

OSINT en investigación privada: metodología, herramientas y límites legales en España

Introducción: qué es OSINT y por qué es relevante para el detective privado

OSINT es el acrónimo de Open Source Intelligence —inteligencia en fuentes abiertas—. Designa el conjunto de métodos, técnicas y herramientas orientados a la recopilación, procesamiento y análisis de información procedente de fuentes accesibles públicamente, sin necesidad de acceso no autorizado a sistemas o datos privados.

El concepto tiene origen en el ámbito de la inteligencia militar y gubernamental, pero su aplicación en investigación privada ha crecido de forma exponencial en la última década. Para el detective privado español, el OSINT no es un sustituto de la vigilancia clásica: es una fase previa de inteligencia que permite planificar operaciones con mayor precisión, reducir tiempos de investigación y orientar los recursos hacia las líneas de trabajo más productivas.

El ciclo de inteligencia aplicado a la investigación privada

1. Dirección: definir qué se busca y para qué

Antes de iniciar cualquier búsqueda, el investigador debe tener claridad sobre el objetivo de la investigación, los requisitos de la prueba y los límites del encargo. Si la información va a usarse en un procedimiento judicial, debe poder acreditarse su origen, fecha de obtención y método de captura. El mandato del cliente define el objeto: la curiosidad profesional no es base legitimadora del tratamiento de datos.

2. Recopilación: fuentes y herramientas por capas

La recopilación en OSINT se organiza por capas de profundidad:

- Capa 1 — Web superficial indexada: motores de búsqueda con operadores avanzados. Los operadores booleanos y los operadores específicos de Google (site:, filetype:, inurl:, intitle:, cadena exacta) permiten refinar búsquedas de forma significativa. Un investigador que no domina los operadores avanzados trabaja con el 10% de la capacidad de las herramientas que ya tiene disponibles.
- Capa 2 — Registros públicos y bases de datos oficiales: Registro Mercantil Central, Registro de la Propiedad, BORME, BOE y boletines autonómicos, plataforma de contratación del sector público y Catastro. Cada uno con su propio procedimiento de acceso y su alcance específico.
- Capa 3 — Redes sociales y presencia digital: LinkedIn, Facebook, Instagram, X y TikTok. El análisis requiere metodología: buscar únicamente bajo el nombre real, ignorar perfiles con privacidad alta y no documentar correctamente son los errores más frecuentes.
- Capa 4 — Metadatos y huella digital: imágenes publicadas pueden contener metadatos EXIF con fecha, hora y coordenadas GPS. Documentos PDF y Office

pueden contener metadatos de autor y fecha de creación. Técnica de nivel avanzado con alto valor en investigaciones corporativas.

- Capa 5 — Herramientas especializadas OSINT: Maltego (análisis de relaciones entre entidades), Shodan (dispositivos conectados), theHarvester (correos y subdominios), Wayback Machine (versiones históricas de webs) y Google Dorks (combinaciones de operadores avanzados).

3. Procesamiento y análisis

La información bruta recopilada no es inteligencia. El procesamiento consiste en verificar, contrastar y estructurar los datos obtenidos para extraer conclusiones fundamentadas.

Verificación cruzada: ningún dato procedente de una única fuente debe darse por válido sin contraste. Una dirección encontrada en LinkedIn debe verificarse contra el Registro Mercantil, el Catastro o la observación directa antes de incorporarse a un informe.

Construcción de cronología: en muchas investigaciones, el valor de la información no está en cada dato aislado, sino en la secuencia temporal que revelan en conjunto. La reconstrucción de una cronología de actividad puede ser más reveladora que cualquier dato individual.

Análisis de relaciones: identificar vínculos entre personas, sociedades, domicilios o activos es una de las aplicaciones más potentes del OSINT en investigación corporativa. Un administrador que aparece en cinco sociedades, tres en proceso concursal, es un dato que no emerge de una búsqueda simple pero sí de un análisis sistemático de relaciones.

4. Difusión: el informe OSINT

Los resultados del análisis OSINT deben plasmarse en un informe estructurado que especifique, para cada dato: fuente exacta de obtención (URL, nombre del registro, fecha de publicación), fecha y hora de consulta por parte del investigador, método de captura (captura de pantalla, descarga de documento, nota registral) y estado de verificación. Sin esta documentación, la información OSINT tiene valor orientativo pero no puede incorporarse como prueba a un informe pericial.

Marco legal: qué está permitido y qué no en OSINT para investigación privada

Lo que está permitido

Consultar información públicamente disponible no requiere autorización específica. Si una persona ha publicado su domicilio en una red social con perfil público, esa información es accesible y su consulta es lícita. Acceder a registros públicos mediante los canales habilitados —consulta online, solicitud de nota simple, consulta del BORME— es completamente lícito. El análisis de metadatos de documentos o imágenes públicamente accesibles también lo es.

Lo que no está permitido

- Acceso no autorizado a sistemas informáticos: cualquier técnica que implique acceso a cuentas, sistemas o redes sin autorización del titular constituye un delito tipificado en el artículo 197 bis del Código Penal, independientemente de la finalidad de la investigación.
- Suplantación de identidad: crear perfiles falsos para acceder a información privada de un sujeto o para obtener información de sus contactos es ilícito y puede constituir delito. Además, en la mayoría de las investigaciones legítimas es innecesaria.

- Tratamiento de datos sin base legitimadora: el RGPD exige base jurídica válida. En investigación privada, es el interés legítimo del cliente (art. 6.1.f RGPD), pero tiene límites: no puede prevalecer sobre los derechos fundamentales del investigado cuando la intromisión es desproporcionada.
- Uso de datos filtrados o robados: información procedente de filtraciones de datos no puede usarse en investigación privada legítima, independientemente de que esté técnicamente accesible. Su uso expone al investigador a responsabilidad penal y a la nulidad de la prueba.

La zona gris: perfiles semiprivados y información de terceros

La situación más frecuente en la práctica es el perfil de red social con configuración de privacidad intermedia. La doctrina jurídica española no ha establecido una línea clara en todos los supuestos, pero el criterio general es que la información accesible sin necesidad de solicitar acceso específico puede considerarse públicamente disponible, mientras que la que requiere aceptación de una solicitud de amistad está protegida por la expectativa razonable de privacidad del titular.

OSINT en investigación corporativa: aplicaciones específicas

Verificación de contrapartes empresariales

Antes de formalizar un contrato significativo, la verificación mediante OSINT puede revelar historial de procedimientos concursales o insolvencias, existencia de sentencias o procedimientos judiciales en curso, discrepancias entre la presentación comercial y la realidad registral (capital social real, administradores efectivos), y vinculación con otras sociedades problemáticas a través de administradores comunes.

Investigación de competencia desleal

Cuando una empresa sospecha que un empleado ha creado una sociedad competidora utilizando información confidencial, el OSINT puede determinar la fecha de constitución de la nueva sociedad (contrastable con BORME), la identidad de socios y administradores, el domicilio social y sus posibles vinculaciones con clientes de la empresa afectada, y la oferta comercial de la nueva entidad.

Due diligence precontractual

La due diligence es el proceso de verificación de una contraparte antes de cerrar una operación. El OSINT es la primera fase de ese proceso: permite descartar contrapartes evidentemente problemáticas con un coste mínimo, antes de invertir recursos en investigación más profunda.

Errores críticos en OSINT: los más frecuentes en estudiantes y profesionales

Error 1: Confundir accesibilidad técnica con licitud

Que una información sea técnicamente accesible no significa que su obtención sea lícita. Las herramientas OSINT permiten acceder a información que, aunque disponible, puede haber sido publicada sin consentimiento del titular o puede estar sujeta a restricciones de uso. El investigador es responsable de verificar la licitud del método de obtención, no solo del resultado.

Error 2: No documentar el proceso de obtención

La información obtenida mediante OSINT que no está documentada en cuanto a su fuente, fecha y método de captura no puede usarse como prueba. Muchos investigadores recopilan información sin documentarla sistemáticamente, lo que la convierte en inteligencia operativa pero no en prueba.

Error 3: Dar por válida información sin verificación cruzada

Internet contiene información errónea, desactualizada y deliberadamente falsa. Un domicilio en una web de contactos puede ser incorrecto. Un perfil de LinkedIn puede contener datos falsos. La verificación cruzada no es opcional: es un requisito metodológico.

Error 4: Exceder el objeto del encargo

El investigador puede encontrar información relevante que va más allá del encargo del cliente. Incorporar esa información al informe sin autorización expresa puede generar problemas legales y éticos. El mandato del cliente define el objeto de la investigación.

Error 5: Subestimar la velocidad de cambio de la información online

La información online cambia. Un perfil puede eliminarse, una página puede modificarse. La captura estática —captura de pantalla con fecha y hora verificable— es el único método que preserva la información tal como estaba en el momento de la consulta.

Conclusión: OSINT como disciplina, no como atajo

El OSINT es una de las competencias más demandadas en el sector de la investigación privada y la seguridad corporativa. Su dominio requiere conocimiento técnico de herramientas y fuentes, comprensión del marco legal aplicable y rigor metodológico en la documentación del proceso.

Para el estudiante de investigación privada, la tentación de usar el OSINT como atajo — buscar rápidamente en redes sociales sin metodología ni documentación— es el error más común y el que más limita el desarrollo profesional posterior. El OSINT bien practicado es lento, sistemático y documentado. Sus resultados, cuando se obtienen con rigor, son de un valor extraordinario para cualquier investigación.

Contenido elaborado con fines formativos. La aplicación de técnicas OSINT en investigación privada debe realizarse siempre dentro del marco de la Ley 5/2014 de Seguridad Privada, el RGPD y la Ley Orgánica 3/2018 de Protección de Datos Personales. Ineva Detectives · <https://www.inevadetectives.eu>
