formas específicas de exposición y daño.

Por eso, el doxing afecta de manera particularmente grave a **activistas, mujeres, personas LGBTIQNB+, periodistas y defensorxs de derechos humanos**: no solo porque están más expuestxs en el espacio público y digital, sino porque sus cuerpos, voces y trayectorias ya son objeto de vigilancia, cuestionamiento y violencia previa. En estos casos, la difusión de datos personales no busca únicamente incomodar, sino **disciplinar**, reforzar jerarquías y marcar límites sobre quién puede hablar, existir o disputar sentido en el espacio público.

Desde esta mirada, el doxing no es un hecho aislado ni individual, sino una **práctica política** que se inscribe en relaciones de poder desiguales. Funciona como un mecanismo de control social que aprovecha las plataformas digitales para amplificar violencias ya existentes, produciendo miedo, autocensura y desgaste, no solo en la persona atacada, sino también en los colectivos y redes que la rodean.

Pensar el doxing desde la interseccionalidad implica entonces **correrse de una lectura neutral del riesgo** y reconocer que la exposición digital tiene consecuencias distintas según las posiciones que se habitan. Esto es clave para diseñar estrategias de prevención, cuidado y respuesta que no sean genéricas, sino **situadas, colectivas y conscientes de las desigualdades que atraviesan la vida digital**.

¿Qué efectos produce el doxing?

Los efectos del doxing son múltiples y acumulativos. Entre los impactos más frecuentes se identifican:

Impactos psicosociales

El doxing produce efectos profundos en las personas atacadas como miedo permanente, sensación de vigilancia, estrés, ansiedad, agotamiento emocional, autocensura, retraimiento del espacio público (físico y digital), ruptura de vínculos personales y militantes, entre otras. El objetivo no es solo dañar, sino quebrar subjetivamente a la persona.

Impactos en la vida pública y política

El doxing funciona como una tecnología de silenciamiento dado que expulsa voces críticas del debate público, especialmente en personas con exposición pública o militancia política y social (por autocensura o silenciamiento). Esto reduce la participación política e instala un clima de intimidación generalizado en base a la lógica "si hablás, te puede pasar". Esto pone en peligro la calidad democrática.

Impactos económicos y reputacionales

Pérdida de trabajos, contratos o fuentes de ingreso, desvío de recursos económicos para defensa legal, seguridad, mudanzas o reparación de dispositivos. Afectación de organizaciones, medios y colectivos (renuncias, rotación, parálisis). Daños reputacionales, que afectan la trayectoria laboral, profesional o comunitaria. El doxing actúa así como una forma de castigo económico indirecto.

Impacto estructural de normalización de la violencia

Se legitiman como "humor", "batalla cultural" o "libertad de expresión", lo que son ataques de disciplinamiento. Este proceso produce un **corrimiento del marco de lo decible y lo legítimo**, habilitando formas de crueldad como modos aceptados de intervención política y reorganizando las condiciones en las que se disputa el espacio público.