Indagini OSINT e legalità: cosa può fare davvero un’azienda di cybersecurity

Maria Cattini | 30/05/2026 | Sicurezza digitale

L’OSINT è spesso raccontato come una specie di superpotere: trovi un nome, incroci un profilo, risali a un’email, scopri collegamenti, ricostruisci una rete.

In parte è vero.
Ma manca sempre un pezzo della frase.

Il fatto che un’informazione sia pubblica non significa che possa essere raccolta, archiviata, profilata e usata in qualsiasi modo.

Per un’azienda di cybersecurity, questo punto è decisivo. L’OSINT può essere uno strumento legittimo di prevenzione, verifica e protezione. Ma può anche scivolare facilmente in zone rischiose: sorveglianza impropria, stalking digitale, profilazione eccessiva, raccolta di dati non necessari.

La differenza non la fa solo lo strumento.
La fa il metodo.

OSINT non significa “tutto è permesso”

OSINT vuol dire Open Source Intelligence: raccolta e analisi di informazioni accessibili da fonti aperte.

Fonti aperte possono essere:

• siti web pubblici;
• registri aziendali;
• motori di ricerca;
• social network;
• archivi web;
• repository pubblici;
• database di vulnerabilità;
• fonti giornalistiche;
• forum e piattaforme pubbliche;
• documenti istituzionali.

Fin qui tutto chiaro.

Il problema nasce quando “pubblico” viene confuso con “liberamente utilizzabile per qualunque finalità”.

Un post LinkedIn è pubblico? Sì.
Un profilo Instagram aperto è visibile? Sì.
Un vecchio documento indicizzato da Google può essere accessibile? Sì.

Ma se un’azienda raccoglie quei dati, li collega, li conserva, li arricchisce e li usa per prendere decisioni su una persona, sta facendo trattamento di dati personali. E quel trattamento deve avere una base giuridica, una finalità chiara e limiti precisi.

In Europa, questo significa fare i conti con il GDPR.

INDAGINI OSINT E LEGALITÀ

Dati pubblici non significa uso libero

COSA PUÒ FARE

- Monitorare esposizione pubblica
- Verificare domini, IP, repository
- Analizzare phishing e frodi
- Supportare threat intelligence
- Fare due diligence digitale

DOVE INIZIANO I RISCHI

- Raccogliere dati non necessari
- Creare dossier personali sproporzionati
- Monitorare profili privati o semi-privati
- Usare account falsi
- Conservare dati senza limiti

DOMANDE PRIMA DI INIZIARE

- Qual è la finalità?
- Chi ha autorizzato l'indagine?
- Quali dati servono davvero?
- Le fonti sono lecite?
- Quanto tempo conservo i dati?

REGOLA PRATICA

> Se non sai spiegare perché ti serve quel dato, probabilmente **non dovresti raccoglierlo.**

OSINT = METODO, PROPORZIONE, RESPONSABILITÀ

Cosa può fare una società di cybersecurity

Un’azienda di cybersecurity può usare l’OSINT in molti modi leciti e utili.

Può, ad esempio, monitorare l’esposizione pubblica di un’organizzazione: domini, sottodomini, indirizzi IP, servizi esposti, repository pubblici, credenziali finite in data breach, documenti indicizzati per errore, menzioni del brand in forum sospetti.

Può analizzare una campagna di phishing, raccogliendo indicatori pubblici come domini, URL, email mittenti, infrastrutture usate dagli attaccanti, pagine clone e wallet crypto.

Può fare threat intelligence, cioè osservare segnali pubblici collegati a vulnerabilità, gruppi criminali, campagne malware, leak o nuove tecniche di attacco.

Può supportare un’azienda nella gestione della reputazione digitale, ad esempio verificando se dati sensibili, documenti interni o informazioni sui dipendenti siano esposti online.

Può anche aiutare in attività di due diligence: controllare registri pubblici, asset digitali, presenza online di una società, domini collegati, eventuali segnali di frode.

In tutti questi casi, il punto è la proporzione.

La domanda non è solo: “Posso trovare questa informazione?”
La domanda corretta è: “Mi serve davvero per una finalità legittima e documentabile?”

Dove iniziano i rischi

Il confine diventa fragile quando l’indagine si sposta da un obiettivo di sicurezza a un controllo invasivo sulla persona.

Esempi rischiosi:

• raccogliere dati personali non necessari;
• monitorare profili social privati o semi-privati;
• usare account falsi per aggirare restrizioni;
• salvare screenshot di vita privata senza motivo;
• creare dossier personali sproporzionati;
• tracciare abitudini, relazioni, opinioni politiche o sanitarie;
• usare strumenti automatici per profilare persone su larga scala;
• combinare dati pubblici e data broker senza trasparenza;
• accedere a contenuti attraverso credenziali ottenute in modo improprio;
• violare termini di servizio o barriere tecniche.

Qui non siamo più nella semplice ricerca OSINT.

Siamo in una zona dove possono entrare in gioco privacy, diritto del lavoro, responsabilità civile, reati informatici, stalking, diffamazione o trattamento illecito di dati.

Il fatto che un tool permetta di farlo non significa che sia legittimo farlo.

Dati pubblici, dati personali, dati sensibili

Un altro errore comune è pensare che i dati pubblici non siano dati personali.

Non è così.

Un nome, un indirizzo email, un numero di telefono, una foto, un username, un indirizzo IP, una

posizione geografica, una storia lavorativa o un profilo social possono essere dati personali se permettono di identificare una persona.

Alcuni dati sono ancora più delicati: opinioni politiche, convinzioni religiose, dati sanitari, orientamento sessuale, appartenenza sindacale, dati biometrici.

Anche se una persona ha pubblicato qualcosa online, non significa che un'azienda possa usarlo liberamente per qualsiasi scopo.

Il GDPR richiede principi precisi: liceità, correttezza, trasparenza, minimizzazione, limitazione della finalità, esattezza, limitazione della conservazione e sicurezza.

Tradotto in pratica: raccogli il minimo necessario, spiega perché lo fai, conserva solo per il tempo utile, proteggi i dati e non riutilizzarli per scopi incompatibili.

OSINT lecito o stalking digitale?

La differenza spesso sta in tre elementi: finalità, proporzione e autorizzazione.

Un'azienda che controlla se le proprie credenziali sono finite in un leak sta facendo sicurezza.

Un'azienda che controlla ogni giorno i profili personali dei dipendenti senza una ragione specifica entra in una zona molto problematica.

Un consulente che analizza un dominio aziendale su incarico del cliente sta facendo un'attività autorizzata.

Una persona che usa strumenti OSINT per seguire, intimidire o esporre un ex partner sta facendo stalking digitale, non investigazione.

Un analyst che verifica un profilo sospetto collegato a una truffa documenta un rischio.

Un soggetto che crea un dossier sulla vita privata di qualcuno "per curiosità" sta oltrepassando il limite.

L'OSINT non è definito solo dalle fonti usate.
È definito anche dall'uso che ne facciamo.

Una checklist pratica per restare nel perimetro

Prima di avviare un'indagine OSINT, un'azienda dovrebbe rispondere a queste domande.

1. Qual è la finalità?
Sicurezza informatica, prevenzione frodi, due diligence, incident response, tutela del brand. Deve essere chiara prima della raccolta.

2. Chi ha autorizzato l'attività?
C'è un contratto, un incarico, una policy interna, una base giuridica?

3. Quali dati servono davvero?
Se bastano dominio, IP e repository pubblici, non serve raccogliere foto personali o dati familiari.

4. La raccolta è proporzionata?
Un rischio basso non giustifica un dossier invasivo.

5. Le fonti sono legittime?
Fonti pubbliche sì. Accessi abusivi, credenziali leakate, gruppi chiusi aggirati o scraping aggressivo sono un altro discorso.

6. Quanto tempo saranno conservati i dati?
“Per sempre” non è una risposta accettabile.

7. Chi può accedere al report?
Un report OSINT può contenere dati sensibili. Va limitato a chi ne ha reale necessità.

8. Il linguaggio del report è prudente?
Distinguere fatti, ipotesi e inferenze è fondamentale. Scrivere “è collegato a” non è lo stesso che scrivere “potrebbe essere collegato a”.

Il ruolo dell’etica

La legalità è il minimo.
L’etica è il filtro che evita di fare danni anche quando qualcosa sembra tecnicamente possibile.

Un buon professionista OSINT non si chiede solo come trovare un’informazione. Si chiede anche se sia giusto raccoglierla, se sia necessario conservarla, se possa esporre qualcuno a un rischio inutile.

Questo vale ancora di più quando l’indagine riguarda persone vulnerabili, dipendenti, minori, attivisti, vittime di frodi o soggetti privati non coinvolti direttamente nel rischio.

La cybersecurity non deve trasformarsi in sorveglianza privata.

Conclusione

L’OSINT è uno strumento potente per la sicurezza digitale. Aiuta a prevenire attacchi, verificare minacce, smascherare frodi e capire cosa è esposto online.

Ma non è una licenza per investigare chiunque, comunque, per qualsiasi motivo.

Per un’azienda di cybersecurity, la regola dovrebbe essere semplice:

raccogliere solo ciò che serve, da fonti lecite, per una finalità chiara, con un metodo documentabile.

Il resto non è intelligence.

È rischio.
L’OSINT è spesso raccontato come una specie di superpotere: trovi un nome, incroci un profilo, risali a un’email, scopri collegamenti, ricostruisci una rete.

In parte è vero.
Ma manca sempre un pezzo della frase.

Il fatto che un’informazione sia pubblica non significa che possa essere raccolta, archiviata, profilata e usata in qualsiasi modo.

Per un’azienda di cybersecurity, questo punto è decisivo. L’OSINT può essere uno strumento legittimo di prevenzione, verifica e protezione. Ma può anche scivolare facilmente in zone rischiose: sorveglianza impropria, stalking digitale, profilazione eccessiva, raccolta di dati non necessari.

La differenza non la fa solo lo strumento.
La fa il metodo.

OSINT non significa “tutto è permesso”

OSINT vuol dire Open Source Intelligence: raccolta e analisi di informazioni accessibili da fonti aperte.

Fonti aperte possono essere:

• siti web pubblici;
• registri aziendali;
• motori di ricerca;
• social network;
• archivi web;
• repository pubblici;
• database di vulnerabilità;
• fonti giornalistiche;
• forum e piattaforme pubbliche;
• documenti istituzionali.

Fin qui tutto chiaro.

Il problema nasce quando “pubblico” viene confuso con “liberamente utilizzabile per qualunque finalità”.

Un post LinkedIn è pubblico? Sì.
Un profilo Instagram aperto è visibile? Sì.
Un vecchio documento indicizzato da Google può essere accessibile? Sì.

Ma se un’azienda raccoglie quei dati, li collega, li conserva, li arricchisce e li usa per prendere decisioni su una persona, sta facendo trattamento di dati personali. E quel trattamento deve avere una base giuridica, una finalità chiara e limiti precisi.

In Europa, questo significa fare i conti con il GDPR.

INDAGINI OSINT E LEGALITÀ

Dati pubblici non significa uso libero

COSA PUÒ FARE

- Monitorare esposizione pubblica
- Verificare domini, IP, repository
- Analizzare phishing e frodi
- Supportare threat intelligence
- Fare due diligence digitale

DOVE INIZIANO I RISCHI

- Raccogliere dati non necessari
- Creare dossier personali sproporzionati
- Monitorare profili privati o semi-privati
- Usare account falsi
- Conservare dati senza limiti

DOMANDE PRIMA DI INIZIARE

- Qual è la finalità?
- Chi ha autorizzato l'indagine?
- Quali dati servono davvero?
- Le fonti sono lecite?
- Quanto tempo conservo i dati?

REGOLA PRATICA

> Se non sai spiegare perché ti serve quel dato, probabilmente **non dovresti raccoglierlo.**

OSINT = METODO, PROPORZIONE, RESPONSABILITÀ

Cosa può fare una società di cybersecurity

Un’azienda di cybersecurity può usare l’OSINT in molti modi leciti e utili.

Può, ad esempio, monitorare l’esposizione pubblica di un’organizzazione: domini, sottodomini, indirizzi IP, servizi esposti, repository pubblici, credenziali finite in data breach, documenti indicizzati per errore, menzioni del brand in forum sospetti.

Può analizzare una campagna di phishing, raccogliendo indicatori pubblici come domini, URL, email mittenti, infrastrutture usate dagli attaccanti, pagine clone e wallet crypto.

Può fare threat intelligence, cioè osservare segnali pubblici collegati a vulnerabilità, gruppi criminali, campagne malware, leak o nuove tecniche di attacco.

Può supportare un’azienda nella gestione della reputazione digitale, ad esempio verificando se dati sensibili, documenti interni o informazioni sui dipendenti siano esposti online.

Può anche aiutare in attività di due diligence: controllare registri pubblici, asset digitali, presenza online di una società, domini collegati, eventuali segnali di frode.

In tutti questi casi, il punto è la proporzione.

La domanda non è solo: “Posso trovare questa informazione?”
La domanda corretta è: “Mi serve davvero per una finalità legittima e documentabile?”

Dove iniziano i rischi

Il confine diventa fragile quando l’indagine si sposta da un obiettivo di sicurezza a un controllo invasivo sulla persona.

Esempi rischiosi:

• raccogliere dati personali non necessari;
• monitorare profili social privati o semi-privati;
• usare account falsi per aggirare restrizioni;
• salvare screenshot di vita privata senza motivo;
• creare dossier personali sproporzionati;
• tracciare abitudini, relazioni, opinioni politiche o sanitarie;
• usare strumenti automatici per profilare persone su larga scala;
• combinare dati pubblici e data broker senza trasparenza;
• accedere a contenuti attraverso credenziali ottenute in modo improprio;
• violare termini di servizio o barriere tecniche.

Qui non siamo più nella semplice ricerca OSINT.

Siamo in una zona dove possono entrare in gioco privacy, diritto del lavoro, responsabilità civile, reati informatici, stalking, diffamazione o trattamento illecito di dati.

Il fatto che un tool permetta di farlo non significa che sia legittimo farlo.

Dati pubblici, dati personali, dati sensibili

Un altro errore comune è pensare che i dati pubblici non siano dati personali.

Non è così.

Un nome, un indirizzo email, un numero di telefono, una foto, un username, un indirizzo IP, una

posizione geografica, una storia lavorativa o un profilo social possono essere dati personali se permettono di identificare una persona.

Alcuni dati sono ancora più delicati: opinioni politiche, convinzioni religiose, dati sanitari, orientamento sessuale, appartenenza sindacale, dati biometrici.

Anche se una persona ha pubblicato qualcosa online, non significa che un'azienda possa usarlo liberamente per qualsiasi scopo.

Il GDPR richiede principi precisi: liceità, correttezza, trasparenza, minimizzazione, limitazione della finalità, esattezza, limitazione della conservazione e sicurezza.

Tradotto in pratica: raccogli il minimo necessario, spiega perché lo fai, conserva solo per il tempo utile, proteggi i dati e non riutilizzarli per scopi incompatibili.

OSINT lecito o stalking digitale?

La differenza spesso sta in tre elementi: finalità, proporzione e autorizzazione.

Un'azienda che controlla se le proprie credenziali sono finite in un leak sta facendo sicurezza.

Un'azienda che controlla ogni giorno i profili personali dei dipendenti senza una ragione specifica entra in una zona molto problematica.

Un consulente che analizza un dominio aziendale su incarico del cliente sta facendo un'attività autorizzata.

Una persona che usa strumenti OSINT per seguire, intimidire o esporre un ex partner sta facendo stalking digitale, non investigazione.

Un analyst che verifica un profilo sospetto collegato a una truffa documenta un rischio.

Un soggetto che crea un dossier sulla vita privata di qualcuno "per curiosità" sta oltrepassando il limite.

L'OSINT non è definito solo dalle fonti usate.
È definito anche dall'uso che ne facciamo.

Una checklist pratica per restare nel perimetro

Prima di avviare un'indagine OSINT, un'azienda dovrebbe rispondere a queste domande.

1. Qual è la finalità?
Sicurezza informatica, prevenzione frodi, due diligence, incident response, tutela del brand. Deve essere chiara prima della raccolta.

2. Chi ha autorizzato l'attività?
C'è un contratto, un incarico, una policy interna, una base giuridica?

3. Quali dati servono davvero?
Se bastano dominio, IP e repository pubblici, non serve raccogliere foto personali o dati familiari.

4. La raccolta è proporzionata?
Un rischio basso non giustifica un dossier invasivo.

5. Le fonti sono legittime?
Fonti pubbliche sì. Accessi abusivi, credenziali leakate, gruppi chiusi aggirati o scraping aggressivo sono un altro discorso.

6. Quanto tempo saranno conservati i dati?
“Per sempre” non è una risposta accettabile.

7. Chi può accedere al report?
Un report OSINT può contenere dati sensibili. Va limitato a chi ne ha reale necessità.

8. Il linguaggio del report è prudente?
Distinguere fatti, ipotesi e inferenze è fondamentale. Scrivere “è collegato a” non è lo stesso che scrivere “potrebbe essere collegato a”.

Il ruolo dell’etica

La legalità è il minimo.
L’etica è il filtro che evita di fare danni anche quando qualcosa sembra tecnicamente possibile.

Un buon professionista OSINT non si chiede solo come trovare un’informazione. Si chiede anche se sia giusto raccoglierla, se sia necessario conservarla, se possa esporre qualcuno a un rischio inutile.

Questo vale ancora di più quando l’indagine riguarda persone vulnerabili, dipendenti, minori, attivisti, vittime di frodi o soggetti privati non coinvolti direttamente nel rischio.

La cybersecurity non deve trasformarsi in sorveglianza privata.

Conclusione

L’OSINT è uno strumento potente per la sicurezza digitale. Aiuta a prevenire attacchi, verificare minacce, smascherare frodi e capire cosa è esposto online.

Ma non è una licenza per investigare chiunque, comunque, per qualsiasi motivo.

Per un’azienda di cybersecurity, la regola dovrebbe essere semplice:

raccogliere solo ciò che serve, da fonti lecite, per una finalità chiara, con un metodo documentabile.

Il resto non è intelligence.

È rischio.