Cómo un desconocido puede saber dónde estudia tu hijo en menos de 3 minutos

Lo que no te han contado sobre la huella digital de tu familia y por qué importa ahora mismo.

Hace unos meses, en una charla sobre seguridad digital con un grupo de padres, hice una demostración que nadie olvidó. Pedí voluntarios. Una madre, con total confianza, me dijo que su hija de doce años "no tenía redes sociales" y que en casa eran "muy cuidadosos". En menos de tres minutos, y usando únicamente información pública disponible en internet, pude decirle en qué colegio estudiaba su hija, en qué barrio vivían, a qué actividad extraescolar iba los martes y cómo se llamaban dos de sus mejores amigas.

La madre se quedó pálida. No porque yo sea un hacker. Sino porque esa información la había publicado ella misma, sin saberlo, a lo largo de los últimos meses.

Esto no es un artículo de alarmismo. Es un artículo de conciencia. Porque el problema no es internet. El problema es que nadie nos ha enseñado cómo funciona realmente la exposición digital, y eso tiene consecuencias muy concretas para la seguridad de nuestros hijos.

Qué es el OSINT y por qué deberías conocer esa palabra

OSINT son las siglas en inglés de *Open Source Intelligence*: inteligencia de fuentes abiertas. En términos sencillos, es la capacidad de recopilar información sobre una persona utilizando únicamente datos que están disponibles públicamente en internet, sin acceder a nada privado, sin hackear nada, sin violar ningún sistema.

Es una disciplina legítima que usan los cuerpos de seguridad del Estado, los periodistas de investigación y los profesionales de ciberseguridad. Pero también la usan personas con intenciones muy distintas. Y lo que hace al OSINT especialmente relevante en el contexto familiar es que sus fuentes principales no son bases de datos oscuras ni la dark web: son

Instagram, Facebook, LinkedIn, Google Maps y los grupos de WhatsApp con enlace abierto.

La información que usó ese hipotético investigador para localizar a la hija de aquella madre no estaba oculta en ningún lugar. Estaba en la foto del primer día de cole que ella publicó en Instagram con el hashtag del nombre del colegio. En la mención de la actividad de teatro que hizo en una story. En la etiqueta de localización del parque donde suele pasear. En el comentario de una amiga en una foto familiar que decía "¡Qué bonita vuestra casa en el barrio de...!".

Piezas sueltas, inofensivas por separado. Devastadoras cuando alguien las conecta con intención.

La anatomía de una exposición: cómo se construye el perfil de un menor en minutos

Entender el proceso ayuda a entender el riesgo. Un analista de OSINT o cualquier persona con conocimientos básicos y tiempo sigue una metodología bastante predecible cuando construye el perfil digital de un menor.

El primer paso es siempre el entorno adulto. No empieza por el niño, porque los niños suelen tener menos presencia digital directa. Empieza por los padres. Una búsqueda simple del nombre completo de un progenitor en Google, combinada con la ciudad de residencia, suele devolver en pocos segundos un perfil de LinkedIn, una cuenta de Instagram, quizás una mención en el portal de la AMPA del colegio, una entrada en el padrón municipal de algún directorio, o una aparición en la web de la empresa donde trabaja.

A partir de ahí, el proceso se ramifica. Las fotos de Instagram de un padre o una madre son una fuente de información extraordinaria: uniformes escolares con escudos identificables, murales del colegio al fondo de una foto, camisetas de equipos deportivos locales con el nombre del club, fotos del cumpleaños que permiten estimar la edad del menor. La geolocalización de las imágenes, cuando está activada, hace el resto.

El segundo vector habitual es el entorno social del propio menor. Aunque un niño no tenga cuentas propias, aparece en las de sus amigos. Los adolescentes etiquetan, mencionan y

comparten con una naturalidad que no perciben como riesgo porque, para ellos, no lo es en su contexto social. Lo que cambia es cuando esa información sale de ese contexto.

El tercer vector, y el más infraestructural, es la huella institucional. El boletín digital del colegio, el acta de la asamblea de la AMPA publicada en la web del centro, la lista de participantes de un campeonato deportivo municipal, la foto de grupo de la actuación de fin de curso. Información publicada con buenas intenciones, accesible para todo el mundo.

La combinación de estos tres vectores, en manos de alguien con criterio y herramientas básicas, puede producir en minutos un perfil que incluye nombre completo, edad aproximada, centro escolar, domicilio o barrio, actividades extracurriculares, horarios habituales y red social más cercana.

Por qué esto importa más allá del "miedo a los pedófilos"

Cuando se habla de seguridad digital de menores, el debate público tiende a colapsar en un único miedo: el grooming, la captación de menores con fines sexuales. Es un riesgo real y grave, pero reducir la conversación a ese único escenario tiene un efecto secundario peligroso: hace que los padres que piensan "eso no le va a pasar a mi hijo" desactiven toda su vigilancia digital.

La exposición OSINT de un menor tiene consecuencias que van mucho más allá. El secuestro con fines de extorsión familiar, que ha crecido en los últimos años especialmente en contextos de alta visibilidad económica, se facilita enormemente cuando los patrones de movimiento de un niño son predecibles y públicos. El acoso escolar digital, que con frecuencia migra del patio al teléfono, se intensifica cuando los agresores tienen acceso a información del entorno del menor fuera del colegio. La suplantación de identidad de menores para crear perfiles falsos en redes sociales es un problema creciente y muy poco visibilizado.

Pero hay algo más sutil, y en cierto modo más preocupante: la normalización de la vigilancia hacia los propios menores. Un niño cuya vida se documenta y publica de forma sistemática desde que nace crece con una noción distorsionada de la privacidad. No la percibe como un derecho, sino como una ausencia de contenido interesante. Esa percepción les hace más vulnerables, no menos, cuando se convierten en adolescentes y empiezan a gestionar su propia presencia digital.

El error que cometemos sin darnos cuenta: el "sharenting"

Existe un término que cada vez aparece más en los informes de protección de menores: *sharenting*. Es la combinación de *sharing* (compartir) y *parenting* (crianza), y describe la práctica de compartir en redes sociales contenido relacionado con los hijos de forma habitual y continuada.

No es un fenómeno marginal. Según datos recientes de organizaciones europeas de protección de la infancia, un niño medio acumula más de mil fotografías publicadas por sus padres en internet antes de cumplir los cinco años. Antes de que pueda consentir. Antes de que pueda comprender qué significa tener esa presencia digital.

El *sharenting* no es un acto irresponsable en sí mismo. Es un acto humano, afectivo, completamente comprensible. El problema es que se realiza sin conciencia de sus implicaciones a medio y largo plazo, en un entorno donde esa información no desaparece, donde los metadatos de una imagen pueden revelar la localización exacta donde fue tomada, y donde los algoritmos de reconocimiento facial han alcanzado una precisión que hubiera parecido ciencia ficción hace diez años.

Un perfil de Instagram privado no es una solución completa. Cuando etiquetas a una amiga en una foto de tu hijo, esa imagen entra en la red de seguidores de esa amiga. Cuando alguien hace una captura de pantalla, pierde toda restricción de privacidad. La ilusión de control es, con frecuencia, solo eso: una ilusión.

Lo que las plataformas no te dicen sobre los datos de tus hijos

Las grandes plataformas de redes sociales prohíben formalmente que los menores de 13 años tengan cuentas propias. Es una política que cumple con la regulación, pero que en la práctica no impide que los menores aparezcan masivamente en sus bases de datos, a través de las cuentas de sus padres, sus familiares y sus amigos.

Cada foto que publicas de tu hijo en una plataforma es procesada por sistemas de reconocimiento facial e inteligencia artificial que, en muchos casos, identifican y etiquetan a las personas de la imagen aunque no las menciones explícitamente. Esos datos forman parte de los modelos de entrenamiento de la plataforma. Se usan para optimizar publicidad, para mejorar el reconocimiento de imágenes y para construir perfiles de usuario más precisos.

Tu hijo, que nunca ha aceptado ningún término y condición, tiene ya una huella digital en los sistemas de las mayores empresas tecnológicas del mundo. Eso no es una acusación: es una descripción del ecosistema en el que vivimos. Y el primer paso para gestionarlo de forma responsable es entenderlo.

Tres preguntas para hacer una auditoría rápida de tu huella familiar

No necesitas ser experto en tecnología para reducir significativamente la exposición digital de tu familia. El primer ejercicio útil es hacerte estas tres preguntas con honestidad:

¿Qué puede saber alguien de mi hijo mirando mis últimos 30 posts? Abre tu perfil como si fueras un desconocido. Anota qué colegio, qué barrio, qué rutinas y qué amigos se deducen de esas imágenes. El resultado suele sorprender.

¿Qué información sobre mi hijo está en internet sin que yo la haya publicado? Busca el nombre de tu hijo en Google. Busca su nombre junto al del colegio. Busca el colegio en Google Maps y mira las fotos que hay etiquetadas. Revisa si el centro escolar publica fotos de actividades en las que aparezca. Este ejercicio revela fuentes de exposición que habitualmente se pasan por alto.

¿Sabe mi hijo qué significa publicar algo en internet? No me refiero a si conoce las normas de su red social favorita. Me refiero a si comprende que lo que se publica no desaparece, que puede ser visto por personas fuera de su entorno y que cada imagen contiene información que no siempre es visible a simple vista. Esta conversación es más importante que cualquier configuración de privacidad.

Reflexión estratégica: la privacidad no es paranoia, es higiene digital

Vivimos en una cultura que ha normalizado la exposición como forma de conexión. Compartir momentos, celebrar hitos, documentar la vida cotidiana son impulsos completamente humanos y legítimos. El objetivo de este artículo no es que dejes de publicar fotos de tus hijos ni que conviertas tu vida digital en un búnker.

El objetivo es que lo hagas con criterio. Con conciencia de lo que compartes, con quién lo compartes y qué información adicional —no siempre visible— contiene lo que publicas.

La privacidad digital no es un tema técnico. Es una forma de pensar. Y como toda forma de pensar, se aprende, se practica y se transmite. La mejor protección que puedes dar a tus hijos en el entorno digital no es un control parental ni un perfil privado: es enseñarles a pensar críticamente sobre lo que comparten y por qué.

Esa cultura, cuando se instala en una familia, es más robusta que cualquier herramienta tecnológica. Y se construye con conversaciones, no con restricciones.

Tu próximo paso (y son solo 15 minutos)

Hoy mismo puedes hacer tres cosas concretas. Primero, activa la opción de desactivar la geolocalización en las fotos de tu teléfono antes de publicarlas: en iOS y Android está en la configuración de la cámara o en los permisos de ubicación de cada aplicación. Segundo, busca tu nombre completo en Google junto a la ciudad donde vives y observa qué información tuya y de tu familia aparece públicamente. Tercero, habla con tu hijo esta semana sobre qué significa que una foto "es para siempre" en internet, con un lenguaje adaptado a su edad.

No necesitas más tiempo. Necesitas hacerlo.

Si este artículo te ha hecho pensar, compártelo con otro padre o madre. Una familia informada es una familia más difícil de exponer. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero