OPEN SOURCE INTELLIGENCE (OSINT)

Strumenti, limiti e best practice in ambito aziendale e nelle investigazioni private

L'Open Source Intelligence (OSINT) – ossia la raccolta di informazioni da fonti aperte e pubblicamente accessibili – è uno strumento sempre più utilizzato in ambito aziendale e investigativo per **raccogliere e analizzare informazioni da fonti pubblicamente accessibili**. Non a caso, le stime di crescita del settore, a livello globale prevedono un **mercato da circa 63 miliardi di dollari entro il 2031**. Questo dato non è casuale: riflette la crescente consapevolezza delle potenzialità dell'OSINT nel rispondere alle sfide contemporanee. Tuttavia, il suo utilizzo deve rispettare precisi **vincoli normativi**, sia per garantire la **compliance** aziendale sia per tutelare la **privacy** dei soggetti coinvolti.

L'obiettivo di questo elaborato è quindi contribuire a fare chiarezza circa il corretto utilizzo dell'OSINT, al fine di promuovere il concetto di OSINT quale **moltiplicatore di valore**, ma sempre in una prospettiva etica e legale.

Mirko Lapi è Consulente e Formatore specializzato in Open Source Intelligence (OSINT), sicurezza delle informazioni e sviluppo del pensiero critico applicato ai processi decisionali. Ha prestato servizio nelle Forze Armate italiane per 27 anni, di cui 16 anni all'interno del II Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa, dove ha lavorato come analista presso il Centro Intelligence Interforze dello Stato Maggiore della Difesa e come docente di Intelligence presso il Centro Interforze di Formazione Intelligence (CIFIGE). È Professore a contratto di Open Source Intelligence (OSINT) presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Foggia. Inoltre, ricopre il ruolo di Professore a contratto di Cyber Security per il Corso di Laurea Magistrale in Ingegneria dei Sistemi Intelligenti presso la Facoltà di Ingegneria, Università Campus Bio-Medico di Roma.

OPEN SOURCE INTELLIGENCE (OSINT)

Il fine non giustifica mai i mezzi, ma trova legittimità sono nel rispetto delle norme

Nella **prima parte** dell'articolo, analizziamo il rapporto tra **OSINT e il Decreto Legislativo 231/2001**, che disciplina la responsabilità amministrativa delle imprese per illeciti commessi nel proprio interesse o vantaggio. Approfondiamo poi il ruolo dell'OSINT nel **monitoraggio dei dipendenti**, nelle strategie di **corporate security** e nella prevenzione dei reati-presupposto previsti dalla normativa, con un focus sulla gestione della compliance e sull'integrazione dell'OSINT nei **Modelli Organizzativi 231**. Vengono infine delineate le **best practice** per un utilizzo legittimo delle fonti aperte in azienda, evitando violazioni delle normative sulla privacy e sulla protezione dei dati personali.

Nella **seconda parte**, ci concentriamo sull'impiego dell'OSINT nelle **investigazioni private**, analizzando il quadro normativo che regola l'attività degli investigatori privati in Italia. Esaminiamo il **TULPS (Testo Unico delle Leggi di Pubblica Sicurezza)** e il **D.M. 269/2010**, che stabiliscono i requisiti per svolgere indagini in modo lecito. Approfondiamo inoltre le implicazioni **del GDPR e del Codice Privacy italiano**, evidenziando i rischi di compliance e le limitazioni imposte alla raccolta di dati personali. L'articolo fornisce infine una serie di **best practice operative**, delineando i confini tra investigazioni legittime e potenziali violazioni della privacy, con esempi concreti di utilizzo dell'OSINT per il **monitoraggio di soggetti, verifiche patrimoniali e prevenzione delle frodi**.

L'obiettivo è offrire una guida di riferimento per professionisti della sicurezza, investigatori privati e responsabili della compliance aziendale, fornendo indicazioni utili per sfruttare l'OSINT in modo efficace, nel rispetto delle normative vigenti e dei principi etici.

OSINT e Decreto Legislativo 231/2001

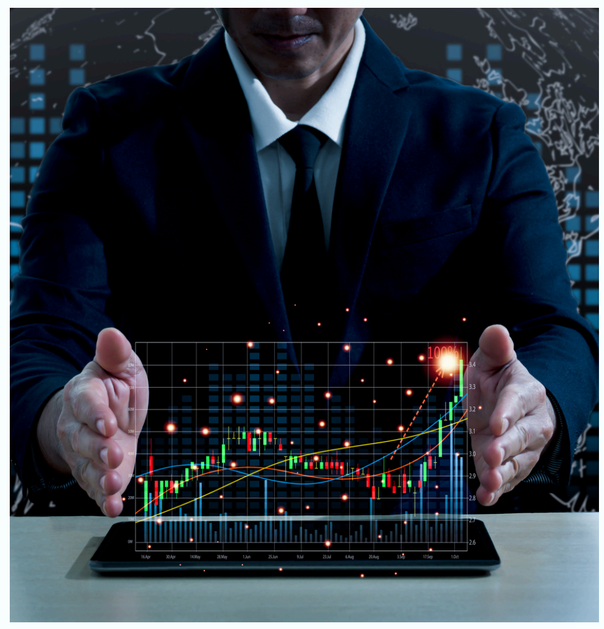
- OSINT e monitoraggio dei dipendenti: contesto e finalità
- Limiti legali al monitoraggio dei dipendenti tramite OSINT
- Implicazioni delle normative sulla privacy
- Decreto Legislativo 231/2001: compliance aziendale e controlli
- Best practice per un uso lecito dell'OSINT in ambito HR e security
- Casi studio e precedenti rilevanti

OSINT nelle Investigazioni private: normativa, privacy e best practice

- Licenza di investigatore privato: TULPS e D.M. 269/2010
- Uso di fonti aperte: normative e limiti per gli investigatori privati
- Privacy e rischi nell'utilizzo dell'OSINT
- Regole deontologiche e Codice di condotta
- Linee guida e best practice

OSINT E DECRETO LEGISLATIVO 231/2001

In ambito aziendale l'OSINT indica la raccolta e analisi di informazioni da fonti aperte e pubblicamente accessibili. Ciò include dati reperibili sul web, social network, forum, media tradizionali, registri pubblici e altri archivi disponibili al pubblico.



In particolare, possono rientrare nell'OSINT anche informazioni come profili aziendali, pubblicazioni ufficiali o persino i curriculum e i profili pubblici dei dipendenti. Le aziende impiegano tecniche OSINT, ad esempio, per il **recruiting** (social recruiting e controlli pre-assunzionali), per verifiche reputazionali sui propri dipendenti o candidati, nonché per finalità di **corporate security** (indagini interne, prevenzione di minacce e tutela del know-how aziendale). Tuttavia, l'uso di informazioni "aperte" non esonera dal rispetto delle normative: i dati devono essere **legalmente accessibili al pubblico senza violare le leggi sulla privacy**. Di seguito analizziamo i limiti e le tutele legali nell'utilizzo dell'OSINT per monitorare i lavoratori in Italia, con particolare riguardo al Decreto Legislativo 231/2001, al GDPR e allo Statuto dei Lavoratori, evidenziando best practice e casi concreti.

OSINT e monitoraggio dei dipendenti: contesto e finalità

In ambito HR, i datori di lavoro possono essere tentati di raccogliere informazioni online su candidati e dipendenti per ottenere un quadro più completo del profilo personale e professionale. Ad esempio, nei processi di selezione del personale, molte aziende confrontano le informazioni del CV con quelle disponibili sui social media del candidato (social recruiting). Allo stesso modo, durante il rapporto di lavoro, alcuni datori consultano i social network per verificare la condotta online dei propri dipendenti e tutelare l'immagine o gli interessi aziendali. In ambito di corporate security e compliance, le tecniche OSINT possono servire a individuare comportamenti anomali (es. divulgazione di informazioni riservate online, condotte illecite vantate sui social) o minacce interne, supportando audit e indagini interne. L'OSINT offre dunque un potente strumento di **monitoraggio proattivo**, ma il suo impiego sul personale aziendale solleva questioni giuridiche rilevanti in materia di **privacy**, **diritto del lavoro e tutela dei diritti fondamentali del lavoratore**.

Limiti legali al monitoraggio dei dipendenti tramite OSINT

In Italia esistono precisi limiti legali all'attività di sorveglianza del personale, anche quando si utilizzano informazioni pubbliche. L'Art. 8 dello Statuto dei Lavoratori (L. 300/1970) pone un divieto tassativo al datore di "effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, **nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale**". Ciò significa che **l'azienda non può raccogliere** indiscriminatamente qualsiasi informazione reperita online sul dipendente o candidato, soprattutto se attinente alla sfera privata e non pertinente alle sue capacità professionali. Ad esempio, dati estratti dai social network di natura strettamente personale (orientamenti politici, credo religioso, vita familiare, salute, ecc.) sono off-limits: tali informazioni sarebbero sia **irrilevanti** ai fini lavorativi sia potenzialmente **discriminatorie**, e il loro monitoraggio violerebbe la legge. Anche il **Garante** ha più volte richiamato questo principio, chiarendo che il datore di lavoro deve tutelare la sfera privata del lavoratore e **ridurre al minimo l'uso di dati personali non indispensabili** rispetto alle finalità perseguite. Inoltre, lo Statuto dei Lavoratori (art. 4) limita i controlli a distanza: l'uso di strumenti tecnologici per sorvegliare l'attività dei dipendenti richiede accordi sindacali o autorizzazione ispettiva, e in ogni caso **qualsiasi controllo non può essere "indiscriminato" né lesivo della dignità del lavoratore**. Questi principi si applicano in generale a qualunque forma di monitoraggio, compresa la consultazione di attività online: l'azienda può effettuare verifiche solo se giustificate, proporzionate e nel rispetto delle procedure previste dalla legge.

Implicazioni delle normative sulla privacy

L'utilizzo dell'attività OSINT su candidati o dipendenti comporta a tutti gli effetti un trattamento di dati personali, soggetto al Regolamento UE 2016/679 (GDPR) e al D.lgs. 101/2018. In questo senso è importante sottolineare che anche **i dati pubblicamente reperibili online rientrano nell'ambito esteso del GDPR**. Infatti, la natura "pubblica" dell'informazione non esenta dall'obbligo di trattarla secondo le basi giuridiche e i principi di liceità, correttezza e trasparenza. Innanzitutto, serve quindi individuare una base giuridica appropriata per raccogliere e utilizzare tali informazioni. Nella relazione datore-dipendente il consenso dell'interessato è in genere inidoneo, poiché non sarebbe libero a causa del rapporto sbilanciato di potere. I Garanti europei hanno ribadito che il consenso del lavoratore non può costituire fondamento valido per questi trattamenti. Il datore di lavoro dovrà dunque basarsi su altre condizioni di liceità, ad esempio il perseguimento di obblighi legali/contrattuali o il proprio **legittimo interesse**, purché quest'ultimo sia proporzionato e bilanciato con i diritti e le libertà del dipendente.

Con riferimento al legittimo interesse, il datore deve condurre un'**attenta valutazione comparativa**: l'interesse aziendale (ad esempio tutelare la sicurezza informatica, la reputazione aziendale o prevenire violazioni di norme interne) va ponderato con il diritto del lavoratore alla privacy e alla non discriminazione. Il GDPR impone inoltre i principi di **minimizzazione e proporzionalità**: ogni trattamento dev'essere necessario rispetto alla finalità perseguita e non eccedere quanto strettamente richiesto. Ciò implica che un monitoraggio massivo e costante della presenza online di tutti i dipendenti sarebbe difficilmente giustificabile. Al contrario, sono ammissibili controlli mirati e limitati nel tempo, ad esempio verifiche ad hoc in caso di sospetti fondati di comportamenti illeciti o raccoglimento di informazioni strettamente legate a una posizione lavorativa.

la natura "pubblica" dell'informazione non esenta dall'obbligo di trattarla secondo le basi giuridiche e i principi di liceità, correttezza e trasparenza

Il Garante Privacy, in un caso recente, ha ribadito il **"no" al controllo indiscriminato** dell'attività Internet dei dipendenti e ha sanzionato un ente pubblico che monitorava in modo sistematico la navigazione Internet dei propri dipendenti (inclusi accessi a Facebook e YouTube) senza adeguate garanzie. In questa vicenda, i log di navigazione erano stati usati dall'ente per contestare a un dipendente l'accesso a Facebook durante l'orario di lavoro; il Garante, oltre a rilevare irregolarità procedurali, ha stabilito che **anche con accordo sindacale, il monitoraggio deve rispettare i principi di necessità e proporzionalità del GDPR** e non può tradursi in una sorveglianza continua priva di giustificazione. Quindi l'Autorità ha ritenuto che il trattamento dei dati fosse **non necessario e proporzionato rispetto alle finalità dichiarate** (sicurezza della rete). Questo provvedimento del 2024 conferma quindi, **anche con una base giuridica astrattamente valida, che le modalità concrete di monitoraggio devono rispettare i principi del GDPR**, pena l'illiceità del trattamento e sanzioni.

Un ulteriore aspetto è la **trasparenza**: il GDPR richiede di informare chiaramente gli interessati sulle modalità di trattamento dei loro dati (artt. 13-14 GDPR). In ambito lavorativo, i dipendenti dovrebbero essere messi a conoscenza – ad esempio tramite l'**informativa privacy aziendale** o policy interne – se e quali tipi di controlli su fonti aperte possono essere effettuati dal datore di lavoro (fermo restando che alcuni controlli, come quelli difensivi in caso di illeciti, possono avvenire senza preavviso purché conformi alla legge).

In fase di **selezione del personale**, il Garante ha recentemente tracciato confini netti: nel 2024 è stato approvato un Codice di condotta per le Agenzie per il Lavoro che limita la raccolta e il trattamento dei dati personali, inerenti il profilo presenti sui social di natura professionale relativi ai candidati, al **rispetto del principio di minimizzazione e solo nella misura in cui la raccolta di tali dati sia necessaria e pertinente allo svolgimento del lavoro per il quale si effettua la ricerca**. Questo codice (promosso da Assolavoro) stabilisce che i colloqui e le valutazioni devono basarsi su dati oggettivi e professionali, escludendo indagini sulla vita privata online del candidato. **È quindi ammessa solo la consultazione di canali social a carattere professionale** (es. LinkedIn) e unicamente per verificare competenze e informazioni attinenti alla posizione lavorativa, nel rispetto della privacy. Sebbene tale codice riguardi la fase pre-assunzionale e le agenzie interinali, esso riflette un orientamento generale: utilizzare OSINT in ambito HR solo **nei limiti di pertinenza e rilevanza professionale**, evitando qualunque intrusione arbitraria nella sfera privata online. Il Codice quindi è rilevante perché per la prima volta stabilisce formalmente che **i social network privati dei candidati non vanno "spiati" ai fini della selezione**. Le agenzie che aderiscono a questo codice si impegnano a escludere tali pratiche, concentrandosi semmai su informazioni fornite direttamente dall'interessato o presenti su profili professionali. Ciò tutela i candidati da valutazioni occulte basate sulla vita privata online e costituisce un modello di riferimento anche per i datori di lavoro diretti, indicando la strada di una selezione **meritocratica e trasparente.**

Decreto Legislativo 231/2001: compliance aziendale e controlli

Il D.Lgs. 231/2001 ha introdotto in Italia la **responsabilità amministrativa (parapenale) delle società** per determinati reati commessi nel loro interesse o a loro vantaggio da dirigenti o dipendenti. In pratica, se un soggetto apicale o subordinato commette un illecito (fra quelli previsti dal decreto, come reati societari, corruzione, reati informatici, ecc.) per favorire l'azienda, anche quest'ultima può essere chiamata a rispondere e subire sanzioni pecuniarie o interdittive.

La norma spinge quindi le imprese ad adottare un **Modello di Organizzazione, Gestione e Controllo** ("Modello 231" o MOG) idoneo a prevenire tali reati e a istituire un **Organismo di Vigilanza (OdV)** che supervisioni l'efficace attuazione del modello. **Adottare un modello 231 efficace può esonerare l'ente dalla responsabilità**, perché significa che l'illecito è avvenuto eludendo fraudolentemente le misure preventive dell'azienda. In sostanza, il D.Lgs. 231/2001 ha inaugurato un approccio di **compliance aziendale integrata**, imponendo alle imprese di controllare e indirizzare i comportamenti di manager e dipendenti verso il rispetto della legge e delle procedure interne. Ciò si traduce nello sviluppo di **processi di monitoraggio e protocolli** atti a individuare tempestivamente violazioni o condotte a rischio. Anche le politiche di **whistleblowing** e le verifiche interne (audit) rientrano in questo contesto di controllo.

In relazione all'OSINT e al monitoraggio dei dipendenti, il modello 231 può legittimare l'azienda a svolgere **attività di verifica su informazioni** pubbliche allo scopo di prevenire reati-presupposto o condotte contrarie al codice etico. Ad esempio, per prevenire reati informatici o di violazione di segreti aziendali, l'OdV potrebbe monitorare il web per rilevare divulgazioni non autorizzate di dati riservati da parte di dipendenti. Analogamente, per prevenire reati di corruzione, frodi o conflitti d'interesse, l'azienda potrebbe raccogliere tramite OSINT segnali di stile di vita incompatibile, frequentazioni rischiose o altre informazioni pubbliche sugli addetti a funzioni sensibili. Tali attività, però, **devono sempre conciliarsi con le tutele privacy e lavoristiche** viste sopra.

Il modello 231, infatti, **non autorizza affatto un controllo illimitato sui lavoratori**, ma anzi deve essere costruito tenendo conto di tutte le normative settoriali (come quelle privacy, sicurezza sul lavoro, ecc...).

Non a caso, le Linee Guida di Confindustria sulla redazione dei modelli organizzativi sottolineano che il sistema di controllo interno 231 deve integrarsi con il **sistema di gestione della privacy** (GDPR) e con le altre procedure di conformità presenti in azienda. Dunque, un'azienda virtuosa in ottica 231 è chiamata anche a **formare il personale** sul rispetto delle norme (privacy compresa) e a prevedere misure disciplinari per chi le viola. Ad esempio, un dipendente che effettui in autonomia attività OSINT invasive o trattamenti illeciti di dati potrebbe esporre l'azienda a sanzioni (si pensi all'accesso abusivo a sistemi informatici altrui o al trattamento illecito di dati personali, che in certi casi configurano reati): il modello 231 dovrà prevedere controlli e sanzioni interne per prevenire anche queste condotte. In definitiva, il **ruolo del D.Lgs. 231/2001** è quello di spingere le imprese a una **gestione etica e conforme alle leggi**, bilanciando l'esigenza di controllo (anche tramite OSINT) con il rispetto dei diritti dei lavoratori.

Una compliance efficace sarà quindi quella che **previene illeciti** senza sfociare in una sorveglianza illegittima.

Best practice per un uso lecito dell'OSINT in ambito HR e security

Per conciliare le esigenze aziendali con il rispetto della privacy dei dipendenti, è opportuno adottare una serie di best practice nell'utilizzo di OSINT:

- **Definire policy e finalità chiare**: l'azienda dovrebbe predisporre policy interne che disciplinino in modo trasparente se e come possono essere raccolte informazioni online su candidati o dipendenti. Le finalità consentite devono essere specifiche e legittime (es. verifica dei requisiti professionali, tutela del patrimonio aziendale, sicurezza informatica);
- **Pertinenza e minimizzazione dei dati**: si raccolgano solo informazioni rilevanti e attinenti alla sfera professionale della persona. È buona norma limitarsi ai profili social professionali (come LinkedIn) o a contenuti pubblici riferiti alla vita lavorativa, evitando di ispezionare la sfera privata online. Qualunque dato eccedente (gossip, opinioni personali non connesse al lavoro) non va considerato.
- **Evitare categorie "sensibili" o protette**: come previsto dallo Statuto dei Lavoratori e dal GDPR, non si devono utilizzare come già precisato a fini valutativi informazioni su opinioni politiche, fede religiosa, orientamento sessuale, stato di salute, appartenenza sindacale o altri dati sensibili del dipendente. Anche se tali dati fossero pubblicamente visibili, il loro trattamento da parte del datore sarebbe vietato o altamente sconsigliato (a meno di eccezioni legali specifiche).
- **Base giuridica e valutazione d'impatto**: assicurarsi che ogni attività di OSINT abbia una solida base di liceità (es. legittimo interesse documentato) e condurre, se necessario, una Valutazione d'impatto sulla protezione dei dati (DPIA) quando il monitoraggio è sistematico o può presentare rischi elevati per i diritti degli interessati. Il coinvolgimento del DPO (Data Protection Officer) aziendale è raccomandato per valutare i rischi e le misure di garanzia.

- **Trasparenza verso gli interessati:** fornire, compatibilmente con le esigenze di sicurezza, un'informativa chiara ai dipendenti sui trattamenti di dati che l'azienda può effettuare, compresa l'eventuale consultazione di fonti online. Ad esempio, indicare nel regolamento interno che l'azienda si riserva di verificare le informazioni pubbliche divulgate dal dipendente in rete quando ciò sia necessario per tutelare interessi aziendali legittimi (comunicando sempre nel rispetto delle norme).
- **Proporzionalità e controllo mirato**: adottare un approccio graduale: l'OSINT sul dipendente non dovrebbe essere continuativo e indiscriminato, ma attivato in presenza di specifiche ragioni (es. fase di assunzione, sospetto di grave inadempimento, indagine su un incidente di sicurezza). Ogni controllo dev'essere documentato nelle motivazioni e nei risultati, così da poter dimostrare di aver operato in modo non arbitrario ma necessario.

- **Accuratezza e verifica delle fonti**: Le informazioni raccolte online vanno sempre prese con cautela e verificate se possibile. L'azienda dovrebbe evitare di trarre conclusioni affrettate da un dato OSINT (es. un post sui social frainteso). Se si intende usare una certa informazione in un processo decisionale (come un procedimento disciplinare), meglio assicurarsi della fondatezza (es. conservando uno screenshot autenticato, o raccogliendo testimonianze)
- **Limitare accesso e conservazione**: I dati raccolti via OSINT su dipendenti/candidati devono essere accessibili solo a personale autorizzato (HR, security manager, OdV) e conservati per il tempo strettamente necessario. Trascorso l'obiettivo (es. conclusione della selezione o dell'indagine interna), le informazioni dovrebbero essere cancellate o archiviate in forma anonima/aggregata.
- **Formazione e responsabilizzazione**: Formare i recruiter, i manager HR e i responsabili della sicurezza sulle implicazioni legali dell'OSINT. Devono conoscere cosa possono o non possono fare (ad esempio, che è vietato "pedinare" digitalmente un dipendente nella sua vita privata o raccogliere dati sensibili). Promuovere un uso etico degli strumenti OSINT fa parte della cultura di compliance aziendale.

- **Coordinamento con il Modello 231 e l'OdV:** Se l'azienda ha un OdV ex D.Lgs.231, questo organo dovrebbe essere coinvolto nel definire controlli leciti sui dipendenti. Procedure di indagine interna che prevedono l'utilizzo di fonti OSINT devono essere inserite nel modello organizzativo e approvate dall'OdV, assicurando che siano rispettosi dei diritti dei lavoratori e finalizzati solo alla prevenzione di illeciti rilevanti.

Seguire queste best practice consente di sfruttare le potenzialità dell'OSINT (che può effettivamente dare un valore aggiunto in termini di sicurezza e conoscenza) senza incorrere in violazioni della privacy o abusi dei diritti dei dipendenti. L'obiettivo è mantenere un equilibrio: l'OSINT deve restare un mezzo di tutela e prevenzione mirata, non uno strumento di sorveglianza generale sul personale.

Casi studio e precedenti rilevanti

La giurisprudenza e gli interventi normativi recenti forniscono utili indicazioni sui confini dell'uso delle informazioni online in ambito lavorativo. In ambito disciplinare, numerosi casi hanno riguardato dipendenti sanzionati o licenziati a causa di post o comportamenti su social network. La Corte di Cassazione ha affermato in più occasioni che offendere o diffamare l'azienda su Facebook costituisce una violazione grave del dovere di fedeltà e può legittimare il licenziamento per giusta causa. Ad esempio, la Cassazione (ord. n. 12142/2024) ha confermato il licenziamento di un lavoratore che aveva pubblicato frasi gravemente denigratorie verso i vertici aziendali, ritenendo che la diffusione di un commento offensivo su Facebook – mezzo potenzialmente idoneo a raggiungere un numero indeterminato di persone – lede irreparabilmente il vincolo fiduciario ed integra gli estremi della diffamazione.

Anche se il post era visibile solo agli "amici" dell'autore, la natura del social fa sì che il messaggio possa facilmente circolare in pubblico, giustificando la sanzione. In altri casi, tuttavia, i giudici hanno valutato le circostanze attenuanti: con l'ord. 26446/2024, la Cassazione ha ritenuto non licenziabile un dipendente che aveva insultato a caldo il datore su Facebook, poiché lo sfogo era consequenziale a un illecito subito (un grave comportamento ingiusto dell'azienda) e dunque in parte "scusato" dal contesto. Queste pronunce indicano che, sul piano probatorio, le informazioni tratte dai social network possono essere utilizzate nel giudizio (ad es. screenshot dei post, testimonianze di colleghi che hanno visto il contenuto) e che ogni caso va valutato bilanciando la libertà di espressione del lavoratore con i doveri di lealtà e decoro verso l'azienda.

Infine, in termini di responsabilità 231, vale la pena menzionare che se un'azienda adottasse prassi sistematiche di monitoraggio illegittimo (magari tramite software non autorizzati o investigatori senza titolo) potrebbe incorrere non solo in sanzioni privacy ma anche in profili di responsabilità penale-amministrativa. Ad esempio, l'accesso abusivo a sistemi informatici o il trattamento illecito di dati personali sono reati informatici contemplati tra quelli presupposto del D.Lgs. 231/2001.

Un modello 231 efficace dovrebbe prevenire anche tali condotte: se un dipendente dell'area security, nel fare OSINT, superasse i limiti di legge (violando account privati, raccogliendo dati in violazione di provvedimenti del Garante, ecc.), l'azienda rischierebbe conseguenze sia sul piano del GDPR (sanzioni fino a milioni di euro) sia, in casi estremi, sul piano penale qualora si configuri un reato informatico. Perciò, i confini legali analizzati non sono meri formalismi, ma parte integrante della compliance complessiva dell'azienda.

L’uso dell’OSINT per monitorare dipendenti e candidati è un terreno insidioso che richiede un equilibrio delicato tra interessi aziendali e diritti individuali. Da un lato, le informazioni open-source possono aiutare le imprese a **prevenire rischi, proteggere il patrimonio e assumere decisioni informate**; dall’altro, i lavoratori hanno diritto a non essere sottoposti a una sorveglianza indebita o discriminatoria nella loro vita digitale. La normativa italiana (Statuto dei Lavoratori, Codice Privacy) ed europea (GDPR) traccia confini precisi: **il monitoraggio è ammissibile solo se lecito, trasparente, pertinente e proporzionato**. Il Decreto 231/2001 aggiunge un ulteriore livello, stimolando le aziende a dotarsi di controlli interni efficaci ma anche imponendo loro di rispettare tutte le leggi rilevanti nel farlo. In pratica, un’azienda responsabile dovrà integrare le **best practice** sopra descritte nella propria prassi quotidiana, così da sfruttare l’OSINT in modo **etico e legale**. Ciò significa **formare** il personale, aggiornare le policy interne, coinvolgere gli **organismi di vigilanza** e il DPO, e coltivare una cultura aziendale che valorizzi sì la sicurezza e la compliance, ma **mai a scapito della privacy e della dignità delle persone**.

Solo in questo modo l’OSINT potrà rivelarsi uno strumento davvero utile e sostenibile nel lungo periodo, contribuendo alla sicurezza e alla conformità dell’organizzazione senza infrangere la fiducia tra datore di lavoro e lavoratore.

OSINT NELLE INVESTIGAZIONI PRIVATE: NORMATIVA, PRIVACY E BEST PRACTICE

L' OSINT – ossia la raccolta di informazioni da fonti aperte e pubblicamente accessibili – è diventata uno strumento fondamentale anche nel campo delle investigazioni private. Tuttavia, in Italia l'uso dell'OSINT da parte di investigatori privati è subordinato a precisi limiti legali. Occorre infatti rispettare le norme in materia di pubblica sicurezza (licenze ex TULPS), le disposizioni specifiche per gli investigatori privati, nonché le stringenti regole sulla privacy. Di seguito analizziamo il quadro normativo applicabile e le best practice per un uso legittimo dell'OSINT in ambito investigativo.

Licenza di investigatore privato: TULPS e D.M. 269/2010

In Italia l'attività di investigazione per conto di privati è strettamente regolamentata. L'art. 134 del Testo Unico delle Leggi di Pubblica Sicurezza (TULPS) proibisce a chiunque di svolgere "investigazioni o ricerche o di raccogliere informazioni per conto di privati" senza apposita licenza prefettizia. Ciò significa che anche le investigazioni svolte tramite OSINT rientrano tra le attività riservate agli investigatori autorizzati. In altre parole, chiunque effettui investigazioni per terzi (anche solo raccogliendo informazioni online) deve possedere la licenza ex art. 134 TULPS, pena l'esercizio abusivo di attività investigativa.

Il Decreto Ministeriale 269/2010 (Ministero dell'Interno) ha dato attuazione a tali principi, delineando requisiti rigorosi e tipologie operative per ottenere e mantenere la licenza di investigatore privato. Questo regolamento ha colmato un vuoto normativo, distinguendo nettamente l'attività di **investigazione privata** (ad esempio indagini familiari, infedeltà, controllo dipendenti) da quella di **informazione commerciale** (raccolta di dati su imprese o persone ai fini economico-commerciali). Il D.M. 269/2010 specifica i requisiti di onorabilità, formazione (laurea in materie pertinenti, corsi specialistici) ed esperienza professionale necessari per ottenere la licenza. Inoltre, introduce diverse figure professionali (investigatore privato titolare, investigatore dipendente, informatore commerciale, ecc.) e impone che ogni investigazione sia svolta nel rispetto della legge e delle normative vigenti in materia di privacy e sicurezza.

In sintesi, per utilizzare legittimamente l'OSINT in un'indagine privata in Italia occorre essere un investigatore autorizzato, operante secondo i titoli e le modalità stabilite dal TULPS e dal D.M. 269/2010.

Uso di fonti aperte: normative e limiti per gli investigatori privati

Le fonti OSINT includono siti web, motori di ricerca, registri pubblici, social network, media tradizionali, documenti pubblicati e più in generale tutte le informazioni di dominio pubblico. Un principio cardine è che l'investigatore può attingere solo a fonti aperte **legalmente accessibili a chiunque**, senza forzare restrizioni, violare sistemi di protezione e normativa sulla privacy. Ciò implica ad esempio che l'**investigatore non può**: accedere ad account privati, commettere accessi abusivi a sistemi informatici, effettuare intercettazioni o altre attività riservate alle forze dell'ordine. Tali metodi illeciti esulano dall'OSINT e costituirebbero reato. Allo stesso modo, pratiche borderline come il "dumpster diving" (rovistare nei rifiuti in cerca di documenti) sono considerate illegali e dunque precluse.

L'OSINT propriamente detto si limita quindi a informazioni liberamente reperibili: ad esempio profili social pubblici, post su blog, articoli di giornale, visure camerali e dati catastali pubblici, informazioni presenti su siti istituzionali, ecc. L'investigatore privato, pur potendo analizzare in profondità queste fonti, deve sempre operare **nel rispetto dei diritti altrui**. Infatti, un fattore fondamentale da considerare è che anche i dati pubblicamente visibili possono riguardare la sfera personale e privata di un individuo: quindi la loro raccolta e ulteriore trattamento rientra nelle tutele previste dalla legge (come vedremo in tema di GDPR).

Inoltre, come approfondiremo più avanti, l'investigatore è tenuto a rispettare i **limiti del mandato ricevuto**: non può svolgere ricerche estranee o eccedenti rispetto all'incarico concordato con il cliente. Ad esempio, l'agenzia investigativa non può "allargare" l'indagine ad altre persone o aspetti non pertinenti, né avviare di propria iniziativa investigazioni senza richiesta formale. Infatti, è espressamente vietato condurre investigazioni di propria iniziativa: ogni attività deve essere giustificata da un incarico scritto del cliente, che indichi gli elementi di fatto e il diritto da tutelare. In sintesi, le norme italiane consentono agli investigatori privati di impiegare tecniche OSINT, ma sempre entro **confini ben definiti**:

- solo soggetti muniti di licenza possono offrire tali servizi;
- le informazioni raccolte devono provenire da fonti aperte accessibili legalmente;
- l'attività investigativa deve restare nei limiti dell'incarico e della legge, senza sconfinare in violazioni di sistemi o diritti altrui.

Privacy e rischi nell'utilizzo dell'OSINT

Un uso disinvolto dell'OSINT può facilmente sfociare in violazioni della privacy se non si adottano le dovute cautele. Bisogna considerare che **qualsiasi informazione personale raccolta**, ancorché pubblica online, costituisce "dato personale" e il suo trattamento deve rispettare i principi del Regolamento UE 2016/679 (GDPR) e il Codice Privacy italiano (D.lgs. 196/2003 come modificato dal D.lgs. 101/2018) che costituiscono il riferimento centrale in materia di trattamento dati anche per le investigazioni private. Di seguito vengono illustrati alcuni principi fondamentali che possono trovare applicazione diretta nell'attività OSINT degli investigatori:

- **Base giuridica del trattamento**: L'art. 6 GDPR richiede una base di liceità. Nelle investigazioni private, poiché è impraticabile ottenere il consenso dell'interessato (sarebbe contraddittorio informarlo dell'indagine), ci si basa in genere sul legittimo interesse (art. 6, par.1, lett. f) del titolare o del cliente nel far valere un diritto) oppure sulla necessità di accertare o difendere un diritto in sede giudiziaria. Quest'ultima evenienza è esplicitamente riconosciuta come deroga nel GDPR (art. 9, par.2, lett.f) ove si evince che l'investigatore può trattare dati personali senza consenso quando la finalità è appunto "far valere o difendere un diritto in sede giudiziaria" del proprio cliente. Deve però risultare da un atto scritto (mandato) e sussistere la proporzionalità tra il diritto perseguito e la lesione della privacy che l'indagine comporta. In pratica, il diritto fatto valere deve essere di rango almeno pari a quello dell'interessato alla tutela dei propri dati (ad es. tutela della propria incolumità, difesa patrimoniale da un illecito, tutela dei figli, ecc.). Senza un valido interesse giuridico, un'indagine investigativa non sarebbe lecita.

- **Trattamento di categorie particolari di dati**: il già citato art. 9 GDPR vieta anche il trattamento di dati sensibili (origine etnica, opinioni politiche, credo religiosi, salute, vita sessuale, ecc.). Questi dati godono di tutela rafforzata: l'investigatore privato può raccoglierli solo se strettamente necessario per le finalità dell'incarico e se sussiste una specifica base giuridica (tipicamente, la necessità di far valere un diritto in sede giudiziaria, come dettaglieremo oltre). In mancanza di tali condizioni, il trattamento di informazioni sensibili o giudiziarie costituisce grave violazione privacy. Un rischio concreto, ad esempio, sarebbe profilare dettagli sulla vita privata di un soggetto indagato (gusti, frequentazioni, credo religioso) che non siano rilevanti per l'indagine: ciò oltrepasserebbe il lecito e potrebbe configurare un trattamento illecito di dati sensibili. In tal senso la normativa italiana si è adeguata prevedendo che gli investigatori privati possano trattare categorie particolari di dati esclusivamente per le finalità connesse alla difesa di un diritto in giudizio o all'attività di investigazione difensiva penale (vds. Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]. Ad esempio, un investigatore potrà raccogliere dati sulla salute o vita intima di una persona solo se strettamente rilevanti per un processo (si pensi a un'indagine in ambito assicurativo per verificare un finto infortunio, dove i dati medici sono necessari alla prova). In ogni caso, tali dati vanno maneggiati con estrema cautela e protetti secondo le regole deontologiche e l'art. 10 del Codice Privacy (che disciplina i dati giudiziari relativi a reati e condanne).

Anche i dati su procedimenti penali o condanne possono essere trattati dall'investigatore privato unicamente se indispensabili per l'indagine in corso (es. verificare precedenti penali di un soggetto se rilevanti per la causa) e nei limiti autorizzati dalla legge. In ogni caso, tali dati vanno maneggiati con estrema cautela e protetti secondo le regole deontologiche e l'art. 10 del Codice Privacy (che disciplina i dati giudiziari relativi a reati e condanne).
finalità e minimizzazione: i dati raccolti devono essere pertinenti e limitati a quanto necessario rispetto alle finalità dell'indagine. Se un investigatore accumula una mole di informazioni eccedenti (magari "scaricando" tutto il profilo social di una persona, comprese informazioni irrilevanti), viola i principi di pertinenza e non eccedenza.
Il Garante Privacy, con il Provvedimento del 16 settembre 2021 [9718933] ha ammonito un'agenzia investigativa proprio per aver trattato dati non pertinenti ed eccedenti rispetto all'oggetto dell'indagine. Nello specifico, l'agenzia incaricata di investigare una dipendente bancaria ha indebitamente raccolto e diffuso dati riguardanti la madre di lei, estranea all'indagine: il trattamento di queste informazioni "ultra vires" ha portato alla sanzione dell'ammonimento per violazione dei principi di minimizzazione (art. 5 GDPR).

- **Sicurezza e conservazione dei dati**: raccogliere dati OSINT significa anche archiviarli temporaneamente (es. screenshot di pagine web, profili social, copie di documenti trovati online). Questi archivi devono essere protetti da accessi non autorizzati e violazioni di sicurezza. Un investigatore privato ha l'obbligo deontologico di garantire la massima riservatezza e sicurezza alle informazioni acquisite. Data la sensibilità di certe indagini, è fondamentale implementare misure tecniche adeguate (dispositivi sicuri, crittografia, ecc.) per evitare data breach. In caso di violazione dei dati raccolti, l'agenzia investigativa ne risponderebbe sia verso gli interessati sia verso l'Autorità Garante. Inoltre, occorre rispettare il principio di limitazione della conservazione: i dati personali vanno cancellati al termine dell'attività investigativa, salvo conservarli solo per il tempo necessario alla trasmissione al cliente o al loro utilizzo in giudizio. Trattenere copie dei dati senza motivo legale espone a sanzioni.
- **Altri rischi legali**: un investigatore che uscisse dal perimetro dell'OSINT (fonti aperte) e ricorresse a metodi invasivi incorrerebbe in responsabilità sia penali che civili. Ad esempio, accedere a comunicazioni riservate (chat private, email) senza autorizzazione configura reati (interferenze illecite, violazione di corrispondenza); pubblicare o diffondere informazioni personali non pertinenti potrebbe integrare diffamazione o violazione della privacy dell'art. 167 del Codice Privacy. Anche l'utilizzo di informazioni OSINT in modo non conforme allo scopo comporta rischi: se un cliente utilizzasse il rapporto investigativo per fini diversi (es. per ricattare qualcuno o diffondere sui social dettagli della vita privata altrui), potrebbe scaturire una responsabilità sia per il cliente sia per l'investigatore se consenziente. È dunque cruciale che l'agenzia educhi il cliente sul corretto uso delle informazioni fornite.

In definitiva, l'OSINT è perfettamente legale solo se inserito in un contesto di liceità e proporzionalità. Il mancato rispetto delle regole di privacy e deontologia può comportare sanzioni amministrative, la nullità/inutilizzabilità in giudizio delle prove raccolte e danni reputazionali per l'investigatore. I rischi riguardano sia le investigazioni private (ad es. casi familiari o personali) sia le indagini commerciali per aziende: in entrambi i casi occorre garantire che l'uso di dati aperti non leda indebitamente la privacy individuale e che ogni attività sia giustificata da un interesse legittimo concreto (tutela di un diritto, prevenzione di illecito, ecc...).

Regole deontologiche e Codice di condotta

In attuazione dell'art. 20, comma 4, D.lgs. 101/2018, il Garante Privacy ha emanato e pubblicato in G.U. (15 gennaio 2019) le "Regole deontologiche relative al trattamento di dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria". Queste regole, vincolanti per chi esercita la professione investigativa autorizzata, integrano il quadro normativo. Tra le prescrizioni principali vi sono:

- **Incarico scritto e motivato**: l'investigatore deve ricevere un mandato formalizzato per iscritto prima di iniziare l'indagine. Nell'incarico vanno indicati il diritto che si intende tutelare in giudizio (o il riferimento a un procedimento penale) e i motivi concreti che giustificano l'indagine, oltre all'arco temporale di svolgimento. Ciò garantisce trasparenza e legittimità dello scopo.
- **Obbligo di Informativa**: di regola l'investigatore dovrebbe fornire al soggetto indagato l'informativa sul trattamento dei dati (art. 13-14 GDPR). Tuttavia, la regola deontologica conferma che vi è un'eccezione quando ciò risulti impossibile o in contrasto con la finalità dell'indagine. In pratica, se informare la persona significa vanificare l'investigazione, l'informativa può essere omessa o differita. Come già specificato rappresenta una deroga al principio di trasparenza, ammessa dal GDPR stesso (art. 14, par.5) ma limitata a questi casi particolari.
- **Limiti alla delega e sub-incarichi**: l'investigazione deve essere eseguita personalmente dall'investigatore o da eventuali collaboratori nominativamente indicati nel mandato. Non è lecito "passare" l'incarico ad altri non autorizzati all'insaputa del cliente o dell'interessato. Questo tutela sia la riservatezza sia il controllo sull'operato (evitando che qualcuno senza licenza partecipi alle indagini).
- **Conservazione e cessazione del trattamento**: al termine dell'indagine, il trattamento dei dati personali deve cessare immediatamente, fatti salvi giusto il tempo e le modalità per comunicare i risultati al committente. L'investigatore non può creare archivi permanenti con i dati delle persone investigate, né riutilizzarli per altri scopi. I dati vanno cancellati (o resi anonimi) una volta consegnata la relazione finale al cliente, salvo che debbano essere conservati per esercitare a propria volta un diritto in sede di eventuale controversia con il cliente o per difendersi (ad es. conservare copia del rapporto come prova del lavoro svolto).
- **Principio di pertinenza e aggiornamento**: le regole deontologiche enfatizzano il dovere di trattare solo dati pertinenti e non eccedenti. Se durante l'indagine si raccolgono informazioni non utili o coinvolgenti terzi estranei, queste vanno eliminate. Inoltre, l'investigatore dovrebbe assicurarsi dell'esattezza e attualità dei dati (principio di accuratezza, art. 5 GDPR) – ad es. verificare che le notizie trovate siano aggiornate e attendibili, specie se provengono dal web dove circolano anche informazioni obsolete o inesatte.
- **Rispettare segreto professionale e sicurezza**: il codice deontologico ribadisce il dovere di riservatezza. L'investigatore deve mantenere il segreto professionale sulle informazioni acquisite, analogamente a quanto fa un avvocato. Ciò significa non divulgare a terzi estranei i dati raccolti, proteggere i fascicoli e riferire solo al cliente e, se richiesto, all'autorità giudiziaria. Questo vincolo, oltre a tutelare la privacy degli interessati, è fondamentale per la fiducia nel rapporto investigatore-cliente.

In caso di violazioni di queste regole il Garante può comminare sanzioni amministrative. Inoltre, l'uso indebito di dati potrebbe esporre l'agenzia investigativa anche a richieste risarcitorie da parte degli interessati lesi.
Infine, va ricordato che certe violazioni della privacy costituiscono reato in Italia (art. 167 e 167-bis D.lgs. 196/2003, ad esempio, puniscono la comunicazione o diffusione illecita di dati personali).

L'aderenza alle normative privacy non è solo un onere burocratico, ma una componente essenziale della liceità dell'indagine

Linee guida e best practices

Alla luce del quadro normativo sopra delineato, è possibile enucleare alcune best practice operative affinché l'uso dell'OSINT da parte di investigatori privati sia sempre legittimo e rispettoso di privacy e compliance:

- **Operare solo se autorizzati e con mandato valido**: chi effettua ricerche OSINT per conto terzi deve essere un investigatore munito di licenza prefettizia ex TULPS. È buona prassi indicare nel mandato scritto tutti i dettagli richiesti (soggetti coinvolti, diritto da tutelare, durata, ecc.). Non iniziare mai un'indagine OSINT senza un incarico formale; ciò garantisce la copertura di una base giuridica solida (legittimo interesse/difesa di un diritto) e protegge l'investigatore da accuse di abuso.
- **Rispettare il perimetro delle fonti aperte**: limitarsi a raccogliere informazioni da fonti pubbliche e liberamente accessibili. Prima di usare uno strumento o accedere a una risorsa, chiedersi: questa informazione è pubblicamente disponibile a chiunque? Se la risposta è no (es. profilo social privato, database protetto, email interna trafugata), allora non rientra nell'OSINT lecito. Evitare qualunque espediente che configuri un accesso abusivo (hacking, social engineering, furto di credenziali, ecc.) o preveda l'utilizzo di identità fittizie online, finalizzate ad "adescare" il soggetto investigato spingendolo a condividere informazioni.

- **Minimizzazione e pertinenza**: adottare un approccio di *data minimization* fin dall'inizio. Definire chiaramente quali informazioni si cercano in base agli scopi dell'indagine. Durante la fase di raccolta, filtrare subito i risultati, evitando di conservare dati palesemente estranei. Ad esempio, se si indaga su sospetti ammanchi in azienda, potrebbero essere rilevanti notizie su precedenti frodi o attività economiche occulte del dipendente, ma probabilmente non lo sono dettagli sulla sua vita privata (hobby, foto di famiglia) che eventualmente emergano online – questi andrebbero scartati immediatamente. I dati "non pertinenti la finalità prevista" devono essere eliminati e non inclusi nel rapporto di indagin. Questo vale in particolare per dati di terze persone: se nel materiale OSINT compaiono informazioni su persone non oggetto diretto dell'indagine (colleghi, familiari, amici del soggetto investigato), vanno ignorate salvo che abbiano uno stretto collegamento con l'indagine stessa.
- **Accuratezza e verifica delle fonti**: le informazioni open source possono talvolta essere inesatte, obsolete o manipolate. È buona norma verificarle incrociando più fonti affidabili. Ad esempio, se si trova sul web un riferimento a un precedente penale del soggetto, andrebbe riscontrato (quando possibile) con registri ufficiali o documenti giudiziari pubblici, per evitare errori di persona o fake news. Allo stesso modo, per profili social, assicurarsi che appartengano effettivamente al soggetto in questione (molti individui hanno omonimi). Mantenere evidenza delle fonti consultate e, quando le informazioni saranno inserite nel rapporto finale, citarne la provenienza (es. URL, data di acquisizione) così da dimostrare trasparenza e consentire eventuali controlli futuri. Questo non è solo metodo investigativo corretto ma anche requisito implicito del principio di esattezza dei dati (art. 5 GDPR).

- **Informativa e diritti degli interessati**: come visto, l'investigatore ha facoltà di differire o omettere l'informativa privacy all'indagato durante l'indagine. Ciò non toglie che debba farsi trovare preparato a gestire i diritti dell'interessato eventualmente esercitati. Ad esempio, se la persona oggetto d'indagine, venutane a conoscenza (magari perché citata in giudizio con prove raccolte dall'investigatore), presenta una richiesta di accesso ai suoi dati, l'investigatore dovrà rispondere nei termini di legge. Il Codice Privacy consente limitazioni all'esercizio dei diritti per non pregiudicare la difesa in giudizio, ma tali valutazioni devono essere fatte caso per caso e preferibilmente con l'ausilio del legale del cliente. Best practice è predisporre un'informativa generale sul sito o documenti dell'agenzia, rivolta ai potenziali interessati, che spieghi in che casi i loro dati possono essere trattati (per incarico investigativo) e con quali garanzie, indicando anche la possibilità di esercitare i diritti in differita. Ciò aumenta la trasparenza complessiva dell'attività investigativa senza comprometterne l'esito.
- **Sicurezza dei dati e segreto professionale**: trattare dati personali nelle indagini comporta l'obbligo di custodirli in modo sicuro. È consigliato utilizzare sistemi informatici protetti, aggiornati e possibilmente isolati per le ricerche OSINT (ad esempio, usare un PC dedicato o macchine virtuali, evitare di fare login con account personali durante le indagini online, usare connessioni VPN per anonimizzare le ricerche e proteggersi da occhi esterni – questo sia per sicurezza sia per non allertare il soggetto lasciando tracce evidenti delle proprie consultazioni). I file e i report dovrebbero essere criptati o comunque protetti da password, e condivisi col cliente con canali sicuri. Dal punto di vista organizzativo, solo il personale strettamente coinvolto nell'indagine deve avervi accesso (principio del need-to-know). Mantenere il segreto professionale significa anche che l'investigatore non discuterà dell'indagine con nessuno al di fuori del cliente e, se necessario, dell'autorità giudiziaria. Anche all'interno dell'agenzia, eventuali assistenti o consulenti tecnici dovrebbero essere vincolati da accordi di riservatezza. In caso di cessazione anticipata dell'incarico o esito negativo, i dati raccolti vanno restituiti al cliente o distrutti, a seconda degli accordi, certificando la distruzione se richiesto.
- **Documentazione della compliance**: per maggiore tutela, l'agenzia investigativa dovrebbe tenere un registro interno delle attività di trattamento (come previsto dall'art. 30 GDPR se applicabile, o comunque come buona prassi anche se non obbligatorio per dimensione aziendale). Nel registro si potrà annotare per ogni caso: base giuridica (incarico per diritto in giudizio), categorie di dati trattati (es. dati anagrafici, dati giudiziari, etc.), misure di sicurezza adottate, tempi di cancellazione previsti. Ciò torna utile in caso di verifiche del Garante o contestazioni, per dimostrare l'accountability richiesta dal GDPR. Ugualmente, seguire eventuali Linee guida del Garante o provvedimenti simili: ad esempio il provvedimento n. 9718933 citato in precedenza, con cui il Garante ha ammonito sugli obblighi di eliminare dati non pertinenti, diventa un riferimento da tenere presente per evitare analoghi errori.
- **Aggiornamento professionale e collaborazione con esperti**: l'ambito OSINT è in continua evoluzione (nuove fonti, nuove tecniche, aggiornamenti normativi). È importante che l'investigatore privato si aggiorni regolarmente: partecipare a corsi specifici su OSINT e GDPR, aderire ad associazioni di categoria (come Federpol, ONISSF, etc.) che diffondono best practice, consultare le newsletter del Garante Privacy per restare informato sulle novità normative e sui casi sanzionati. In casi complessi, può essere utile coinvolgere un Data Protection Officer (DPO) o un consulente legale esperto in privacy per valutare a monte i profili di rischio dell'indagine e predisporre misure di garanzia (ad esempio, un'analisi d'impatto sulla protezione dati – DPIA – se l'investigazione prevede una sorveglianza sistematica su larga scala online, benché raramente ciò ricorra nelle investigazioni private standard).

In definitiva, l'uso legittimo dell'OSINT in ambito investigativo richiede un equilibrio tra efficacia dell'indagine e rispetto dei diritti individuali. **Seguendo scrupolosamente le normative (TULPS, D.M. 269/2010) e i dettami di privacy e deontologia, l'investigatore può sfruttare le fonti aperte come preziosa risorsa informativa senza incorrere in illeciti**. Le best practice sopra descritte – dal rigore nella definizione dell'incarico, alla cura nella gestione dei dati – rappresentano linee guida fondamentali. **L'obiettivo è garantire che le investigazioni OSINT forniscano risultati utili e utilizzabili (ad esempio prove in giudizio) ottenuti con metodi leciti, tutelando al contempo la riservatezza e la dignità delle persone coinvolte.**

Solo in questo modo l'OSINT potrà esprimere tutto il suo potenziale nell'investigazione privata, rimanendo entro limiti etici e legali.